EXAMTOPICS
- Expert Verified, Online, **Free**.

Custom View Settings

Topic 1 - Question Set 1

Question #1 *Topic 1*

After your company migrates their on-premises email solution to Microsoft Exchange Online, you are tasked with assessing which licenses to acquire.

You are informed that licenses acquired for the company's IT and Managers groups should allow for the following:

- The IT group needs to have access to the Microsoft Azure Active Directory (Azure AD) Privileged Identity Management.
- Both the IT and Managers groups should have access to Microsoft Azure Active Directory (Azure AD) conditional access.

You need to make sure that the licensing costs are kept to a minimum.

Which two of the following options should you recommend? (Choose two.)

A. You should acquire Microsoft 365 E3 licenses for the Managers group members.

B. You should acquire Microsoft 365 E5 licenses for the Managers group members.

C. You should acquire Microsoft 365 E3 licenses for the IT group members.

D. You should acquire Microsoft 365 E5 licenses for the IT group members.

Correct Answer: *AD*

The Managers group and the IT group require access to conditional access, which is available in Microsoft 365 E3 and higher.

The IT group requires access to PIM, which is available in Microsoft 365 E5.

Community vote distribution

AD (100%)

fofo1960 Highly Voted 12 months ago

IT = E5
Mangers = E3

upvoted 34 times

EG_Jack 11 months, 3 weeks ago

Correct

upvoted 3 times

ElimGarak Highly Voted 1 year ago

Answer B and answer D are exactly the same:
You should acquire Microsoft 365 E5 licenses for the Managers group members.

I guess answer D should be :
You should acquire Microsoft 365 E5 licenses for the IT group members.

upvoted 15 times

NASH77 Most Recent 4 weeks ago

Selected Answer: AD

PIM only available in E5, IT users will get E5.
Manager Groups require CAP which is available in E3 and E5 but E3 is least cost option.

upvoted 1 times

Contactfornitish 5 months, 4 weeks ago

Sample of blunder copy paste.

PIM not available without E5. Trust me I managed enterprise for half decade and more
CAS available with Azure AD P1, which comes with E3. So IT needs PIM which is logical as high risk accounts should be protected and access given with justification. Managers need E3 only for CAS

upvoted 1 times

JamesM9 7 months ago

The answers are worded incorrectly, but in short - IT group need E5 licenses for PIM and the Managers group need E3 licenses.

upvoted 1 times

fmagnani 7 months, 4 weeks ago

B and D are the same answer. So why B is wrong?

upvoted 1 times

joergsi 8 months ago
Where is the difference between answers B and D?
upvoted 2 times

joergsi 8 months ago
Passed the Exam with 830 Points!
upvoted 1 times

Zethembiso 8 months, 2 weeks ago
This Question and provided answers does not make sense, but Privileged Identity Management only comes a part of E5 Plan, while you can have access to Conditional Access on E3 plan and and above
upvoted 1 times

Glorence 9 months ago
I think there's a mistake in the answer options, isn't D: E5 licenses for IT group members? so the answer is correct A and D.
upvoted 2 times

mikl 9 months, 1 week ago
IT needs : Microsoft 365 E5 = Azure P2 = Privileged Identity Management
Managers needs : Microsoft 365 E3 = Azure P1 = Conditional Access
upvoted 8 times

tcmaggio 9 months, 3 weeks ago
I love these ExamTopics and all the good stuff but sincerelly, this one BEGINS with a silly mistake... IT = E5 for the PIM features, E3 for managers since MFA is a common feature, life goes on. Readers, always check comments, follow the links and do not thrust what you s specially if you think you have a better answer.. go for it!
upvoted 3 times

mfaisal786 10 months ago
it should be B and D , because Azure AD Premium 2 contains both conditional and Privileged Identity which is part of E5 plan
upvoted 1 times

Oceanide 10 months, 2 weeks ago
Answer D must be E5 to IT group members.
So A and D are correct.
upvoted 1 times

sabin001 10 months, 4 weeks ago
Microsoft Azure Active Directory Privileged Identity Management requires an Azure AD Premium P2 license. This license comes as part the Microsoft 365 E5 license.

Conditional Access requires the Azure AD Premium P1 license. This comes as part of the Microsoft E3 license.
upvoted 3 times

mikl 9 months, 1 week ago
I agree.
upvoted 1 times

Ronger 1 year, 3 months ago
IT needs E5 for PIM? im confused
upvoted 3 times

tarakuds 1 year, 3 months ago
there was an error in the options, should be - E3 for managers and E5 for IT.
upvoted 20 times

FumerLaMoquette 1 year, 2 months ago
Yeah i agree, E3 for managers, E5 for IT. E5 has PIM, E3 doesn't. PIM requires AAD P2.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements#valid-licens
upvoted 6 times

zul_n 1 year ago
agree with this one.
upvoted 2 times

lafcow 1 year ago
correct
upvoted 1 times

Question #2 *Topic 1*

Your company's Microsoft 365 tenant includes Microsoft Exchange Online.
You have been tasked with enabling calendar sharing with a partner organization, who also has a Microsoft 365 tenant.
You have to make sure that users in the partner organization has access to the calendar of every user instantly.
Which of the following actions should you take?

A. Configure a conditional access policy via Exchange admin center.

B. Configure a new organization relationship via Exchange admin center.

C. Configure the sharing settings via Exchange admin center.

D. Run the Set-SPOSite cmdlet.

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship

zul_n Highly Voted 1 year ago
B is correct.

Exchange admin centre | organization | new organization sharing
upvoted 6 times

Balvosko Most Recent 6 months, 1 week ago
B seems correct. When you click under https://admin.exchange.microsoft.com/#/sharing the + sign, it will open a new window that is called "new organization relationship" which is described exactly in the answer B
upvoted 3 times

machinegf 6 months, 3 weeks ago
The answer is C
Exchange admin centre | organization | Sharing and add a the policy with the desired domain. No relationship involved
upvoted 2 times

Oceanide 10 months, 2 weeks ago
Correct answer is B.
upvoted 2 times

JakeH 10 months, 3 weeks ago
B for sure.

Was in exam for me today
upvoted 3 times

Question #3 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
After acquiring a Microsoft 365 Enterprise subscription, you are tasked with migrating your company's Microsoft Exchange Server 2016 mailboxes and groups to
Exchange Online.
You have started a new migration batch. You, subsequently, receive complaints from on-premises Exchange Server users about slow performance. Your analysis shows that the issue has resulted from the migration. You want to make sure that the effect the mailbox migration has on users is decreased.
Solution: You create a label policy.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

Community vote distribution

B (100%)

Tanabs Highly Voted 10 months ago
B. No, you need to change the maximum concurrent migration to decrease the connection to the source server.
upvoted 7 times

waterlego Most Recent 5 months, 2 weeks ago
Still valid, April 2022
upvoted 1 times

Moderator 6 months ago
Selected Answer: B
No, a label policy definitely wouldn't help here.
upvoted 1 times

Oceanide 10 months, 2 weeks ago
No, because you need to modify the migration endpoint settings.
upvoted 2 times

cseg 11 months, 4 weeks ago
No because label policies if anything will slow it down even more since they have to be applied to all emails and documents.
upvoted 4 times

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

After acquiring a Microsoft 365 Enterprise subscription, you are tasked with migrating your company's Microsoft Exchange Server 2016 mailboxes and groups to

Exchange Online.

You have started a new migration batch. You, subsequently, receive complaints from on-premises Exchange Server users about slow performance. Your analysis shows that the issue has resulted from the migration. You want to make sure that the effect the mailbox migration has on users is decreased.

Solution: You create a mail flow rule.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

Community vote distribution

B (100%)

myloking Highly Voted 11 months ago

mail flow rules take action on messages while they're in transit, and not after the message is delivered to the mailbox. To resolve the is modify the migration endpoint settings.

upvoted 10 times

waterlego Most Recent 5 months, 2 weeks ago

Still valid, April 2022

upvoted 1 times

Moderator 6 months ago

Selected Answer: B

A mail flow rule won't be able to help you here.

upvoted 1 times

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

After acquiring a Microsoft 365 Enterprise subscription, you are tasked with migrating your company's Microsoft Exchange Server 2016 mailboxes and groups to

Exchange Online.

You have started a new migration batch. You, subsequently, receive complaints from on-premises Exchange Server users about slow performance. Your analysis shows that the issue has resulted from the migration. You want to make sure that the effect the mailbox migration has on users is decreased.

Solution: You modify the migration endpoint settings.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *A*

Community vote distribution

A (100%)

FumerLaMoquette Highly Voted 1 year, 2 months ago

Set migration endpoint and reduce the concurrent migration value.

https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices#factor-3-migration-engine

upvoted 17 times

Tonio77s 12 months ago

Thanks for the link

upvoted 2 times

waterlego Most Recent 5 months, 2 weeks ago

Still valid, April 2022

upvoted 1 times

Moderator 6 months ago

Selected Answer: A

This is the correct answer indeed.

upvoted 2 times

mikl 8 months, 1 week ago

Yes.

https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices#factor-3-migration-engine-for-non-hybrid-deployment-migrations

Set-MigrationEndPoint <Identity> -MaxConcurrentMigrations <value between 1 and 100>

Customers now can specify migration concurrency (for example, the number of mailboxes to migrate simultaneously) by using Windows PowerShell. The default is 20 mailboxes. After you create a migration batch, you can use the following Windows PowerShell cmdlet to increase this to a maximum of 100.

upvoted 2 times

You need to consider the underlined segment to establish whether it is accurate.
You company has a Microsoft 365 subscription.
To prevent your company from receiving phishing email messages, create a new mail flow rule.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required

B. Label policy.

C. Threat management policy.

D. Spam filter policy.

Correct Answer: *C*
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies

gxsh Highly Voted 1 year ago
C is the right answer.
upvoted 5 times

Tanabs Most Recent 10 months ago
C. You can modify Anti-phishing settings there.
upvoted 3 times

Question #7 *Topic 1*

You work for a company manages all their identities in the cloud.

After acquiring a new domain name, you are tasked with making sure that the primary email address of all new mailboxes uses the new domain.

Which of the following is the Microsoft Exchange Online PowerShell cmdlet that you should run?

A. Update-EmailAddressPolicy

B. Update-OfflineAddressBook

C. Set-AddressBookPolicy

D. Set-EmailAddressPolicy

Correct Answer: *D*

References:

https://docs.microsoft.com/en-us/powershell/module/exchange/email-addresses-and-address-books/set-emailaddresspolicy?view=exchange-ps

JakeH Highly Voted 10 months, 3 weeks ago

In exam today. Answer is correct

upvoted 6 times

Jcbrow27 10 months, 3 weeks ago

¿you cleared?

upvoted 2 times

Cisco Most Recent 3 days, 8 hours ago

In the link supplied it says it applies to both on prem and Exchange Online so appears correct.

upvoted 1 times

Tibo49100 5 months, 4 weeks ago

Wrong answer, command only available for O365 groups

upvoted 1 times

Wojer 9 months, 3 weeks ago

Use the Set-EmailAddressPolicy cmdlet to modify email address policies. In Exchange Online, email address policies are only available f
Microsoft 365 Groups.

upvoted 3 times

Wojer 10 months, 1 week ago

in EOL is available only for groups

upvoted 2 times

marcomartinez 10 months, 3 weeks ago

the D answer is for exchange on prem, I believe the answer for EOL should be to make the domain as the default domain through 365 admin centre

upvoted 1 times

sabin001 10 months, 3 weeks ago

Email address policies define the rules that create email addresses for recipients in your Exchange organization whether this is Exchange on-premise or Exchange online.
You can configure email address policies using the graphical interface of the Exchange Admin Center or by using PowerShell with the Set-EmailAddressPolicy cmdlet.
The Set-EmailAddressPolicy cmdlet is used to modify an email address policy. The Update EmailAddressPolicy cmdlet is used to apply a email address policy to users.

upvoted 3 times

Abdoulaz 11 months, 2 weeks ago

The answer given is correct.
See https://docs.microsoft.com/en-us/powershell/module/exchange/set-emailaddresspolicy?view=exchange-ps#example-3

upvoted 3 times

Tonio77s 12 months ago

Email address policies are only available for Exchange on Premise....

upvoted 2 times

EG_Jack 11 months, 3 weeks ago

No, They are not. The command set-emailaddresspolivy is available on-line too.
https://docs.microsoft.com/en-us/powershell/module/exchange/set-emailaddresspolicy?view=exchange-ps

upvoted 2 times

Eggsamine 11 months, 2 weeks ago

They are available for Exchange Online but only for groups.

upvoted 2 times

zul_n 1 year ago

D is correct

https://docs.microsoft.com/en-us/powershell/module/exchange/set-emailaddresspolicy?view=exchange-ps

his cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings may be exclusive to one environment or the other.

Use the Set-EmailAddressPolicy cmdlet to modify email address policies. In Exchange Online, email address policies are only available f Microsoft 365 Groups.

Set-EmailAddressPolicy
[-EnabledPrimarySMTPAddressTemplate <String>]

upvoted 4 times

Eggsamine 11 months, 2 weeks ago

D can't be correct, as you yourself have said here, "In Exchange Online, email address policies are only available for Microsoft 365 Groups."

upvoted 1 times

MomoLomo 1 year, 1 month ago

This question is totally off

You can't use that command in EXO it's only for group mailbox !!

upvoted 4 times

stoneface 9 months ago

So what would you consider to be the answer to this question then?

upvoted 2 times

MartiFC 1 year, 2 months ago

correct!

upvoted 1 times

Question #8 *Topic 1*

You are responsible for your company's Microsoft 365 subscription.

The company introduces a security policy that requires DLP incident reports to be automatically sent to legal department users.

You are required to configure the reports to be delivered via email as often you can.

Which of the following is the option you should use?

A. Annually

B. Monthly

C. Weekly

D. Quarterly

Correct Answer: *C*

zyir Highly Voted 11 months, 2 weeks ago

C

It can be both Monthly and Weekly but the question says "as often you can" So its Weekly

upvoted 7 times

Shun80 Most Recent 8 months, 4 weeks ago

Where can I send report? I couldn't find the place to send email in Report section of M365 Compliance Center

upvoted 1 times

Jkayx94 9 months ago

C - Options are Monthly/Weekly:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-email-security-reports?view=o365-worldwide#schedu
report

upvoted 3 times

JakeH 10 months, 3 weeks ago

In exam today.

upvoted 4 times

Don123 11 months, 2 weeks ago

why is there no "Custom" in the answer.....

upvoted 1 times

zul_n 1 year ago

C - weekly is correct

upvoted 2 times

Davidchercm 1 year, 1 month ago

repeat question

upvoted 1 times

Question #9 *Topic 1*

You have been tasked with detecting all users in your company's Microsoft 365 subscription who has a Microsoft Office 365 license as a result of belonging to a group.
You need to make sure that the group used to assign the license is included in your results.
Which of the following actions should you take?

A. You should access the Azure portal, and navigate to the Licenses blade.

B. You should access the Microsoft 365 admin center, and navigate to the Products blade.

C. You should access the Azure portal, and navigate to the Monitor blade.

D. You should access the Microsoft 365 admin center, and navigate to the Users blade.

Correct Answer: *A*

Community vote distribution

A (100%)

zul_n Highly Voted 1 year ago
A is correct

Azure AD } Licenses | select he licenses | Licensed group
upvoted 11 times

pozzetttt Most Recent 1 month ago
Selected Answer: A
A. for sure
upvoted 2 times

Mthaher 5 months ago
still confused with A but A is the right answer
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign
upvoted 2 times

RiTh73 7 months, 2 weeks ago
Selected Answer: A
A Correct
upvoted 2 times

mikl 8 months, 1 week ago
Selected Answer: A
A. You should access the Azure portal, and navigate to the Licenses blade.
upvoted 3 times

joergsi 8 months, 1 week ago
The question is, why not users, creation of a dynamic group with all users without a license?
upvoted 1 times

Parzival 8 months, 2 weeks ago
Azure Portal or Azure AD Portal? There's a difference.
upvoted 1 times

Contactfornitish 5 months, 4 weeks ago
There is no Azure AD portal. Azure AD blade is part of Azure portal only with url portal.azure.com
upvoted 1 times

JakeH 10 months, 3 weeks ago
In exam today.
upvoted 2 times

myloking 11 months ago
B would not be correct as the that options displays the products you own within your subcription.

upvoted 1 times

juuvvy 11 months, 2 weeks ago

just need to read the question carefully... asking about licenses. go to license tab.

upvoted 2 times

Contactfornitish 5 months, 4 weeks ago

Not that straight. You can see licenses from individual pages of users as well but here its looking for groups which have a certain license, in that case A only makes sense.

Not a great language in the question though

upvoted 1 times

Question #10 *Topic 1*

You have previously accessed the Security & Compliance admin center to upload a number of archive PST files to Microsoft 365.

When you try to run an import job for the PST files 45 days later, you find that they have been removed from Microsoft 365.

Which of the following is the number of days that Microsoft 365 retains PST file before deleting them automatically?

A. 1 day.

B. 30 days.

C. 15 days.

D. 45 days.

Correct Answer: *B*

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/faqimporting-pst-files-to-office-365

zul_n Highly Voted 1 year ago

B is correct

After Microsoft uploads my PST files to Azure, how long are they kept in Azure before they're deleted?

All PST files in the Azure Storage location for your organization (in blob container named ingestiondata), are deleted 30 days after the most recent import job was created on the Import PST files page in the Microsoft 365 compliance center.

This also means that after PST files are deleted from the Azure Storage area, they're no longer displayed in the list of files for a complet import job in the Microsoft 365 compliance center. Although an import job might still be listed on the Import PST files page in the Microsoft 365 compliance center, the list of PST files might be empty when you view the details of older import jobs.

upvoted 9 times

waterlego Most Recent 5 months, 2 weeks ago

Still valid, April 2022

upvoted 1 times

mikl 8 months, 1 week ago

30 days is correct.

https://docs.microsoft.com/en-us/answers/questions/402268/adjusting-version-retention-for-outlook-data-files.html

upvoted 2 times

Glorence 9 months ago

B is correct

The new policy will limit the number of PST versions retained, resulting in greater storage capacity from PST version storage.
• With this new retention policy, PST file versions will be retained for up to 30 days.

upvoted 2 times

Question #11 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
You have been tasked with deploying a Windows 10 Enterprise image to a large number of Windows 8.1 devices. These devices are joined to an Active Directory domain.
You use the in-place upgrade Windows 10 deployment method for the task.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.
What should you recommend?

A. No adjustment required.

B. Windows Autopilot

C. Windows Update

D. Azure AD Connect

Correct Answer: *A*
References:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure

Community vote distribution
A (100%)

MikeMatt2020 Highly Voted 11 months, 2 weeks ago
I believe the answer is A. I understand the confusion because the question mentions the deployment of an "image". I don't think they mean a concrete imagine that's being deployed by MDT or SCCM. I think they basically mean the installation of Windows 10 Enterprise.

1) There is no mention of devices being imported into the Autopilot service via CSV
2) There is no mention that devices are hybrid AAD joined. This would be relevant if devices were hybrid AAD joined so we could onboa them to Intune and use Autopilot to wipe/image "existing" devices. If our devices existed in Intune, we could create a deployment profi and select the option to "Convert all targeted devices". Though I'm still not 100% sure how we'd perform an upgrade to Windows 10 us this method...
3) An in-place upgrade will do exactly what we want
upvoted 10 times

Moderator Most Recent 5 months, 3 weeks ago
Selected Answer: A
The most logical option is an in-place upgrade, so I'd go for that. A.
upvoted 1 times

trexar 7 months, 2 weeks ago
Windows Autopilot: Applies to

Windows 11
Windows 10
Windows Holographic, version 2004

https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-whats-new
upvoted 1 times

L33D 10 months, 3 weeks ago
Selected Answer: A
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment- toolkit
upvoted 4 times

Jcbrow27 11 months ago
I think the answer is correct because windows update in-place is a valid deployment and requiere a AD DS in the network
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
upvoted 1 times

Marcelmikael 11 months ago

https://www.examtopics.com/exams/microsoft/ms-100/view/10/

Here, the link above, the very identical question(basically the same), the same website but different answers.
upvoted 2 times

saadu93 10 months, 4 weeks ago
that question has "custom" image.. so i think maybe the given answer here is true for here.. and on that page it is true there. both seems correct in their own
upvoted 3 times

Lee75 11 months, 1 week ago
I do not see a "You need to consider the underlined segment to establish whether it is accurate." What am I missing?
upvoted 2 times

tendymadu 11 months, 2 weeks ago
A is correct
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
upvoted 2 times

zul_n 1 year ago
A is correct.

watch this video https://www.microsoft.com/en-us/videoplayer/embed/RE201WL
upvoted 1 times

HappyMudd 1 year ago
The question states you are "deploying a Windows 10 Enterprise *image*..." an in place upgrade does not deploy an image. None of th supplied answers meet that requirment?
upvoted 1 times

rfox321 1 year ago
Why would an in place upgrade not work with the upgrade tool? Please explain why and how it's wrong instead of simply stating "N of these meet the requirement?" - You sound unsure yourself, so why even comment to confuse people?
upvoted 6 times

xofowi5140 11 months, 3 weeks ago
https://docs.microsoft.com/en-us/mem/autopilot/existing-devices
upvoted 2 times

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company currently has an on-premises Active Directory forest.
You have been tasked with assessing the application of Microsoft 365 and the utilization of an authentication strategy.
You have been informed that the authentication strategy should permit sign in via smart card-based certificates, and also permitting the use of SSO to connect to on-premises and Microsoft 365 services.
Solution: You recommend the use of pass-through authentication and seamless SSO with password hash synchronization as the authentication strategy.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

Community vote distribution

B (100%)

Ronger Highly Voted 1 year, 3 months ago
federation, Smart card is the key word.
upvoted 17 times

RiTh73 Most Recent 7 months, 2 weeks ago
Selected Answer: B
Federation with Active Directory federation service is the solution
upvoted 3 times

zul_n 1 year ago
B is correct.

the keyword is smart card
upvoted 4 times

MartiFC 1 year, 2 months ago
We need Federation Services
upvoted 4 times

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company currently has an on-premises Active Directory forest.
You have been tasked with assessing the application of Microsoft 365 and the utilization of an authentication strategy.
You have been informed that the authentication strategy should permit sign in via smart card-based certificates, and also permitting the use of SSO to connect to on-premises and Microsoft 365 services.
Solution: You recommend the use of password hash synchronization and seamless SSO as the authentication strategy.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

zul_n Highly Voted 1 year ago
B is correct.

the keyword is smart card
upvoted 7 times

MartiFC Most Recent 1 year, 2 months ago
we nned Federation Services for Smart Card
upvoted 4 times

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company currently has an on-premises Active Directory forest.
You have been tasked with assessing the application of Microsoft 365 and the utilization of an authentication strategy.
You have been informed that the authentication strategy should permit sign in via smart card-based certificates, and also permitting the use of SSO to connect to on-premises and Microsoft 365 services.
Solution: You recommend the use of federation with Active Directory Federation Services (AD FS) as the authentication strategy.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *A*
References:
https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

Community vote distribution
A (100%)

BobDobolina Highly Voted 1 year ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 6 times

Tonio77s 12 months ago
Thanks for the correct link
upvoted 2 times

RiTh73 Most Recent 7 months, 2 weeks ago
Selected Answer: A
Correct
upvoted 1 times

Davidchercm 1 year, 1 month ago
answer is correct
upvoted 3 times

Your company's Microsoft Azure Active Directory (Azure AD) tenant includes four users. Three of the users are each configured with the Password administrator,
Security administrator, and the User administrator roles respectively. The fourth user has no role configured.
Which of the following are the users that are able to reset the password of the fourth user?

A. The users with the Password administrator and the User administrator roles.

B. The users with the Security administrator and the User administrator roles.

C. The users with the Password administrator and the Security administrator roles.

D. The user with the Password administrator role only.

Correct Answer: *A*
References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

Community vote distribution
A (100%)

zul_n Highly Voted 1 year ago
A is correct

HelpDesk Admins
• Reset password - users only
• Manage service requests
• Monitor service health

User Management Admin
• Reset passwords
• Monitor service health
• Add/delete user accounts - users only
• Manage service reqeusts

Security and Compliance
• Archiving
○ Enable / disable users' archive mailboxes
• DLP
○ Create DLP policies - protect sensitive info
○ Prevent inadvertent disclosure
• Device management
○ Create policies to manage devices
• Permissions
○ Grant explicit permissions as required
• Retention
○ Create retention policies
• Auditing and investigation
○ Alerts and monitoring
○ Audit logs
upvoted 29 times

rfox321 1 year ago
Good information and resources.. Thank you
upvoted 3 times

xofowi5140 11 months, 3 weeks ago
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
upvoted 1 times

trexar Most Recent 6 months ago
Selected Answer: A
A. The user with user administrator and what ever other role in this case password administrator can change password. Be carefull and get confuse Password administrator only Can reset passwords for non-administrators and Password Administrators. User administrator Can manage all aspects of users and groups, including resetting passwords for limited admins.

upvoted 1 times

trexar 6 months ago

Password administrator can not change password of user administrator. Test in my tenant Uadministrator1 : You cannot reset the password for this user because they have admin roles, such as global, billing, Exchange, SharePoint, Compliance, or Skype for Business admin. Only global admins can do that.

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today.

upvoted 1 times

DaBummer 1 year ago

correct!

upvoted 2 times

Question #16 *Topic 1*

Your network contains an Active Directory domain that spans a number of cities and a multitude of users.

After acquiring Microsoft 365, you intend to deploy quite a few Microsoft 365 services.

You want to make sure that pass-through authentication and seamless SSO can be used in your environment. You also decide that Azure AD Connect won't be configured to be in staging mode.

With regards to redundancy limits, which of the following is the maximum amount of servers that can run Azure AD Connect?

A. 1

B. 3

C. 5

D. 7

Correct Answer: *A*

Community vote distribution

A (100%)

MartiFC Highly Voted 1 year, 2 months ago

One active mode. A lot of in stagin mode

upvoted 14 times

emilianogalati 1 year, 1 month ago

Correct!

upvoted 4 times

trexar Most Recent 6 months ago

Selected Answer: A

correct

upvoted 2 times

Tonio77s 12 months ago

Correct. Reference is here https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies

upvoted 2 times

Question #17 *Topic 1*

Your network contains an Active Directory domain that spans a number of cities and a multitude of users.
After acquiring Microsoft 365, you intend to deploy quite a few Microsoft 365 services.
You want to make sure that pass-through authentication and seamless SSO can be used in your environment. You also decide that Azure AD Connect won't be configured to be in staging mode.
With regards to redundancy limits, which of the following is the most amount of servers that can run standalone Authentication Agents?

A. 7

B. 9

C. 11

D. 13

Correct Answer: *C*

Community vote distribution

D (100%)

fofo1960 Highly Voted 12 months ago
As to this https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start
we recommend that you have a minimum of 3 Authentication Agents running on your tenant. There is a system limit of 40 Authenticat
Agents per tenant.
So its 40
upvoted 17 times

Turd_Reynolds Highly Voted 1 year, 3 months ago
I thought the maximum number of Agents was 40?
upvoted 12 times

Rickert 1 year, 3 months ago
Yes! Minimum of 3 and a maximun of 40
upvoted 8 times

Turd_Reynolds 1 year, 3 months ago
So then this answer should be 13 (D) shouldn't it?
upvoted 14 times

RiTh73 Most Recent 7 months, 2 weeks ago
Selected Answer: D
Recommended server is 3 and the maximum is 40
upvoted 1 times

sliix 8 months ago
Selected Answer: D
Highest possible is 40.
upvoted 1 times

Musa007 8 months ago
Selected Answer: D
The actually highest number is 40 but in this question 13 is the highest so I'll go with it
upvoted 1 times

mfaisal786 8 months ago
it is stated in question that most which is number 13 in the given choices, however max limit is 40
upvoted 1 times

FabianSchmidt 8 months ago
Selected Answer: D
Answer is D
upvoted 1 times

Pr9 8 months, 1 week ago

Selected Answer: D

Max limit 40
Min is 3

upvoted 2 times

Zethembiso 8 months, 2 weeks ago

Selected Answer: D

The most number is 13 as you can run up the maximum of 40

upvoted 2 times

Bulldozzer 9 months ago

Correct it's 40.

upvoted 2 times

Wojer 10 months, 1 week ago

D is the proper answer

upvoted 2 times

L33D 10 months, 3 weeks ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

Important

In production environments, we recommend that you have a minimum of 3 Authentication Agents running on your tenant. There is a system limit of 40 Authentication Agents per tenant. And as best practice, treat all servers running Authentication Agents as Tier 0 syst (see reference).

upvoted 2 times

Don123 11 months, 2 weeks ago

I hope the moderator is reading the comments and updating the answers

upvoted 4 times

Fcnet 1 year, 2 months ago

D is the right answer (more than 13)

upvoted 3 times

fofo1960 12 months ago

But the question state 'most amount' which mean the max number

upvoted 1 times

Joshycannon 9 months, 3 weeks ago

So, in this case we can just select the most provided since the question is asking what is the most... Don't read so deep into the question, just pick the best answer...

upvoted 1 times

densyo 1 year, 2 months ago

In production environments, we recommend that you have a minimum of 3 Authentication Agents running on your tenant. There is a system limit of 40 Authentication Agents per tenant.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

upvoted 3 times

Question #18 *Topic 1*

Your company's Microsoft Azure Active Directory (Azure AD) tenant includes four users that are configured with the Privileged role administrator, the User administrator, the Security administrator, and the Billing administrator roles respectively.
A security group has been included in the tenant for the purpose of managing administrative accounts.
Which of the four roles can be used to create a guest user account?

A. The Privileged role administrator role.

B. The User administrator role.

C. The Security administrator role.

D. The Billing administrator role.

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

Community vote distribution
B (100%)

MartiFC Highly Voted 1 year, 1 month ago
Is correct! Only Guest inviter and User administrator can create guest user >> https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task
upvoted 7 times

Olamilekinsin 9 months, 1 week ago
Thank you for the link
upvoted 1 times

MartiFC Highly Voted 1 year, 1 month ago
The ask say CREATE. Not say INVITE. This is the keywork
upvoted 6 times

zyir 11 months, 3 weeks ago
You will need to invite before a guest can be created right?
upvoted 2 times

rfox321 1 year ago
1000% correct my dude
upvoted 1 times

mllerena Most Recent 2 days, 6 hours ago
B
https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settin in-the-portal

Solo los usuarios asignados a funciones de administrador específicas pueden invitar a usuarios invitados : para permitir que solo los usuarios con funciones de administrador inviten a personas, seleccione este botón de opción.

Los roles de administrador incluyen Administrador global, Administrador de usuarios e Invitador invitado .
upvoted 1 times

cdatexwintel 8 months, 1 week ago
Selected Answer: B
Is correct
upvoted 1 times

xyzfra 9 months, 4 weeks ago
I passed the exam last week with 822 and these guest related questions are still not clear to me. I perfectly know how guests work. By default, every user can INVITE guests. This action (INVITE) causes the creation of a guest user on your tenant, BUT, you can also go unc Azure AD admin, and CREATE a guest user. So, INVITE and CREATE are different operations. Who knows what Microsoft is asking for in t kind of questions....

upvoted 1 times

tf444 9 months, 3 weeks ago

Wow, the end result is the same , guest user in the tenant.
Invite or create.

upvoted 1 times

Grudo 8 months, 1 week ago

It's not difficult to understand. By default, all users can invite B2B collaboration users, this is correct. Alternatively, administrators ca
also "create" user accounts in the home directory for which the tenant is authoritative (i.e., using your own vanity or custom domain
So yes, they are two distinctly separate operations.

upvoted 1 times

Grudo 8 months, 1 week ago

That should say that administrators can "create" GUEST user accounts in the home directory. That is, user objects with the "Guest
user type attribute.

upvoted 1 times

YClaveria 12 months ago

If you go to https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference, there is an action and description column for each admin role.

The action "microsoft.directory/users/inviteGuest" is included only under Directory Writers, Guest Inviter, and User Admin. It is not included under Billing, Privileged role, and security admin.

upvoted 4 times

zul_n 1 year ago

B is correct

User Management Admin
• Reset passwords
• Monitor service health
• Add/delete user accounts - users only
• Manage service reqeusts

upvoted 6 times

TEEEEEEEEEE 1 year, 1 month ago

Question is "Which of the four roles can be used to create a guest user account?". Roles not Users.
Of the four roles, only the User Administrator can invite guests.

upvoted 1 times

Madball 1 year, 1 month ago

All accounts can invite, however, if it's only asking for one, then I would go with the user administrator on this question, because they n
have changed the default settings.

upvoted 1 times

Davidchercm 1 year, 1 month ago

is the answer correct ?

upvoted 1 times

dminerva94 1 year, 1 month ago

No, all accounts can invite guests

upvoted 1 times

Question #19 *Topic 1*

Your company's Microsoft Azure Active Directory (Azure AD) tenant includes four users that are configured with the Privileged role administrator, the User administrator, the Security administrator, and the Billing administrator roles respectively.
A security group has been included in the tenant for the purpose of managing administrative accounts.
Which of the four roles can be used to add a user with the Security administrator role to the security group?

A. The Privileged role administrator role.

B. The User administrator role.

C. The Security administrator role.

D. The Billing administrator role.

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

Community vote distribution
B (80%) A (20%)

zul_n Highly Voted 1 year ago
I'd say B is correct

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator

User Administrator

Users with this role can create users, and manage all aspects of users with some restrictions (see the table), and can update password expiration policies. Additionally, users with this role can create and manage all groups.
upvoted 8 times

rfox321 1 year ago
This is correct. Read the doc people
upvoted 5 times

mfaisal786 Highly Voted 8 months ago
The "User Administrator Role" is right , when I try to add user using Privileged Administrator I got this "You do not have appropriate permissions to edit this group. You should be a global administrator or user management administrator to manage this group."
upvoted 5 times

mllerena Most Recent 3 days, 4 hours ago
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-are-role-assignable-groups-protected
By default, only Global Administrators and Privileged Role Administrators can manage the membership of a role-assignable group, but you can delegate the management of role-assignable groups by adding group owners.
upvoted 1 times

Sector12 1 month ago
Selected Answer: A
The answer is A (tried and tested). The reason for this is logical, if you make any group role assignable, this could lead to privilege escalation.

Role-assignable groups are designed to help prevent potential breaches by having the following restrictions:

Only Global Administrators and Privileged Role Administrators can create a role-assignable group.
The membership type for role-assignable groups must be Assigned and can't be an Azure AD dynamic group. Automated population o dynamic groups could lead to an unwanted account being added to the group and thus assigned to the role.

https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept
upvoted 1 times

Sector12 1 month ago
Forgot one more point as per documentation: By default, only Global Administrators and Privileged Role Administrators can manag the membership of a role-assignable group, but you can delegate the management of role-assignable groups by adding group own

upvoted 1 times

cluocal 5 months, 2 weeks ago

Selected Answer: B

B is correct.

upvoted 2 times

sandi412 6 months, 1 week ago

Tested.B is correct

upvoted 2 times

dudus999 6 months, 3 weeks ago

Assign group to role require special group.
To that group you can assing member with user administrator role, you need to Global Admin or Priviliged role administrator

upvoted 2 times

dudus999 6 months, 3 weeks ago

*To that group you can't assing member with user administrator

upvoted 1 times

RazielLycas 7 months, 1 week ago

Both of them are correct if you read the role description

"Privileged Role Administrator:
Users with this role can manage role assignments in Azure Active Directory, as well as within Azure AD Privileged Identity Management. They can create and manage groups that can be assigned to Azure AD roles. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units."

"User Administrator:
Users with this role can create users, and manage all aspects of users with some restrictions (see the table), and can update password expiration policies. Additionally, users with this role can create and manage all groups. This role also includes the ability to create and manage user views, manage support tickets, and monitor service health. User Administrators don't have permission to manage some user properties for users in most administrator roles. Admins with this role do not have permissions to manage MFA or manage shared mailboxes. The roles that are exceptions to this restriction are listed in the following table."

upvoted 1 times

Networker97 7 months, 3 weeks ago

Selected Answer: B

B - someone voted incorrectly

upvoted 2 times

cdatexwintel 8 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

Pr9 8 months, 1 week ago

Selected Answer: B

Answer is correct.. B

upvoted 2 times

Musa007 8 months, 2 weeks ago

Selected Answer: A

B is correct

upvoted 1 times

AlexLiourtas 8 months, 1 week ago

selected answer: a
b is correct

what?

upvoted 4 times

KSvh53 6 months, 2 weeks ago

Someone please remove this vote. This is completely unhelpful.

upvoted 1 times

stromnessian 1 year, 2 months ago

Complete **** of a question but that's not unusual in these exams! The answer is...
...it depends if the group is role assignable. If so, the Privileged Role Administrator can; if not, the User Administrator can.
To be fair, this question may have been written before role assignable groups were a thing.
upvoted 3 times

WoVic 1 year, 2 months ago
IMHO this is A

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Privileged Role Administrator
Can manage role assignments in Azure AD, and all aspects of Privileged Identity Management.

User Administrator
Can manage all aspects of users and groups, including resetting passwords for limited admins.
upvoted 4 times

KornienkoBoris 1 year, 1 month ago
there is nothing about role assignment in the question, only about security group, so it's a users administrator
upvoted 5 times

sabin001 10 months, 3 weeks ago
you are going to add user in a security group not to assign a role
upvoted 4 times

Your company has an Active Directory domain as well as a Microsoft Azure Active Directory (Azure AD) tenant.
After configuring directory synchronization for all users in the organization, you configure a number of new user accounts to be created automatically.
You want to run a command to make sure that the new user accounts synchronize to Azure AD in the shortest time required.
Which of the following is the command that you should use?

A. New-ADSyncRule

B. Set-ADSyncSchedulerConnectorOverride

C. Start-ADSyncSyncCycle

D. Set-ADSyncSchema

Correct Answer: *C*
References:
https://blogs.technet.microsoft.com/rmilne/2014/10/01/how-to-run-manual-dirsync-azure-active-directory-sync-updates/

Davidchercm Highly Voted 1 year, 1 month ago
Run the Start-ADSyncSyncCycle command
For delta synchronization use the parameter -PolicyType Delta (used in most situations)
For full synchronization use the parameter -PolicyType Initial (rarely used)
upvoted 12 times

zul_n 1 year ago
agreed, C is correct
upvoted 4 times

k9_bern_001 Most Recent 6 months, 2 weeks ago
Correct
upvoted 2 times

joergsi 8 months, 1 week ago
To sync only the newly created users:
Start-ADSyncSyncCycle -PolicyType Delta
upvoted 2 times

Question #21 *Topic 1*

Your company's Microsoft Azure Active Directory (Azure AD) tenant includes four users. Two of the users are configured with the Global administrator, Password administrator roles respectively. A third user has both the Security administrator and the Guest inviter roles configured. The fourth user has no roles configured.
Which of the following is the user that has the necessary permissions to alter the password protection policy? (Choose all that apply.)

A. The user with the Global administrator role.

B. The user with the Password administrator role.

C. The user with the Security administrator and Guest inviter roles.

D. The user with no roles.

Correct Answer: *A*

Community vote distribution

A (100%)

stromnessian Highly Voted 1 year, 2 months ago
The supplied answer is wrong. Both the global administrator and security administrator can change the password protection policy.
upvoted 10 times

rfox321 1 year ago
Stop providing input without proof or links please.
upvoted 5 times

michszym 1 year, 2 months ago
It's not true. Answer is correct.
See this link: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protectio
Prerequisites: An account with global administrator privileges.
upvoted 13 times

MomoLomo 1 year, 1 month ago
@Mich
Wrong link
https://docs.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide
upvoted 6 times

Eggsamine 11 months, 2 weeks ago
The link that Mich provided is the correct one as it is about password protection whereas yours is about password expiry. Nevertheless, both documents state that global admin is a requirement.
upvoted 3 times

Jcbrow27 11 months ago
in both cases you must be a global admin.
upvoted 1 times

vofka Highly Voted 10 months ago
A - Global admin
C - Security Admin can create password protection
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

Many are confused by the combined role of Guest Inviter. Inviter cannot manage password protection, but as the role is combined - us
has the ability to manage password protection.
upvoted 6 times

Mthaher Most Recent 5 months ago
any user can send the invite if the external collaboration option is enabled
upvoted 1 times

trexar 6 months ago
Selected Answer: A
A & C correct. Tested in my tenant, Global administrator and the 3er user (with this 2 roles)can modify Password protection policy.

upvoted 3 times

k9_bern_001 6 months, 2 weeks ago

Both global admin and security admin can modify password protection policy, but since in the answer there is no combo for both globa admin and sec admin, the correct answer is A.

upvoted 2 times

salla 7 months ago

Selected Answer: A

A and C. Checked. Security Administrator: Configure custom banned password list or on-premises password protection.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

upvoted 3 times

mfaisal786 8 months ago

A is correct because Password Admin can't modify/edit any kind of policies...

upvoted 2 times

Wojer 9 months ago

Checked in my azure portal and its A and C

upvoted 1 times

PDR 9 months, 2 weeks ago

answer is definately A (obviously) AND C - as others have said, regardless of what the docs say Security Administator CAN makes chang to password protection policy and save them. I just tested this and can confirm. The question states 'Choose all that apply' so it would both

upvoted 3 times

tf444 9 months, 3 weeks ago

Both the global administrator and security administrator can change the password protection policy, however, answer C states Security Administrator and Guest inviter role
A is the correct answer.

upvoted 5 times

AlexLiourtas 10 months, 1 week ago

A-C for sure

upvoted 2 times

Stiobhan 10 months, 1 week ago

Answer is A&C, assuming C is talking about 1 person with both roles - https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

upvoted 2 times

MikeMatt2020 11 months, 2 weeks ago

I understand that from some of the documentation that a few of you supplied, that it states you must have Global admin permissions. However, I'm a Security Admin in my tenant and I'm able to access Password Protection without issue.

For clarification, C is NOT saying that Security Administrator and Guest Inviter grants access to Password Protection. It's saying "Can th user who has Sec Admin and Guest Inviter access Password Protection. I would say YES. It doesn't matter that Guest Inviter doesn't gra access to Password Protection. This is granted from he/she being a Security admin.

I'm going with A and C. If you reference the Security Admin individual permissions, it clearly lists "Password Protection"

upvoted 3 times

BenimAdim 12 months ago

can Guest Inviter do that, No. So C is not correct.
Correct one is A Global Admins

upvoted 2 times

zul_n 1 year ago

interesting one...

I'd say
A - global admins is God mode...
and
C - https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

but for the sake of this question, I'll choose A

upvoted 2 times

gonick 1 year ago

@momolomo, that's the wrong link also. Question is asking about the password protection policy from AAD > Security > Auth methods > Password protection. Both global admin and sec admins have permissions here. Tried it now.

upvoted 4 times

Question #22 *Topic 1*

Your company's Microsoft Azure Active Directory (Azure AD) tenant includes four users. Two of the users are configured with the Global administrator, Password administrator roles respectively. A third user has both the Security administrator and the Guest inviter roles configured. The fourth user has no roles configured.
Which of the following is the user that has the necessary permissions to create guest users? (Choose all that apply.)

A. The user with the Global administrator role.

B. The user with the Password administrator role.

C. The user with the Security administrator and Guest inviter roles.

D. The user with no roles.

Correct Answer: *AC*

Community vote distribution



MEG Highly Voted 8 months, 4 weeks ago

Selected Answer: AC

I think A and C is correct. See here: https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#users [Create gues user]

upvoted 6 times

yawb 2 weeks, 4 days ago

Also this: https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal#prerequisites

upvoted 1 times

examjustin Highly Voted 5 months, 1 week ago

Selected Answer: A

Answer is only A. Guest inviter's can only invite guest users, not create. I just tested this in my tenant. Create user is grayed out, invite u is enabled. Answer is only A folks.

upvoted 6 times

mllerena Most Recent 3 days, 2 hours ago

AC
https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#users
Tarea Rol menos privilegiado Funciones adicionales
Crear usuario invitado Invitador invitado Administrador de usuarios

upvoted 1 times

F1B3R 1 week, 1 day ago

Selected Answer: A

My understanding is that it is only A
Inviting a guest that does not have an account, gets one made for them. But you cannot directly use the "Create Guest account" buttor a Guest inviter.
Pretty sure this is a Microsoft certified trick question

upvoted 2 times

cjwebster93 5 months, 3 weeks ago

Selected Answer: A

A guest inviter CAN, but the Security Administrator CANNOT, so C is wrong.

upvoted 2 times

biglittle323 5 months, 1 week ago

It is one user with both roles, not two separate users...

upvoted 1 times

trexar 6 months ago

Selected Answer: AC

Correct tested

upvoted 1 times

sandi412 6 months, 1 week ago

Selected Answer: A

Tested in lab

upvoted 3 times

Legitness 6 months, 1 week ago

Only A is correct - See the table her- https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#guest-invite

upvoted 1 times

denmaillbox 7 months ago

Selected Answer: AC

Inviting guests from aad is creating guest user. Checked

upvoted 2 times

Silverfire 2 weeks, 2 days ago

Sec admin can't access Azure Active Directory Administration... So no, C is wrong.

upvoted 1 times

rockey90 7 months, 1 week ago

for the people who voted for C , please be sure before you vote , you confuse another people with these answers .
i assigned these rules to a different users and only the global admin who could create a guest user

upvoted 2 times

mfaisal786 8 months ago

Only A is correct because Guest Inviter can't create guest user.

upvoted 2 times

FabianSchmidt 8 months ago

Selected Answer: A

Only A. Create Guest and Invite Guest is not the same action. Only Global Admin and User Admin can create Users.

upvoted 3 times

Musa007 8 months, 2 weeks ago

Selected Answer: AC

Definitely A and C

upvoted 2 times

rockey90 7 months, 1 week ago

no , C is wrong

upvoted 1 times

Bulldozzer 9 months ago

Correct answer it A and C.

upvoted 3 times

rockey90 7 months, 1 week ago

just A

upvoted 1 times

fofo1960 9 months, 2 weeks ago

I tried it, and the Guest invitor rule can
open AAD --> User --> Invite guest
I think the create or invite guest are the same
But still the global admin can fill more field such as Account is blocked, first name, last name...
So in general, Guest Invitor rule can invite
Correct me if I was wrog

upvoted 3 times

rockey90 7 months, 1 week ago

in AAD portal when you go to USERS and choose +NewGuestUser , it will ask you either create or invite .
not the same

upvoted 1 times

alex_p 5 months, 3 weeks ago

But did you noticed if you choose the CREATE option - what will you create!? You will not create a Guest user

upvoted 1 times

Shadow983 9 months, 1 week ago

I think that CREATE and INVITE guest are the same too, because there are no any option called "create guest user".
In default, any user in AAD can invite guest user, even they don't have any AAD roles.
This question need to choose all the users who have the necessary permission to create guest user, so I will choose A, B, C, D

upvoted 3 times

Frede 6 months ago

I agree!

upvoted 1 times

Berender 7 months ago

Invite and create guest user do seem the same. When Guest inviter invites someone and this person accepts the invitation, a guest account is created in AAD.

upvoted 1 times

vofka 10 months ago

Only A: Global Admin
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#guest-inviter
Guest Invite role cannot create guest users. He can only invite. Create and invite are different actions.
SecAdm role cannot create any users.

upvoted 3 times

Stiobhan 10 months, 1 week ago

Answers are A&C - Global admin is full rights anyway but guest inviter can also create guest user as the creation of a guest user is ti inv
them (hope that made sense!) https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-us
portal

upvoted 1 times

You have been tasked with enable Microsoft Azure Information Protection for your company's Microsoft 365 subscription.
You are informed that only the members of a group, named Group1, are able to protect content. To achieve your goal, you plan to run a PowerShell cmdlet.
Which of the following is the cmdlet you should run?

A. The Add-AadrmRoleBaseAdministrator cmdlet.

B. The Set-AadrmDoNotTrackUserGroup cmdlet.

C. The Clear-AadrmSuperUserGroup cmdlet.

D. The Set-AadrmOnboardingControlPolicy cmdlet.

Correct Answer: *D*
If you don't want all users to be able to protect documents and emails immediately by using Azure Rights Management, you can configure user onboarding controls by using the Set-AadrmOnboardingControlPolicy
References:
https://docs.microsoft.com/en-us/azure/information-protection/activate-service

MallonoX Highly Voted 10 months, 2 weeks ago
It's Set-AipServiceOnboardingControlPolicy now
upvoted 26 times

gdunlop Most Recent 1 month ago
Unlikely to see on exam - This cmdlet from the AADRM module is now deprecated. After July 15, 2020, this cmdlet name will be support only as an alias to its replacement in the AIPService module.
https://docs.microsoft.com/en-us/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps
upvoted 2 times

Mthaher 5 months ago
- Set-AipServiceOnboardingControlPolicy
https://docs.microsoft.com/en-us/azure/information-protection/activate-service#configuring-onboarding-controls-for-a-phased-deployment
upvoted 1 times

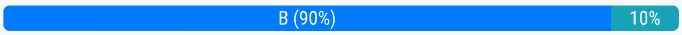
Your company has acquired Microsoft 365 for their Active Directory domain, which includes five domain controllers.
Prior to implementing a number of Microsoft 365 services, you are tasked with making use of an authentication solution that allows users to access Microsoft 365 by using their on-premises credentials. The solution should also only make use of the current server infrastructure. Furthermore, must allow for all user passwords to only be stored on-premises, and be highly available.
Solution: You configure the use of password hash synchronization only.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

Community vote distribution



MartiFC Highly Voted 1 year, 1 month ago
Correct! Password hash synchronization store password on Azure Active Directory
upvoted 8 times

lafcow 1 year ago
Is the question asking if the password hashes are stored in Azure or the passwords ? Does it change the answer ?
upvoted 1 times

BenimAdim 12 months ago
Passwords are never stored in Cloud, just hashes are. Security ;).
upvoted 2 times

dumpmaster 10 months, 1 week ago
Yes, but the point is use the on-premises environment, for me it is B.
upvoted 1 times

rfox321 1 year ago
Correct - question clearly states “Must be stored on-premise”
upvoted 4 times

zul_n Highly Voted 1 year ago
I'd say B is correct

Conditions :
1) must allow for all user passwords to only be stored on-premises,
2) be highly available.

Solution: You configure the use of password hash synchronization only.

only condition 1 is applied, not condition 2.
upvoted 6 times

azexiroyal Most Recent 2 weeks, 4 days ago
answer is NO means B.
upvoted 2 times

trexar 6 months ago
Selected Answer: B
the password is onpremise and the password hash is on the cloud.
upvoted 2 times

joergsi 8 months ago
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy

High availability considerations
The main concern for password protection is the availability of Azure AD Password Protection proxy servers when the DCs in a forest tr

download new policies or other data from Azure. Each Azure AD Password Protection DC agent uses a simple round-robin-style algorith when deciding which proxy server to call. The agent skips proxy servers that aren't responding.

=> Without Azure AD Password Protection proxy servers no HA!

upvoted 1 times

joergsi 8 months, 1 week ago

The answer should be no, the requirements are:
- passwords are not stored in the cloud, only on-prem

This can only be achieved with path-through:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

upvoted 2 times

Joseh23 7 months, 2 weeks ago

The question also states "The solution should also only make use of the current server infrastructure". Path-through runs on one or more on-premises servers

upvoted 1 times

VictorPCS 8 months, 2 weeks ago

Selected Answer: B

Stored ONLY on premises, so there shouldn't be any password syncronisation with AAD

upvoted 2 times

tf444 9 months, 2 weeks ago

the answer is PTA , not PHS.

upvoted 2 times

natazar 9 months, 2 weeks ago

Selected Answer: B

"Furthermore, must allow for all user passwords to only be stored on-premises, and be highly available."
PHS uses on-premises password and store them HASHED in CLOUD.
So the answer is B.

upvoted 3 times

Stiobhan 10 months, 1 week ago

Selected Answer: B

Answer is B as even though no passwords are stored on the cloud, hashes of the passwords are and if hacked could be used in a rainbo table to get the decrypted password. The only solution to this question would be to use pass-through authentication or federated servi

upvoted 2 times

Cazaciuc 10 months, 2 weeks ago

Selected Answer: A

Password hash does NOT store the password in M356

upvoted 1 times

fofo1960 12 months ago

The question says "user passwords to only be stored on-premises", the Password Hash will keep a copy of the password hash in Micros cloud, so another copy of the password are stored in the cloud.

upvoted 2 times

fofo1960 12 months ago

So the Answer is B

upvoted 3 times

tf444 9 months, 4 weeks ago

No, it does not!

upvoted 2 times

zacmzee 1 year ago

These answers don't make any sense. It is 'A' for me.

upvoted 2 times

gxsh 1 year ago

Answer A should be correct.

upvoted 1 times

gxsh 1 year ago

PHS stores hashes of passwords, not passwords.

upvoted 2 times

Question #25 *Topic 1*

Your company has acquired Microsoft 365 for their Active Directory domain, which includes five domain controllers.
Prior to implementing a number of Microsoft 365 services, you are tasked with making use of an authentication solution that allows users to access Microsoft 365 by using their on-premises credentials. The solution should also only make use of the current server infrastructure.
Furthermore, must allow for all user passwords to only be stored on-premises, and be highly available.
Solution: You configure the use of pass-through authentication only.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

Community vote distribution

A (83%) B (17%)

Stiobhan Highly Voted 10 months, 1 week ago

Selected Answer: A

100% A. No need for links, do your own research and figure it out. PTA is the only solution here!!!

upvoted 9 times

Durden871 7 months, 2 weeks ago

It mentions that you are configuring the use of PTA, which you would do through Directory Sync. It just says you do this, "only". You need to install two more authentication agents which I don't see anywhere else in this question. The question is asking, how do you this and provide HA. The solution specifically says, "only enable PTA".

I said A, but I think now it's B.

upvoted 1 times

fofo1960 Highly Voted 12 months ago

I think its A, HA is also can be done by installing multiple PTA, in my org, I have three.

upvoted 6 times

bake73 9 months ago

The question is not if it's feasible. Yes HA is possible but in the question it is not stated if you install agents, only PTA. So HA not met. Never assume more than the question in Microsoft exams.

upvoted 1 times

bake73 9 months ago

Edit; and the minimum agent for PTA is 1 sooo.... no HA

upvoted 1 times

gdunlop Most Recent 1 month ago

This is just a bad question - PTA should be the answer, but the question is too vague

upvoted 1 times

Mea988 7 months, 3 weeks ago

Selected Answer: A

Can become HA by installing agents. You have five DCs, so no worries. PTA is fine

upvoted 1 times

joergsi 8 months ago

Selected Answer: B

B
=> Without Azure AD Password Protection proxy servers no HA!

upvoted 2 times

alex_p 7 months ago

So, you say that without Password Protection proxy agents installed - the passwords on five DCs on prem are not higly available!? :)

upvoted 1 times

joergsi 8 months, 1 week ago

The answer should be YES, the requirements are:
- passwords are not stored in the cloud, only on-prem

This can only be achieved with path-through:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

upvoted 1 times

joergsi 8 months ago

Changed my mind, it's B:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy

High availability considerations
The main concern for password protection is the availability of Azure AD Password Protection proxy servers when the DCs in a fores
to download new policies or other data from Azure. Each Azure AD Password Protection DC agent uses a simple round-robin-style
algorithm when deciding which proxy server to call. The agent skips proxy servers that aren't responding.

=> Without Azure AD Password Protection proxy servers no HA!

upvoted 1 times

jill44 9 months ago

You configure the use of pass-through authentication only?
Needs SSO!
B is correct.

upvoted 1 times

Davidchercm 9 months ago

i would choose no as no sso

upvoted 1 times

bake73 9 months ago

B it is.
HA requirement not met.
Never assume more than what is in the question for Microsoft exams.

upvoted 1 times

tschlappinger 9 months, 2 weeks ago

In my opinion B is the correct answer. If the answer where "PTA with SSO" than it would be A but there is no "SSO".

upvoted 1 times

vnet1 10 months, 1 week ago

A: Additional agents can be installed on multiple on-premises servers to provide high availability of sign-in requests.

upvoted 2 times

vnet1 10 months, 1 week ago

Correction B - Additional agents can be installed on multiple on-premises servers to provide high availability of sign-in requests.

upvoted 1 times

Jcbrow27 10 months, 2 weeks ago

how PTA is highly available ?

upvoted 1 times

gxsh 1 year ago

PTA is not highly available, so second criteria not met.

upvoted 4 times

rfox321 1 year ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta - CLEARLY STATES is highly available..

upvoted 6 times

bake73 9 months ago

Learn to read;
Highly available
Additional agents can be installed on multiple on-premises servers to provide high availability of sign-in requests.
Question NEVER states if you install additional agents and the minimum is 1.

upvoted 2 times

zul_n 1 year ago

I think B is correct.

'PTA only' met the first condition. if the answer said PTA with multiple authentication agents, then it will meet 2nd condition.

upvoted 4 times

rfox321 1 year ago
Jesus people.. where is your links and proof??
upvoted 2 times

YClaveria 12 months ago
same link under "Feature highlights"
upvoted 1 times

Aurenx 1 year, 2 months ago
I think this should be A
PTA stored only On-Prem, is highly available, and does not require extra servers.

See: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta
upvoted 3 times

Aps123 1 year ago
Answer A
upvoted 1 times

miul84 1 year, 3 months ago
Goals met: passwords are only stored on-premise
Goals not met: ??? (maybe not HA? I mean you could install authentications agents on each DC)
upvoted 1 times

Bobalo 1 year, 2 months ago
Solution requires users to use on prem credentials to access Microsoft 365 resources, so SSO is needed.
upvoted 3 times

mfaisal786 8 months ago
both SSO and PTA meet this criteria but SSO doesn't meet H.A ,
upvoted 1 times

Aps123 1 year ago
SSO is optional, so Answer would be A
upvoted 1 times

Question #26 *Topic 1*

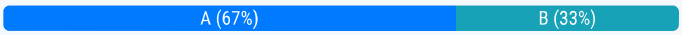
Your company has acquired Microsoft 365 for their Active Directory domain, which includes five domain controllers.
Prior to implementing a number of Microsoft 365 services, you are tasked with making use of an authentication solution that allows users to access Microsoft 365 by using their on-premises credentials. The solution should also only make use of the current server infrastructure.
Furthermore, must allow for all user passwords to only be stored on-premises, and be highly available.
Solution: You configure the use of pass-through authentication and seamless SSO.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *A*

Community vote distribution



TimurKazan Highly Voted 1 year ago
correct, PTA is also considered as highly available by Microsoft
upvoted 6 times

bake73 9 months ago
No no and no.
PTA is considered HA IF you have more than 1 agent. The minimum for PTA is 1, thus no redundancy IF only 1 agent.
upvoted 2 times

Mea988 7 months, 3 weeks ago
But it's not stated you can only install one, only that you have to use the existing infrastructure and have HA. So it's ok, PTA is HA this case
upvoted 3 times

MikeMatt2020 Highly Voted 11 months, 2 weeks ago
I don't really see how Seamless SSO has anything to do with what the question is asking. It's asking that we choose and authentication method that has high availability, which PTA offers (especially with the scalability of its PTA agents) and passwords are stored on-prem, which PTA also does. Question does not mention any parameter that requires users be automatically signed in while on-prem without cred prompts...Am I wrong?
upvoted 5 times

Contactfornitish Most Recent 5 months, 3 weeks ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

Seamless SSO can be combined with PTA and PTA only fills the requirement of keeping passwords On-Premise. Adding Seamless doesn change a thing so A is right
upvoted 3 times

trexar 6 months ago
Selected Answer: A
Password are onpremise first requirement is ok, HA the sentence say you configure it means you install the agents
upvoted 1 times

joergsi 8 months ago
Selected Answer: B
Following the argument of the previous question, to achieve HA we need PTA +, at least, three Agents.
What we get is PTA and Seamless, in this case the answer could only be NO!
upvoted 2 times

Durden871 7 months, 2 weeks ago
The previous question said enabling the feature of PTA only. This is talking of configuring PTA with SSO, but doesn't use the delimite "Only". These questions are awful. Even with these study aides I'm incredibly confused.
upvoted 1 times

Bulldozzer 9 months ago

In my opinion, the answer of the previous question is A and for this one, it' B.

upvoted 1 times

tf444 9 months, 4 weeks ago

So what is the difference between this Q and the previous one?
SSO has anything to do with what the question is asking, why this q is yes and the other one is No?

upvoted 3 times

Eggsamine 11 months, 2 weeks ago

Once Seamless SSO has been enabled by Azure AD connect is AD connect required for Seamless SSO to work? Enabling it creates a computer account, AZUREADSSOACC, in your on-prem AD that allows the authentication to proceed.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-how-it-works
I think that so long as there are enough authentication agents for PTA then the solution is HA.

upvoted 1 times

feekah 11 months, 3 weeks ago

SSO is a feature that can be enabled or disabled on Azure AD connect, so it's not by default

upvoted 1 times

fofo1960 12 months ago

Wait, correct me if I am wrong, SSO is part of ADConnect, not the PTA, so I think its B

upvoted 3 times

zul_n 1 year ago

I'd say B.

PTA met the first criteria, but SSO won't meet the second crteria.

upvoted 2 times

rfox321 12 months ago

Weird logic. Just because it's configured in addition to outside of the scope, wouldn't necessarily make it incorrect right? However, it not stated in the request.. interesting...

upvoted 2 times

Question #27 *Topic 1*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant with multi-factor authentication enabled.

You have also configured the Allow users to submit fraud alerts, and the Block user when fraud is reported settings to ON.

A tenant user has submitted a fraud alert for his account.

Which of the following is the length of time that the user's account will automatically be blocked for?

A. 24 hours

B. 90 days

C. 1 month

D. 1 week

Correct Answer: *B*

References:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert

hussain2000 5 months, 1 week ago

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert

upvoted 1 times

Your company has a Microsoft Azure Active Directory (Azure AD) tenant with multi-factor authentication enabled.

You have also configured the Allow users to submit fraud alerts, and the Block user when fraud is reported settings to ON.

A tenant user has submitted a fraud alert for his account. After receiving an alert call, the user needs to enter a special code followed by #.

Which of the following is default special code?

A. 0

B. 9

C. 0000

D. 1234

Correct Answer: *A*

References:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert

Davidchercm Highly Voted 1 year, 1 month ago

Code to report fraud during initial greeting: When users receive a phone call to perform multi-factor authentication, they normally pres to confirm their sign-in. To report fraud, the user enters a code before pressing #. This code is 0 by default, but you can customize it.

upvoted 14 times

simoen Most Recent 2 weeks, 1 day ago

such a useless question...

upvoted 1 times

invaderzim48 1 week, 3 days ago

Really though, what is this designed to test other than the ability to memorize niche features.

upvoted 1 times

Nilz76 7 months, 3 weeks ago

Fraud greeting (standard): Thank you for using Microsoft's sign-in verification system. Please press the pound key to finish your verification. If you did not initiate this verification, someone may be trying to access your account. Please press zero pound to submit a fraud alert. This will notify your company's IT team and block further verification attempts.

upvoted 2 times

Your company has a Microsoft Office 365 subscription with a number of Microsoft SharePoint Online sites.
Currently, users are able to invite external users to access files on the SharePoint sites. You are tasked with making sure that users are only able to authenticated guest users to the SharePoint sites.
Which of the following actions should you take?

A. You should create a threat management policy via the Security & Compliance admin center.

B. You should run the Set-SPOSite cmdlet.

C. You should run the Add-SPOUser cmdlet.

D. You should modify the sharing settings via the SharePoint admin center.

Correct Answer: *D*

FleurJ Highly Voted 1 year ago
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off
upvoted 7 times

francklinmg Most Recent 1 year ago
Correct!
upvoted 2 times

Question #30 *Topic 1*

Your company has a Microsoft 365 subscription.

You have been tasked with configuring external collaboration settings for your company's Microsoft Azure Active Directory (Azure AD) tenant.

You want to make sure that authorized users are able to create guest users in the tenant.

Which of the following actions should you take?

Which setting should you modify?

A. You should make sure that the Guests can invite setting is set to NO.

B. You should make sure that the Guest users permissions are limited setting is set to Yes.

C. You should make sure that the Members can invite setting is set to NO.

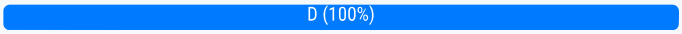
D. You should make sure that the Admins and users in the guest inviter role can invite setting is set to Yes.

Correct Answer: *D*

References:

https://docs.microsoft.com/en-us/azure/active-directory/b2b/delegate-invitations https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions

Community vote distribution



MEG 7 months, 1 week ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#to-configure-external-collaboration-settings

upvoted 2 times

Durden871 7 months, 2 weeks ago

The question asks, "You want to make sure that authorized users are able to create guest users in the tenant."

There is no mention of making them the ONLY ones who can create guest accounts. The answer is D because D allows the permission. Again, no mention that others shouldn't.

upvoted 2 times

Wojer 9 months, 3 weeks ago

Truly speaking if A is not set up to NO then D has no point.
Because everyone can invite guest by default

upvoted 2 times

Wojer 9 months, 3 weeks ago

I had in mind c need to be set to NO

upvoted 1 times

Don123 11 months, 1 week ago

I think this answers need to be updated, check the 365 portal, setting are different than than the answers related in this question.

upvoted 1 times

emilianogalati 1 year, 1 month ago

I think there is an error.

If I change the D to NO, I will NOT be able to allow users to invite guest.
Therefore it should be set on NO, or there should be another answer.

I am right, aren't I?

upvoted 2 times

Aps123 1 year ago

No, it says authorised users. So you need to add those users to guest inviter role.

upvoted 1 times

Question #31 *Topic 1*

After acquiring a Microsoft 365 subscription, you configure the use of Microsoft Azure Multi-Factor Authentication (MFA) for all users in the Azure Active Directory
(Azure AD) tenant.
You want to produce a report that includes all the users who finished the Azure MFA registration process. You want to make use of an Azure Cloud Shell cmdlet.
Which of the following is the cmdlet you should use?

A. Get-AzureADUser

B. Get-MsolUser

C. New-AzureADMSInvitation

D. Set-MsolUserPrincipalName

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting

Community vote distribution
B (100%)

ItsMax Highly Voted 1 year, 3 months ago
sure
complete command is:
Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods -ne $null -and $_.BlockCredential -eq $False} | Select-Object -Prope
UserPrincipalName
upvoted 23 times

extrankie 9 months ago
great explanation
upvoted 1 times

emilianogalati 1 year, 1 month ago
Thank you.
I will test it later on my tenant!
upvoted 1 times

Ademar 1 year ago
Thanks
upvoted 2 times

Mthaher Most Recent 5 months ago
B. Get-MsolUser
upvoted 2 times

Tibo49100 5 months, 1 week ago
MSOL commands are not available in Cloud Shell so I think this question is not valid any more
upvoted 2 times

trexar 6 months ago
Selected Answer: B
Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods -ne $null -and $_.BlockCredential -eq $False} | Select-Object -Prope
UserPrincipalName
upvoted 2 times

bakkus 10 months, 1 week ago
According to https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0 all MSOL cmdlets are being deprecated: "Please note that we will begin to deprecate this module when the functionality of this module is migrated to the Azure Ac
Directory PowerShell for Graph. We advise customers who are creating new PowerShell scripts to use the newer module instead of this module."
upvoted 2 times

Razgrad 1 year ago

Is this still the correct answer? If we consider that this module is going to be deprecated shouldn't be the AzureAD cmdlet the valid one

upvoted 2 times

PDR 10 months ago

certainly outdated question / answer now , but the msol commands sometimes do still contain options/properties that the AzureAd commands do not and can be the better option in some scenarios even now. For example , you cannot look for a user with a particu domain in the UPN with Get-AzureADUser but the MSOL command allows you to specify with -Domain switch. Yes you can use 'Whe Object' to pipe through but when you are working with large sets of users it is better to have your filters in the first command to be most efficient.
Back to the OP though - main reason it needs updating is that the MFA and registration info is now available directly via a downloadable report in the portal and there is a new Authentication Methods experience that is is actually using different propertie now only exposable via Graph API. You can use MGGraph powershell module and the Get-MgUserAuthenticationPhoneMethod to g the info via powershell also, or just graph API rest calls

upvoted 3 times

FumerLaMoquette 1 year ago

I'm not sure msol is going to be deprecated soon. It's AzureRM that's deprecated and replaced by Az.

upvoted 2 times

Question #32 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.

You have recently configured a conditional access policy to force mobile device users to use multi-factor authentication when accessing Microsoft SharePoint.

To check who used multi-factor authentication to authenticate, you view the Usage reports from Azure Active Directory admin center.

Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required

B. user sign-ins

C. event logs

D. audit logs

Correct Answer: *B*

References:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting

Community vote distribution

B (100%)

HenriksDisciple 6 months ago

A will show you which users are required to use MFA, but
B will show you which users gained access by using MFA.

Therefor B, is the correct answer.
A doesn't show how users logged in at a certain time by using MFA.

upvoted 2 times

Wojer 9 months ago

Truly speaking A and B is the proper answer

upvoted 1 times

PDR 10 months ago

B is correct because Sign-Ins allow you to add custom filters to show access to sharepoint, using conditional access and MFA . Using ot
MFA reports doesnt give this kind of targeting

upvoted 4 times

Stiobhan 10 months, 1 week ago

Selected Answer: B

B is the answer - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

upvoted 3 times

Khaldunazar 10 months, 2 weeks ago

A is the correct answer you can't view MFA registered user from singn-ins
to report who have active or inactive MFA go to:
azure family group >Usage & insights>Authentication methods activity>(User registration detailsy)

upvoted 2 times

Wojer 9 months, 2 weeks ago

agree with Khaldunazar

upvoted 1 times

sliix 8 months, 1 week ago

The question asked who used MFA to authenticate. That's the keyword. Therefore we can view it using the View Sign-ins. What you share is to view which users have MFA enabled.

upvoted 2 times

TeejayOne 1 year ago

Answer is correct

upvoted 2 times

emilianogalati 1 year, 1 month ago

Correct!

upvoted 2 times

Your company has an Enterprise E5 subscription of Microsoft 365.

You have been tasked with making sure that sales department users are compelled to make use of multi-factor authentication for all cloud-based applications.

Which of the following actions should you take?

A. You should create an DLP.

B. You should create a new app registration.

C. You should create a session policy.

D. You should create a sign-in risk policy.

Correct Answer: *D*

References:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

YClaveria Highly Voted 12 months ago

The how-to is in the provided reference: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#sign-in-risk-with-conditional-access

....
6. Under Cloud apps or actions > Include, select All cloud apps.
7. Under Conditions > Sign-in risk, set Configure to Yes. Under Select the sign-in risk level this policy will apply to
a. Select High and Medium.
b. Select Done.
8. Under Access controls > Grant, select Grant access, Require multi-factor authentication, and select Select.
...

upvoted 12 times

Storm 7 months, 3 weeks ago

Why would you assume that our sales personnel has done anything to be recognized by MS as risky users ???

upvoted 6 times

TimurKazan Highly Voted 11 months, 1 week ago

actually this is implemented in conditional access policies. I don think it has something to do with sign in risk policies regarding cloud a

upvoted 6 times

extrankie 9 months ago

Conditional access should be best be approach but risky policy also force MFA

upvoted 2 times

Pha0691 Most Recent 4 weeks, 1 day ago

Risk-based policies
If your organization uses Azure AD Identity Protection to detect risk signals, consider using risk-based policies instead of named locatio
Policies can be created to force password changes when there is a threat of compromised identity or require MFA when a sign-in is deemed at risk such as leaked credentials, sign-ins from anonymous IP addresses, and more.

Risk policies include:

Require all users to register for Azure AD Multi-Factor Authentication
Require a password change for users that are high-risk
Require MFA for users with medium or high sign in risk

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

upvoted 1 times

hussain2000 5 months, 1 week ago

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy
here it is boys

D is the answer

upvoted 1 times

Storm 7 months, 3 weeks ago

There is no way we can force all sales personel to be risky users...
I have no idea why people are upvoting suggestions to create a risk policy that requires MFA for all users with medium or high risk leve
think we can assume that the people we have hired in out sales department are not doing impossible travel, logging in from unknown
or other stuff that would make them risky...
The correct answer should be conditional access policy...

upvoted 6 times

HenriksDisciple 6 months ago

This is the truth.

upvoted 1 times

Frede 6 months ago

You are correct Sir!

upvoted 1 times

joergsi 8 months, 1 week ago

if you follow this link:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

you will find:
Risk-based policies
If your organization uses Azure AD Identity Protection to detect risk signals, consider using risk-based policies instead of named locatio
Policies can be created to force password changes when there is a threat of compromised identity or require multifactor authentication
when a sign-in is deemed risky by events such as leaked credentials, sign-ins from anonymous IP addresses, and more.

Risk policies include:
- Require all users to register for Azure AD MFA
- Require a password change for users that are high-risk
- Require MFA for users with medium or high sign-in risk

=> D is correct

upvoted 2 times

Tuno 1 year ago

I would say the answer is correct: " The sign-in risk policy detects suspicious actions that come along with the sign-in. It is focused on th
sign-in activity itself and analyzes the probability that the sign-in may not have been performed by the user. The sign-in risk checks for
things like whether a user has signed in from an unfamiliar location or unfamiliar IP address. You can then choose to require MFA for
users based on the risk level of their sign-ins."

upvoted 2 times

Rlcky 1 year ago

i think the right answer is to create a session policy https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

upvoted 1 times

joergsi 8 months, 1 week ago

If you follow the link, you will find this requirement for session policy :
Azure AD Premium P1 license, or the license required by your identity provider (IdP) solution
=> We don't have this license!

upvoted 1 times

fofo1960 1 year ago

I am not sure that this is correct answer

upvoted 1 times

Noie 1 year, 2 months ago

It is not possible to CREATE a sign-in risk policy.
Only configure and activate is possible.

upvoted 2 times

Question #34 *Topic 1*

Your company has a Microsoft 365 subscription.

After implementing Active Directory Federation Services (AD FS), you are instructed to configure AD FS user authentication auditing.

You are preparing to run the Register-AzureADConnectHealthSyncAgent cmdlet.

Which of the following is the server that the cmdlet should be run from?

NOTE: Each correct selection is worth one point.

A. A member server.

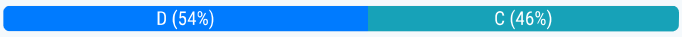
B. A domain controller.

C. An Azure AD Connect server.

D. An AD FS server.

Correct Answer: *C*

Community vote distribution



vasyab Highly Voted 1 year, 3 months ago

Answer is correct. This cmdlet available after you install AzureAD Connect
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#manually-register-azure-ad-conne
health-for-sync

upvoted 13 times

tejb Highly Voted 1 year ago

ADFS Server - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

upvoted 9 times

Nastha 9 months, 3 weeks ago

Your AD FS server should be different from your Sync server. Don't install the AD FS agent on your Sync server.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install. Could it be only Azure AD Conn
Server? Not ADFS server, right?

upvoted 4 times

Eggsamine 11 months, 2 weeks ago

Agreed, the important part of that doc is:
"Health agents must be installed and configured on targeted servers so that they can receive data and provide monitoring and analytics capabilities.

For example, to get data from your Active Directory Federation Services (AD FS) infrastructure, you must install the agent on the AD server and the Web Application Proxy server. Similarly, to get data from your on-premises Azure AD Domain Services (Azure AD DS) infrastructure, you must install the agent on the domain controllers."

Therefore correct answer should be D. An AD FS server.

upvoted 7 times

kanag1 8 months, 3 weeks ago

Thats is correct, AAD Connect server doesn't provide sig-in logs (what is needed in this case). Its the ADFS server that logs these details. So , deploy the agent on the ADFS server and run the command to get the required details.

upvoted 2 times

mmraouf Most Recent 1 week, 3 days ago

C is the correct answer
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#manually-register-azure-ad-conn
health-for-sync

upvoted 1 times

fcmtz 2 weeks, 5 days ago

Respuesta correcta es C

upvoted 1 times

ovd 4 weeks, 1 day ago

Answer is correct. This cmdlet available after you install AzureAD Connect
Register-AzureADConnectHealthSyncAgent cmdlet - Azure AD Connect Health for Sync srv
Register-AzureADConnectHealthADFSAgent cmdlet - Azure AD Connect Health for ADFS srv
upvoted 3 times

relaxswe 2 weeks, 4 days ago
This answer should get more votes. The powershell command to register Health Agents are different depending on what server and service it is you want to register.

Register-AzureADConnectHealthSyncAgent - Is for AAD Connect
Register-AzureADConnectHealthADFSAgent - IS for ADFS
Register-AzureADConnectHealthADDSAgent - IS for AADS

The Question was what server we should run the command "Register-AzureADConnectHealthSyncAgent" on. And the answer should the AAD Connect server.
The fact that there is ADFS infrastructure is irrelevant to the question and answer.
upvoted 3 times

relaxswe 2 weeks, 4 days ago
PS: This alone would not meet the requirements to audit sign in logs though.
You would have to install ADFS Health agent on the ADFS server and enable auditing as well to meet the requirements of sign in auditing.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install
upvoted 2 times

pozzetttt 1 month ago
Selected Answer: D
Look at this link.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install
upvoted 1 times

Contactfornitish 5 months, 3 weeks ago
You can't run Register-AzureADConnectHealthSyncAgent on ADFS
upvoted 1 times

Contactfornitish 5 months, 3 weeks ago
Selected Answer: C
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

Register-AzureADConnectHealthADFSAgent goes to ADFS. Sync agent talks about sync errors while ADFS agent talk about sign in audit
upvoted 1 times

musiman 6 months ago
The answer should be: B and D.
According to this article: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install
you should install the health agent on the ADFS server, the WAP server and on all Domain Controllers.

<quote>
Health agents must be installed and configured on targeted servers so that they can receive data and provide monitoring and analytics capabilities.

For example, to get data from your Active Directory Federation Services (AD FS) infrastructure, you must install the agent on the AD FS server and the Web Application Proxy server. Similarly, to get data from your on-premises Azure AD Domain Services (Azure AD DS) infrastructure, you must install the agent on the domain controllers.
</quote>
upvoted 1 times

itmaster 6 months, 1 week ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#:~:text=For%20example%2C%20to,the%20domain%20controllers.
upvoted 1 times

rahul_c92 6 months, 3 weeks ago
I thought this is a multiple choice Q, Which means both C & D are correct Answers.
upvoted 1 times

Nilz76 7 months ago
Selected Answer: D
You install the agent on the server you wish to audit. In this case, it's the ADFS server.

upvoted 1 times

jage01 7 months ago

D.

Remember that before you see any AD FS data in your instance of Azure AD Connect Health, you will need to install the Azure AD Conn Health Agent on your targeted servers.

https://github.com/toddkitta/azure-content/blob/master/articles/active-directory/active-directory-aadconnect-health-agent-install.md#installing-the-azure-ad-connect-health-agent-for-ad-fs

upvoted 1 times

jage01 7 months ago

Selected Answer: D

Health agents must be installed and configured on targeted servers so that they can receive data and provide monitoring and analytics capabilities.

For example, to get data from your Active Directory Federation Services (AD FS) infrastructure, you must install the agent on the AD FS server and the Web Application Proxy server. Similarly, to get data from your on-premises Azure AD Domain Services (Azure AD DS) infrastructure, you must install the agent on the domain controllers.

upvoted 1 times

MEG 7 months ago

Selected Answer: C

Read this: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#manually-register-azur ad-connect-health-for-sync
...If the Azure AD Connect Health for Sync agent registration fails after you successfully install Azure AD Connect, then you can use a PowerShell command to manually register the agent.

That means Register-AzureADConnectHealthSyncAgent is used to be on Azure AD Connect server.

upvoted 1 times

RiTh73 7 months, 1 week ago

Selected Answer: D

D -> Correct.

Health agents must be installed and configured on targeted servers so that they can receive data and provide monitoring and analytics capabilities.

For example, to get data from your Active Directory Federation Services (AD FS) infrastructure, you must install the agent on the AD FS server and the Web Application Proxy server. Similarly, to get data from your on-premises Azure AD Domain Services (Azure AD DS) infrastructure, you must install the agent on the domain controllers.

Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#:~:text=The%20Azure%20AD,the%20domain%20controllers.

upvoted 2 times

Youwork67 7 months, 3 weeks ago

Selected Answer: D

The Azure AD Connect Health agent is installed on each targeted server. Health agents must be installed and configured on targeted servers so that they can receive data and provide monitoring and analytics capabilities.

For example, to get data from your Active Directory Federation Services (AD FS) infrastructure, you must install the agent on the AD FS server and the Web Application Proxy server. Similarly, to get data from your on-premises Azure AD Domain Services (Azure AD DS) infrastructure, you must install the agent on the domain controllers.

upvoted 1 times

You need to consider the underlined segment to establish whether it is accurate.
Your company has deployed a Microsoft 365 tenant and to implemented multi-factor authentication.
They have four offices, of which one houses the R&D department. You have been asked to make sure that multi-factor authentication is compulsory only for users in the office houses the R&D department.
You create a conditional access policy.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required

B. password protection

C. DLP

D. label

Correct Answer: *A*

Wojer 9 months ago
security -> conditional access -> create policy
upvoted 1 times

YClaveria 11 months, 4 weeks ago
Sign in risk policy through conditional access, so answer is correct https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#sign-in-risk-with-conditional-access
upvoted 2 times

zul_n 1 year ago
A is correct
upvoted 4 times

Your company has configured all user email to be stored in Microsoft Exchange Online.
You have been tasked with keeping a duplicate of all the email messages from a specified user that includes a specific word.
Solution: You start by creating a spam filter policy via the Security & Compliance admin center.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

Mercious 4 days, 7 hours ago
The answer is right
upvoted 1 times

Your company has configured all user email to be stored in Microsoft Exchange Online.

You have been tasked with keeping a duplicate of all the email messages from a specified user that includes a specific word.

Solution: You start by initiating a message trace via the Security & Compliance admin center.

Does the solution meet the goal?

A. Yes

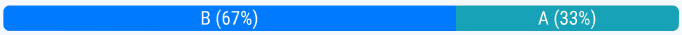
B. No

Correct Answer: *B*

References:

https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

Community vote distribution



neeewbi 3 weeks, 3 days ago

Selected Answer: B

correct

upvoted 2 times

ajiejeng 1 month ago

Selected Answer: B

B is correct , i use message trace when checking emails statuses

upvoted 2 times

Wesje 7 months, 2 weeks ago

Selected Answer: A

duplicate

upvoted 2 times

Your company has configured all user email to be stored in Microsoft Exchange Online.

You have been tasked with keeping a duplicate of all the email messages from a specified user that includes a specific word.

Solution: You start by creating a label and label policy via the Security & Compliance admin center.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *A*

References:

https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

joergsi 8 months, 1 week ago

In the provided link you will find:
When you configure conditions for a label, you can automatically assign a label to a document or email. Or, you can prompt users to se the label that you recommend.

When you configure these conditions, you can use predefined patterns, such as Credit Card Number or USA Social Security Number (SS Or, you can define a custom string or pattern as a condition for automatic classification. These conditions apply to the body text in documents and emails, and to headers and footers. For more information about the conditions, see step 5 in the following procedure.

upvoted 1 times

Fcnet 1 year, 2 months ago

We should talk about retention label not only label policy as there are sensitive labels too so it's confusing by the way if the answer talk about retention label then it' ok
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

upvoted 3 times

Your company has a Microsoft 365 subscription.

You have previously created a group that includes users who send email messages to external users on a regular basis. The group's manager would like to group wants to examine messages that include attachments at random.

You are required to make sure that the manager can achieve his goal, but only make ten out of a hundred messages accessible to him.

You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

Which of the following should you create?

A. A label policy.

B. A conditional access policy.

C. A DLP policy.

D. A supervisor policy.

Correct Answer: *D*

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/supervision-policies

Community vote distribution

D (100%)

ExamTraining24 8 months, 1 week ago

Selected Answer: D

Outdated question as Supervisor Policies are now deprecated and replaced with the Communication Compliance Policy... But D is the o option here.

upvoted 4 times

Glorence 8 months, 4 weeks ago

As per the link provided, isn't supposed to be a Communication Compliance Policy?
https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide

upvoted 2 times

Stiobhan 10 months ago

Yeah, it should state a communication-compliance policy - https://docs.microsoft.com/en-us/microsoft-365/compliance/communicatior compliance?view=o365-worldwide
I guess Supervision Policy would be the closest answer here.

upvoted 3 times

Jcbrow27 11 months ago

It is a comunication policy, i think.

upvoted 1 times

You need to consider the underlined segment to establish whether it is accurate.
Your company has recently acquired a new sales application.
You navigate to the Discovered apps page in Cloud Discovery via Microsoft Cloud App Security to check the application's score. You then notice that a number of the applications have a low score as a result of omitted domain registration and consumer popularity data.
You want to make sure that the score is not affected by the omitted data.
You have to configure app tags via the Cloud Discover settings
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.
What should you configure from the?

A. No adjustment required

B. a label

C. App Connector flow

D. a custom key

Correct Answer: *A*
References:
https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries

hopalong 1 week, 2 days ago
D I think?
https://learn.microsoft.com/en-us/defender-cloud-apps/risk-score
This doc clearly shows us that to make domain registration status not count you go to cloud discovery -> score metrics
So I assume custom key is the only answer that makes sense?
upvoted 1 times

Nastha 9 months, 3 weeks ago
I think the correct URL is:-
https://docs.microsoft.com/en-us/defender-cloud-apps/discovered-app-queries
upvoted 1 times

Question #41 *Topic 1*

You have been tasked with migrating your company's on-premises Microsoft Exchange Server 2013 organization to Microsoft 365.

You plan to make use of the cutover migration method.

Which of the following is the maximum recommended number of mailboxes that you should migrate?

A. 2000

B. 1000

C. 150

D. 75

Correct Answer: *C*

References:

https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365

MomoLomo Highly Voted 1 year, 2 months ago

maximum number of 2000
maximum -recommended- number 150

upvoted 16 times

Bobalo Highly Voted 1 year, 2 months ago

Unnecessary convoluted question. There is a maximum number of 2000 for a cutover migration and a recommended number of 150. Asking what the maximum recommended number is, is just wrong.

upvoted 11 times

[Removed] 8 months ago

It's not that convoluted when you think about it. There's many things that have a "maximum" value. In this case, the maximum it is capable of doing is 2000, but this would take a long time to migrate that many users, so the maximum they recommend is 150. If yo just say recommended, that makes it sound like it has to be exactly 150, no more no less, for the recommended number, which wou be false. Less is better because it would take less time to migrate, so the maximum they recommend is 150, but less is even better. Hence maximum recommended.

upvoted 2 times

Genius1289 Most Recent 5 months ago

https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices.
"You can migrate a maximum of 2,000 mailboxes from your on-premises Exchange organization to Microsoft 365 or Office 365 using a cutover migration. The recommended number of mailboxes, however, is 150. Performance suffers with numbers higher than that. The mail contacts and distribution groups in your on-premises Exchange organization are also migrated."
Confusing....

upvoted 1 times

kanag1 8 months, 3 weeks ago

The questions says: maximum recommended ; hence the answer is 150

upvoted 2 times

mfaisal786 10 months ago

Even though cutover migration supports moving up to 2000 mailboxes, due to length of time it takes to create and migrate 2000 users is more reasonable to migrate 150 users or fewer.

upvoted 3 times

sabin001 10 months, 3 weeks ago

Even though cutover migration supports moving up to 2000 mailboxes, due to length of time it takes to create and migrate 2000 users is more reasonable to migrate 150 users or fewer.
So answer will be 2000

upvoted 1 times

Fcnet 1 year, 2 months ago

the question is clearly not well formulated as there are so much comments...

upvoted 2 times

jnashville 1 year, 3 months ago

https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365

Maximum does show 2000 but recommended is 150 or fewer

upvoted 3 times

Tullow_Steve 1 year, 3 months ago

Actuallt the answer is correct, 150 mailboxes:
'A maximum of 2,000 mailboxes can be migrated to Microsoft 365 or Office 365 by using a cutover Exchange migration. However, it is recommended that you only migrate 150 mailboxes.'
https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365

upvoted 2 times

AlexLiourtas 10 months, 3 weeks ago

recommended for 150 though, not maximum

upvoted 3 times

cloudboys 1 year, 3 months ago

The correct answer is C, that means 150
Please read this article: "A maximum of 2,000 mailboxes can be migrated to Microsoft 365 or Office 365 by using a cutover Exchange migration. However, it is recommended that you only migrate 150 mailboxes"
Reference: https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365

upvoted 2 times

larnyx 1 year, 3 months ago

I take back my previous answer, I missunderstood the question.

While Cutover Migration supports up to 2000, the RECOMMENDED number of max is 150, due to the time it takes to migrate a bigger number.

C is correct.

upvoted 2 times

larnyx 1 year, 3 months ago

The correct answer is A - 2000.

There is no migration method that has 150 as a max number,

upvoted 1 times

vasyab 1 year, 3 months ago

Question asks about maximum recommended not maximum possible. So answer is correct - 150 is recommended value.

upvoted 3 times

subbuhotmail 1 year, 2 months ago

Yes, they just asked the max recommended only. So answer is correct.

upvoted 1 times

You have recently created a Microsoft 365 Enterprise subscription and assigned all users licenses for all products.
You want to configure all Microsoft Office 365 ProPlus installations to be done via a network share. You also want to make sure that users are prevented from using the Internet to install Office 365 ProPlus.
Which of the following is the type of file that you should create?
NOTE: Each correct selection is worth one point.

A. An HTML download file.

B. An XML download file.

C. An HTTP download file.

D. An EXE download file.

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/deployoffice/overview-of-the-office-2016-deployment-tool#download-the-installation-files-for-office-365-proplus-from-a-local- source

joergsi 8 months, 1 week ago
following the link:

When running the Office Deployment Tool (ODT), you provide the location of the configuration file and define which mode the ODT sho run in:

To download Microsoft 365 Apps products and languages, use download mode. Example: setup.exe /download downloadconfig.xml. When you download Office to a folder that already contains that version of Office, the ODT will conserve your network bandwidth by downloading only the missing files. For example, if you use the ODT to download Office in English and German to a folder that already contains Office in English, only the German language pack will be downloaded.
upvoted 1 times

gxsh 11 months, 4 weeks ago
Definitively .xml file, so answer is correct.
upvoted 2 times

Rickert 1 year, 1 month ago
Should be XLM & Exe IMHO
upvoted 3 times

emilianogalati 1 year, 1 month ago
You know how to create a .exe file, don't you?
I don't. ;)
Jokes apart, I think the keypoint is "create".
upvoted 6 times

Question #43 *Topic 1*

You have recently created a Microsoft 365 subscription.

You have prepared an XML file for the upcoming Microsoft Office 365 ProPlus deployment.

The Channel attribute for the OfficeClientEdition attribute is set to Broad, while the Channel attribute for the Updates element is set to Targeted.

Which of the following the following is the frequency with which the installation of Office 365 ProPlus feature updates will occur?

A. Weekly.

B. Monthly

C. Six monthly

D. Annually

Correct Answer: *C*

References:

https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool#updates-element

https://docs.microsoft.com/en-us/deployoffice/overview-of-update-channels-for-office-365-proplus

Community vote distribution

C (100%)

larnyx Highly Voted 1 year, 3 months ago

Answer is correct, C.

OfficeClientEdition can be set to 32 or 64, references the build to Install.

But Targeted is no longer a valid attribute, it's been changed to SemiAnnualPreview.
See: https://docs.microsoft.com/en-us/deployoffice/update-channels-changes

https://docs.microsoft.com/en-us/deployoffice/overview-update-channels

upvoted 8 times

mfaisal786 Most Recent 10 months ago

Previous attribute value: Broad
New attribute value: SemiAnnual

upvoted 2 times

davem90 10 months, 2 weeks ago

Selected Answer: C

Answer is correct!
These are the new names for the update channels:

Previous attribute value: Broad
New attribute value: SemiAnnual

Previous attribute value: Targeted
New attribute value: SemiAnnualPreview

https://docs.microsoft.com/en-us/deployoffice/update-channels-changes

upvoted 3 times

rfox321 1 year ago

All these answers are so correct MY guy

upvoted 3 times

zul_n 1 year ago

C is correc
• Targeted : SemiAnnualReview / next semi-annually channel release
• broad : semiannual
• Monthly : current / current channel
• Insiders : CurrentPreview channel

upvoted 4 times

1ewj7 1 year, 1 month ago

C. Admin can set the updates to any length of time but 2 times a year is standard from MS

upvoted 2 times

Question #44 *Topic 1*

You have recently created a Microsoft 365 subscription.

You have prepared an XML file for the upcoming Microsoft Office 365 ProPlus deployment.

The Channel attribute for the OfficeClientEdition attribute is set to Broad, while the Channel attribute for the Updates element is set to Targeted.

Which of the following the following are the months of the year that security updates will be installed?

A. January and July.

B. March and September

C. June and December

D. April and October

Correct Answer: *B*

References:

https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool#updates-element

https://docs.microsoft.com/en-us/deployoffice/overview-of-update-channels-for-office-365-proplus

junior6995 Highly Voted 1 year ago

I hate this kind of "memorize" question, we should be tested in Key features of Microsoft 365 and AzureAD and not these stupid questi

upvoted 20 times

[Removed] 8 months ago

I don't know. I feel like I learned so much memorizing 2 random months. I'm so glad Microsoft decided to test us all on this to demonstrate knowledge. No sarcasm whatsoever.

upvoted 2 times

xelirec 9 months, 3 weeks ago

wth is the learning goal with this question right? no sense at all.

upvoted 6 times

stromnessian Highly Voted 1 year, 2 months ago

Messed up question. Security updates are installed on a monthly basis regardless of channel.

upvoted 19 times

stealthster Most Recent 2 weeks, 4 days ago

can be found here: https://learn.microsoft.com/en-us/training/modules/deploy-microsoft-365-apps-for-enterprise/9-explore-update-channels

upvoted 1 times

MEG 8 months, 3 weeks ago

B is correct.

WHY:
Check the previous attribute with the new one for Targeted and Broad: https://docs.microsoft.com/en-us/deployoffice/update-channels changes

Read this: https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#preview-upcoming-new-features-of-semi-annual-enterprise-channel

Semi-Annual Enterprise Channel (Preview) has only two release dates per year.

upvoted 1 times

JMB7448 9 months, 3 weeks ago

All channels getting security updates every month (if needed)
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels

upvoted 2 times

sabin001 10 months, 3 weeks ago

There are 3 primary update channels
1) current channel/ current channel(preview)
- Provides updates as soon as they're ready.
- New features at least once a month.

- No schedule for update.

2) Monthly Enterprise Channel
- Receive one update per month on a predictable release date
- Release on Second Tuesday of the month
- No dedication preview channel

3) Semi-Annual Enterprise Channel
- Update Twice a year
- January and July --> Update includes Features, security and non-security updates

Semi-Annual Enterprise Channel(Preview)
-- release new features twice a year.
-- Second Tuesday in MARCH and SEPTEMBER .

upvoted 8 times

YClaveria 11 months, 4 weeks ago

We are talking specifically about security updates.

"Semi-Annual Enterprise Channel (Preview) [Previously called Semi-Annual Channel (targeted)] is released with new features twice a yea
on the second Tuesday in March and September. This provides you with four months before those same new features are released in
Semi-Annual Enterprise Channel. Semi-Annual Enterprise Channel (Preview) also receives, if needed, security and non-security updates
every month, on the second Tuesday of the month"
- https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#preview-upcoming-new-features-of-semi-annual-enterpris
channel

All answers are incorrect. Correct answer is monthly, on the second Tuesday of the month.

upvoted 6 times

Turd_Reynolds 1 year, 3 months ago

This is a very confusing topic as nowhere in any Microsoft docs do I find March and September. Everything lists as January and July. I'm
questioning if a change was made by Microsoft on this and nobody saw it.

upvoted 2 times

subbuhotmail 1 year, 2 months ago

Semi Annual - Releases in Jan and July .
Semi Annual Targeted - Releases in March and September.

So answer is correct.

upvoted 8 times

vasyab 1 year, 3 months ago

Topic is clear if spend some time to googling

In this topic we can find that Targetes now has name Semi-Annual Enterprise (Preview) https://docs.microsoft.com/en-
us/deployoffice/update-channels-changes#office-deployment-tool

This topic mentioned about release date:
Semi-Annual Enterprise Channel (Preview) is released with new features twice a year, on the second Tuesday in March and Septemb
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#preview-upcoming-new-features-of-semi-annual-enterpr
channel

upvoted 2 times

larnyx 1 year, 3 months ago

A is correct.

SemiAnnualPreview releases 2 times each year, March and September.
SemiAnnual releases 2 times each yer, January and July.

upvoted 2 times

Velda 1 year, 3 months ago

"Channel attribute for the Updates element is set to Targeted." -> SemiAnnualPreview
which means that B is correct imho

Reference:
https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool#updates-element

upvoted 1 times

larnyx 1 year, 3 months ago

Ofcourse this is correct, My bad! I mixed the context up, It is B!

More info here on the changes that was made https://docs.microsoft.com/en-us/deployoffice/update-channels-changes

upvoted 1 times

Question #45 *Topic 1*

Your company's network contains two Active Directory forests, with two domains configured per forest. All workstations are domain-joined and have Windows 10 installed.
You have created a Microsoft Azure Active Directory (Azure AD) tenant in preparation for configuring Hybrid Azure AD join for the workstations.
You want to make sure that the tenant can be discovered by the workstations.
Which of the following should you create in each forest?

A. A migration endpoint.

B. A new conditional access policy.

C. A new trust relationship.

D. A new service connection point (SCP).

Correct Answer: *D*
References:
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-manual

Community vote distribution
D (100%)

AlexLiourtas Highly Voted 10 months, 1 week ago
D

Service Connection Points (SCPs) are objects in Active Directory that hold information about services. Services can publish information about their existence by creating serviceConnectionPoint objects in Active Directory. Client applications use this information to find and connect to instances of the service
upvoted 5 times

DArnett Most Recent 1 week, 2 days ago
Selected Answer: D
Valid; on exam 27 September 2022
upvoted 1 times

Mthaher 5 months ago
Selected Answer: D
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-manual#configure-a-service-connection-point
upvoted 1 times

waterlego 5 months, 2 weeks ago
Still valid, April 2022 - it talked about multiple forests trying to throw you off the scent though.
upvoted 3 times

After your company acquires a Microsoft 365 subscription, they instruct you to move all email data from their corporate Gmail to Microsoft Exchange Online.
The migration will be done via the Exchange admin center.
Which of the following is the migration method you should use?

A. Exchange Hybrid

B. IMAP migration

C. Cutover

D. Express migration

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrate-g-suite-mailboxes

mfaisal786 10 months ago
it should be clear that whether it is migration technique or migration strategy...
upvoted 1 times

Davidchercm 1 year, 1 month ago
repeat question
upvoted 1 times

larnyx 1 year, 3 months ago
Answer is correct, B.
upvoted 2 times

Question #47 *Topic 1*

After your company acquires a Microsoft 365 subscription, they instruct you to move all email data from their corporate Gmail to Microsoft Exchange Online.

The migration will be done via the Exchange admin center.

Which of the following is TRUE with regards to the data included in the migration?

A. All data will be migrated.

B. Only email data will be migrated.

C. Email and task data will be migrated.

D. Email and contact data will be migrated.

Correct Answer: *B*

References:

https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrate-g-suite-mailboxes

Community vote distribution

B (100%)

mfaisal786 Highly Voted 10 months ago

depends on which connector we use to migrate if IMAP then only emails and if GSuite Connector then All
https://docs.microsoft.com/en-us/exchange/mailbox-migration/perform-g-suite-migration

upvoted 7 times

extrankie 9 months ago

Yes, Gsuite will move all

upvoted 1 times

Mthaher Most Recent 5 months ago

You can migrate the following functionalities from Google Workspace to Microsoft 365 or Office 365:

Mail & Rules
Calendar
Contacts but still there are some limitation

upvoted 1 times

MEG 7 months ago

Selected Answer: B

IMAP migration will only migrate emails, not calendar, and contact information.

upvoted 1 times

sabin001 10 months, 3 weeks ago

with IMAP migration, only emails will get migrated.

upvoted 1 times

extrankie 11 months, 2 weeks ago

the question is not typically clear, what if one perform Gsuite migration

upvoted 1 times

Joshycannon 10 months ago

It is extremely clear. It says they are using the MS method, so this would obviously lead someone with any reading comprehension t
believe they are using the methods they learned about with MS, and that is it. Nowhere does it mention it was using that method, a
if they were then the question would be framed around this....

upvoted 2 times

xofowi5140 11 months, 3 weeks ago

https://docs.microsoft.com/en-us/exchange/mailbox-migration/automated-migration-neweac

upvoted 1 times

YClaveria 11 months, 4 weeks ago

Heads up on this, Google workspace migration is available that migrates emails, contacts, and calendars: https://docs.microsoft.com/en-us/exchange/mailbox-migration/perform-g-suite-migration. Good luck!

upvoted 1 times

zul_n 1 year ago

B is correct

for IMAP migration type, only emails will be mirad

upvoted 3 times

Topic 2 - Question Set 2

Question #1 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a Microsoft Office 365 tenant.
You suspect that several Office 365 features were recently updated.
You need to view a list of the features that were recently updated in the tenant.
Solution: You use the View service requests option in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

A service request is a support ticket. Therefore, the View service requests option in the Microsoft 365 admin center displays a list of support tickets. It does not display a list of the features that were recently updated in the tenant so this solution does not meet the goal.
To meet the goal, you need to use Message center in the Microsoft 365 admin center.
Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide

Community vote distribution

B (100%)

simbahmso 3 months, 2 weeks ago

Selected Answer: B

Makes sense, Message Center is the place to go

upvoted 1 times

Moderator 4 months, 2 weeks ago

Selected Answer: B

Correct, Message Center is the right place.

upvoted 2 times

Sh1rub10 4 months, 3 weeks ago

Selected Answer: B

Go to Message Center instead

upvoted 3 times

Question #2 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a Microsoft Office 365 tenant.
You suspect that several Office 365 features were recently updated.
You need to view a list of the features that were recently updated in the tenant.
Solution: You use Dashboard in Security & Compliance.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Depending on what your organization's Office 365 subscription includes, the Dashboard in Security & Compliance includes several widgets, such as Threat
Management Summary, Threat Protection Status, Global Weekly Threat Detections, Malware, etc. It does not display a list of the features that were recently updated in the tenant so this solution does not meet the goal.
To meet the goal, you need to use Message center in the Microsoft 365 admin center.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/security-dashboard https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide

Community vote distribution



Sh1rub10 Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Go to Message Center instead

upvoted 5 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a Microsoft Office 365 tenant.
You suspect that several Office 365 features were recently updated.
You need to view a list of the features that were recently updated in the tenant.
Solution: You use Message center in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where
Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.
Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide

Community vote distribution
A (100%)

Sh1rub10 4 months, 3 weeks ago
Selected Answer: A
Correct
upvoted 4 times

Moderator 4 months, 2 weeks ago
Yesh :)
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a Microsoft Office 365 tenant.
You suspect that several Office 365 features were recently updated.
You need to view a list of the features that were recently updated in the tenant.
Solution: You review the Security & Compliance report in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The Security & Compliance reports in the Microsoft 365 admin center are reports regarding security and compliance for your Office 365 Services. For example, email usage reports, Data Loss Prevention reports etc. They do not display a list of the features that were recently updated in the tenant so this solution does not meet the goal.
To meet the goal, you need to use Message center in the Microsoft 365 admin center.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/download-existing-reports

Community vote distribution
B (100%)

Sh1rub10 4 months, 3 weeks ago

Selected Answer: B
Go to Message Center instead
upvoted 4 times

You recently migrated your on-premises email solution to Microsoft Exchange Online and are evaluating which licenses to purchase.
You want the members of two groups named IT and Managers to be able to use the features shown in the following table.

Feature	Available to
Microsoft Azure Active Directory (Azure AD) conditional access	IT group, Managers group
Microsoft Azure Active Directory (Azure AD) Privileged Identity Management	IT group

The IT group contains 50 users. The Managers group contains 200 users.
You need to recommend which licenses must be purchased for the planned solution. The solution must minimize licensing costs.
Which licenses should you recommend?

A. 250 Microsoft 365 E3 only

B. 50 Microsoft 365 E3 and 200 Microsoft 365 E5

C. 250 Microsoft 365 E5 only

D. 200 Microsoft 365 E3 and 50 Microsoft 365 E5

Correct Answer: *D*
Microsoft Azure Active Directory Privileged Identity Management requires an Azure AD Premium P2 license. This license comes as part of the Microsoft 365 E5 license. Therefore, we need 50 Microsoft 365 E5 licenses for the IT group.
Conditional Access requires the Azure AD Premium P1 license. This comes as part of the Microsoft E3 license. Therefore, we need 200 Microsoft 365 E3 licenses for the Managers group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements

Community vote distribution
D (100%)

PeterC Highly Voted 1 year, 5 months ago
D - E3 has Conditional Access, PIM is E5
upvoted 14 times

melatocaroca Highly Voted 1 year, 4 months ago
PIM is a premium feature of Azure Active Directory, and as such does need licensing.
The license required is Azure AD Premium P2, which is available as a standalone add-on license.
You can also buy it as part of Azure AD Premium P2
• Enterprise Mobility + Security (EMS) E5
• Microsoft 365 Education A5
• Microsoft 365 Enterprise E5

Azure AD Premium P2 license comes as part of the Microsoft 365 E5 license.
Therefore, we need 50 Microsoft 365 E5 licenses for the IT group.

Conditional Access requires the Azure AD Premium P1 license.
This comes as part of the Microsoft E3 license. Therefore, we need 200 Microsoft 365 E3 licenses for the Managers group.

EMS E3, Microsoft 365 E3, and Microsoft 365 Business Premium includes Azure AD Premium P1.
EMS E5 or Microsoft 365 E5 includes Azure AD Premium P2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing
Answer B
upvoted 5 times

Velda 1 year, 3 months ago
You mean D, right? Your analysis contradicts given answer. Answer D should be correct.
upvoted 3 times

Parzival 3 months, 4 weeks ago
My thoughts too. Contradiction
upvoted 1 times

Y2 Most Recent 1 week, 5 days ago
The IT group contains 50 users & the Managers group contains 200 users so wouldn't you need 250 E3 and 50 E5?
upvoted 1 times

mikl 1 month, 3 weeks ago
Selected Answer: D
D. 200 Microsoft 365 E3 and 50 Microsoft 365 E5

PIM is E5 - so we will need E5 license for 50 uers - and E3 for 200 users.
upvoted 1 times

charat 4 months, 1 week ago
Selected Answer: D
E3 - P1 Conditional access
E5 - PIM

Answer is D.
upvoted 1 times

svenhalen 1 year, 3 months ago
PIM is E5 for sure
upvoted 2 times

RAJULROS 1 year, 4 months ago
This question came last week
upvoted 1 times

kutty09 1 year, 6 months ago
Can i get the document that compares with office Licenses with Azure AD?
upvoted 2 times

kikkens23 1 year, 5 months ago
for sure, you can google it > M365 Licenses
upvoted 5 times

Parzival 3 months, 4 weeks ago
https://www.microsoft.com/en-za/microsoft-365/compare-microsoft-365-enterprise-plans
upvoted 1 times

Question #6 *Topic 2*

You have a Microsoft 365 tenant that contains Microsoft Exchange Online.

You plan to enable calendar sharing with a partner organization named adatum.com. The partner organization also has a Microsoft 365 tenant.

You need to ensure that the calendar of every user is available to the users in adatum.com immediately.

What should you do?

A. From the Exchange admin center, create a sharing policy.

B. From the Exchange admin center, create a new organization relationship.

C. From the Microsoft 365 admin center, modify the Organization profile settings.

D. From the Microsoft 365 admin center, configure external site sharing.

Correct Answer: *B*

You need to set up an organization relationship to share calendar information with an external business partner. Office 365 admins can set up an organization relationship with another Office 365 organization or with an Exchange on-premises organization.

Reference:

https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship

ctfalci Highly Voted 2 years, 2 months ago

Explanation
You need to set up an organization relationship to share calendar information with an external business partner. Office 365 admins can set up an organization relationship with another Office 365 organization or with an Exchange on-premises organization.
Reference:
https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship

upvoted 25 times

melatocaroca 1 year, 4 months ago

Correct Answer: B
Use the Exchange admin center to create an organization relationship Or PowerShell
Set up an organization relationship to share calendar information with an external business partner. Microsoft 365 and Office 365 admins can set up an organization relationship with another Microsoft 365 or Office 365 organization or with an Exchange on-prem organization.
https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship

upvoted 3 times

STFN2019 Highly Voted 2 years, 2 months ago

Here's the valid link: https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/organization-relationships

upvoted 10 times

stoneface Most Recent 9 months ago

Repeated question!

upvoted 1 times

Wojer 9 months, 2 weeks ago

I would say C (admin centre -> settings -> org settings ->calendar)

upvoted 1 times

PDR 9 months, 2 weeks ago

If you look at C closely it says 'From the Microsoft 365 admin center, modify the Organization profile settings' and the calendar setti you refer to is not in that tab but under the Services tab in Org Settings. Answer is B

upvoted 2 times

Mujja 3 months, 3 weeks ago

In addition to the above from PDR, in the M365 portal you aren't able to add a specific domain. The question asks to add the dom adatum.com, which can only be done in EAC.

upvoted 1 times

Wojer 10 months ago

I would say C

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

Panku 1 year ago

B is correct answer

upvoted 1 times

Takloy 1 year, 8 months ago

Answer: B
Explanation: https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship

upvoted 5 times

mkoprivnj 1 year, 9 months ago

B for sure!

upvoted 3 times

d6 2 years, 2 months ago

I just had to do this for a client.

upvoted 6 times

DRAG DROP -

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

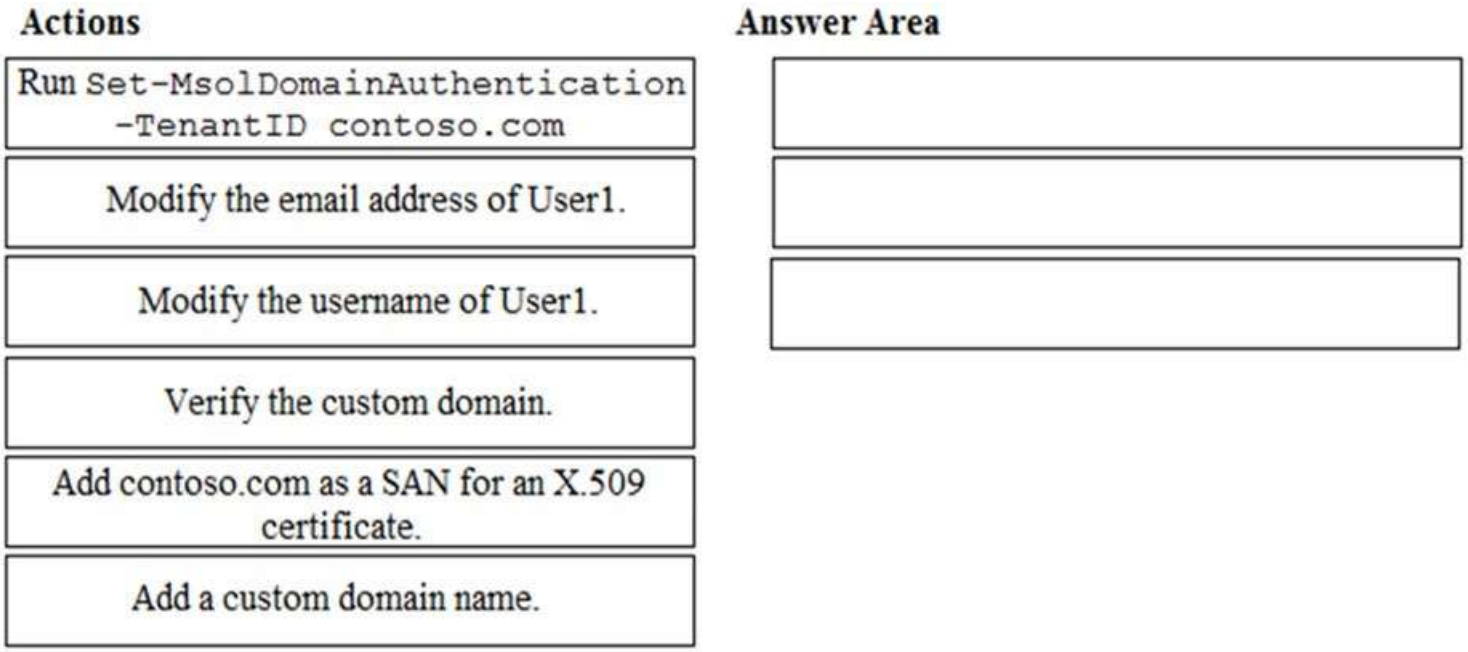
You purchase a domain named contoso.com from a registrar and add all the required DNS records.

You create a user account named User1. User1 is configured to sign in as user1@contoso.onmicrosoft.com.

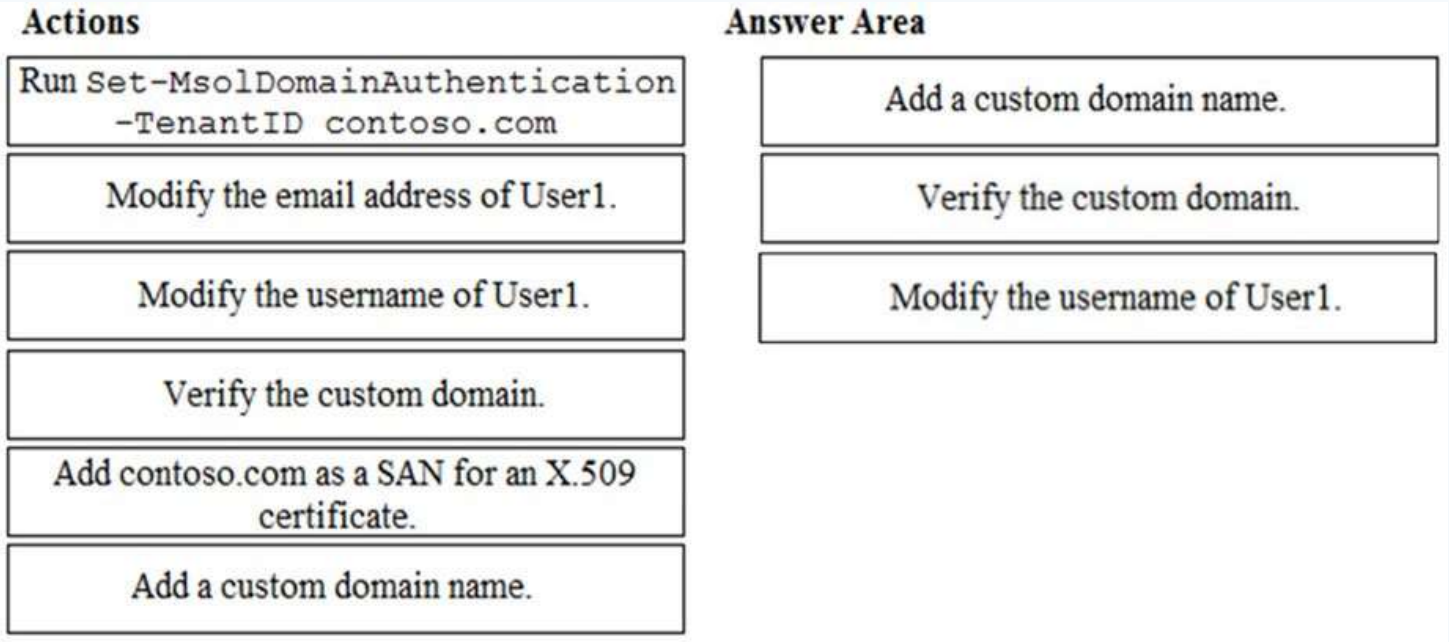
You need to configure User1 to sign in as user1@contoso.com.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



The first step is to add the contoso.com domain to Office 365. You do this by adding a custom domain. When you add a custom domain to office 365, you can use the domain as your email address or to sign in to Office 365.

The second step is to verify the custom domain. This is to prove that you own the domain. You can verify the custom domain by adding a DNS record to the domain DNS zone.

When you have added and verified the domain, you can configure the user accounts to use it. To configure User1 to sign in as user1@contoso.com, you need to change the username of User1. In Office 365, the username is composed of two parts. The first part is the actual username (User1) and the second part is the domain. You need to modify the username of User1 by selecting the contoso.com domain from the dropdown list of domains. The dropdown list of domains contains the <domain>.onmicrosoft.com domain and any custom domains

that have been added.

Reference:

https://docs.microsoft.com/en-us/office365/admin/setup/add-domain?view=o365-worldwide

PDR Highly Voted 1 year, 2 months ago

correct answer and to clarify the comments about changing email address or user name , it is user name that needs changing because the question is asking to change so they user can log in with the changed domain which means changing their UPN (User Principle Nar domain and NOT changing their email address. You can only have one UPN but you can have multiple emails addresses with multiple domains assigned to a user and there will always be an email for the configured UPN address, also for the onmicrosoft.com domain.

upvoted 18 times

tf444 9 months, 3 weeks ago

UPN is the email address, not the user name.
It should be the email address.

upvoted 1 times

TechMinerUK 3 months, 3 weeks ago

UPN is not the email address it is the username, whilst in most organisations the UPN happens to be the same as the email addr we should not mix up the two.

Even on Windows Active Directory the UPN is used as the username alongside the NETBIOS username

upvoted 4 times

sh0wbi Highly Voted 1 year, 4 months ago

correct answer !!

upvoted 14 times

Fcnet 1 year, 2 months ago

not really correct the last should be change email address

upvoted 5 times

Turak64 1 year, 1 month ago

This is why it's important to read the question "You need to configure User1 to sign in as user1@contoso.com." You're asked to configure the sign in which is the UPN, not the email address. They look similar, but they're not the same.

upvoted 18 times

tf444 9 months, 3 weeks ago

wrong, UPN is the email address!

upvoted 2 times

bake73 9 months ago

Confidently wrong

upvoted 7 times

Kalzonee3611 Most Recent 4 months, 1 week ago

“All dns records in place”

So, they have already added the domain and the TXT record for it???

upvoted 3 times

Rudelke 3 months ago

Yea it's dumb. Normally you'd add domain, then get verification record and set it up in DNS registrar and verify.

Still we all need to deal with confusing M$ questions

upvoted 1 times

slaoui 6 months ago

You need to modify the EMAIL Address:
https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/change-a-user-name-and-email-address?view=o365-worldwide

In the "Set Primary Email Address" section:
"1. In the admin center, go to the Users > Active users page.
2. Select the user's name, and then on the Account tab select Manage email aliases.
3. Select Set as Primary for the email address that you want to set as the primary email address for that person.
4. You'll see a big yellow warning that you're about to change the person's SIGN-IN information.'

upvoted 1 times

Koetjeboe 6 months, 1 week ago

From Microsoft website:

You must be a global admin to perform these steps.
- Go to the admin center at https://admin.microsoft.com.
- Go to the Setup > Domains page.
- On the Domains page, select Add domain.
- Follow the steps to confirm that you own your domain. You'll be guided to get everything set - up correctly with your domain in Micro
365.
- Go to Users > Active users.
- Select a user to edit their username and change it to the domain you just added.

So you need to change the username.

upvoted 2 times

Tibo49100 7 months, 1 week ago

Correct

upvoted 1 times

tf444 9 months, 3 weeks ago

.
A UPN (for example: john.doe@domain.com) consists of the user name (logon name), separator (the @ symbol), and domain name (UP
suffix). A UPN is not the same as an email address. Sometimes, a UPN can match a user's email address.

upvoted 5 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 1 times

sabin001 10 months, 3 weeks ago

Correct Answer
The first step is to add the contoso.com domain to Office 365. You do this by adding a custom domain. When you add a custom domain
office 365, you can use the domain as your email address or to sign in to Office365.

The second step is to verify the custom domain. This is to prove that you own the domain. You can verify the custom domain by adding
DNS record to the domain DNS zone.

When you have added and verified the domain, you can configure the user accounts to use it. To configureUser1 to sign in as
user1@contoso.com, you need to change the username of User1. In Office 365, theusername is composed of two parts. The first part i
the actual username (User1) and the second part is the domain. You need to modify the username of User1 by selecting the contoso.co
domain from the dropdownlist of domains. The dropdown list of domains contains the <domain>.onmicrosoft.com domain and any
custom domains that have been added.

Reference:
https://docs.microsoft.com/en-us/office365/admin/setup/add-domain?view=o365-worldwide

upvoted 3 times

Austin_Loh 11 months, 2 weeks ago

Confusing but here you go. It is shown as 'Username' in M365 admin center.
https://docs.microsoft.com/en-us/microsoft-365/admin/email/change-email-address?view=o365-worldwide

upvoted 3 times

Panku 1 year ago

Yes we need to change username however there is no saprate option for change email address

upvoted 1 times

Panku 1 year ago

https://docs.microsoft.com/en-us/microsoft-365/business-video/change-user-name-email?view=o365-worldwide

upvoted 1 times

zacmzee 1 year ago

Last one should be change username. Test it yourself, go to O365 admin center -> select user -> Click manage username -> select doma
name from drop down list.

upvoted 1 times

spg987 1 year, 1 month ago

It is my exam today- last one- modify the email address

upvoted 2 times

LouahZA 1 year, 1 month ago

bad question,

Manage username and email

If the primary email is also their username, then changing the primary email will also change their current username. An alias is anoth email address that people can use to email ben smith.

upvoted 1 times

lengySK 1 year, 1 month ago

correct. last one - modify the email address of User1

upvoted 2 times

spg987 1 year, 1 month ago

It was on my exam 16/8/2021

upvoted 1 times

karank19 1 year, 2 months ago

Last Option should be "Modify the Email Address"

upvoted 1 times

TechMinerUK 3 months, 3 weeks ago

No it shouldn't, the answer is correct as is as the email address is not the username. Many organisations may have usernames whic are identicle to the email but they are still two different objects

upvoted 1 times

JR_63021 1 year, 3 months ago

Whats the difference between username and email address? I thought username in this case would be User1? Doesn't needing to char the domain mean email address?

upvoted 2 times

Rokan 1 year, 3 months ago

Yes, Need to Change domain means email address.

upvoted 2 times

TechMinerUK 3 months, 3 weeks ago

No, the email address is not the username. Many organisations have email addresses which are the same as the username but t are two different variables and changing one automatically doesn't change the other.

This could be seen as early as Active Directory where your username would be %USERNAME%@%DOMAIN%.local but your email address would be %NAME%@%DOMAINE%.tld

Even with 365 and a traditional AD Connect you can see this if the user as the correct SMTP address set with a routable domain b has a .local UPN their username will be %USERNAME%@%ORG%.onmicrosoft.com whilst their email address is %NAME%@%DOMAIN%.tld

upvoted 1 times

Question #8 *Topic 2*

Your company has an on-premises Microsoft Exchange Server 2016 organization and a Microsoft 365 Enterprise E5 subscription.
You plan to migrate mailboxes and groups to Exchange Online.
You start a new migration batch.
Users report slow performance when they use the on-premises Exchange Server organization.
You discover that the migration is causing the slow performance.
You need to reduce the impact of the mailbox migration on the end-users.
What should you do?

A. Create a mail flow rule.

B. Configure back pressure.

C. Modify the migration endpoint settings.

D. Create a throttling policy.

Correct Answer: *C*
The migration is causing the slow performance. This suggests that the on-premise Exchange server is struggling under the load of copying the mailboxes to
Exchange Online. You can reduce the load on the on-premise server by reducing the maximum number of concurrent mailbox migrations.
Migrating just a few mailboxes at a time will have less of a performance impact than migrating many mailboxes concurrently.
Reference:
https://support.microsoft.com/en-gb/help/2797784/how-to-manage-the-maximum-concurrent-migration-batches-in-exchange-onl

LeGluten Highly Voted 2 years, 7 months ago
With the migration endpoint settings you will be able to choose how many simultaneous mailbox will be exported.
upvoted 28 times

ctfalci Highly Voted 2 years, 1 month ago
Answer: C
Explanation
The migration is causing the slow performance. This suggests that the on-premise Exchange server is struggling under the load of copying the mailboxes to Exchange Online. You can reduce the load on the on-premise server by reducing the maximum number of concurrent mailbox migrations. Migrating just a few mailboxes at a time will have less of a performance impact than migrating many mailboxes concurrently.
upvoted 21 times

extrankie 9 months ago
nice explain
upvoted 1 times

waterlego Most Recent 5 months, 2 weeks ago
Still valid, April 2022
upvoted 3 times

Wojer 9 months ago
I think that D is better answer
https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices#microsoft-365-and-office-365-migration-service-throttling
upvoted 1 times

Jcbrow27 10 months, 4 weeks ago
user-throttling is a configuration one by one user, in the scenarios of migration for a company i think is not the best way to migrate an control the performance, for me the answer is C
upvoted 1 times

Panku 1 year ago
C is right answer read the office ref document
upvoted 3 times

melatocaroca 1 year, 4 months ago

I really prefer Answer D, but C is valid too
D
Common migration performance factors
The user-throttling policy has default settings and limits the overall maximum data transfer rate.
https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices
C
On the migration endpoint itself, there are two values that can be changed:
MaxConcurrentMigrations denotes how many mailboxes can concurrently be moved from the migration endpoint during the initial pha
of the migration (copy of the mailbox). The default value is 20.
MaxConcurrentIncrementalSyncs depicts how many delta synchronizations can be active at the same time. The value for the default
endpoint is 20. When you create a new endpoint, the default is 10.
https://www.enowsoftware.com/solutions-engine/intelligently-using-migration-endpoints-to-speed-up-migrations-to-exchange-online

upvoted 4 times

jeffyeh 1 year, 1 month ago

I would prefer D as well. Most of the migration bottleneck is on networking side than the server loading.

upvoted 2 times

lengySK 1 year, 1 month ago

I prefer D as well.

upvoted 2 times

Aysan 1 year, 4 months ago

isn`t this ms-101 question?

upvoted 1 times

zer0en 1 year, 4 months ago

i can confirm that this is in the ms-100 exam per 23.05.21

upvoted 3 times

mkoprivnj 1 year, 9 months ago

C for sure!

upvoted 3 times

emil568 2 years, 1 month ago

Could be a solution

upvoted 1 times

minajahan 2 years, 7 months ago

This is an example cmdlet:
"Set-MigrationEndpoint -Identity CutoverExchangeEndpoint01 -MaxConcurrentIncrementalSyncs 50 -NspiServer Server01.contoso.com

https://docs.microsoft.com/en-us/powershell/module/exchange/move-and-migration/set-migrationendpoint?view=exchange-ps

upvoted 5 times

PDR 2 years, 6 months ago

additional info - looking at the link you provided there is also the parameter option
-MaxConcurrentMigrations , as the question specifies mailbox migrations this could be appropriate but as the question says a
'migration batch' it seems like a staged migration so the one you specified -MaxConcurrentIncrementalSyncs would be the best in th
case. The answer remains correct in either case of course.

upvoted 5 times

Question #9 *Topic 2*

You have a Microsoft 365 subscription.

You need to prevent phishing email messages from being delivered to your organization.

What should you do?

A. From the Exchange admin center, create an anti-malware policy.

B. From the Security & Compliance admin center, create a DLP policy.

C. From the Security & Compliance admin center, create a new threat management policy.

D. From the Exchange admin center, create a spam filter policy.

Correct Answer: *C*

Anti-phishing protection is part of Office 365 Advanced Threat Protection (ATP). To prevent phishing email messages from being delivered to your organization, you need to configure a threat management policy.

ATP anti-phishing is only available in Advanced Threat Protection (ATP). ATP is included in subscriptions, such as Microsoft 365 Enterprise, Microsoft 365

Business, Office 365 Enterprise E5, Office 365 Education A5, etc.

Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies

Community vote distribution

C (100%)

melatocaroca Highly Voted 1 year, 4 months ago

Anti-phishing protection in Exchange Online Protection (EOP) and Defender for Office 365
Anti-phishing protection is available in subscriptions that include EOP. Advanced anti-phishing protection is available in Defender for Office 365.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide#eop-anti-phishing-policy-settings

upvoted 8 times

Nastha Highly Voted 9 months, 3 weeks ago

Direct URLs : https://security.microsoft.com/antiphishing; https://security.microsoft.com/threatpolicy and click on Anti-Phishing; Micros 365 Defender Portal --> Policies & Rules from left pane --> Threat Policies --> Anti-Phishing under Policies.

upvoted 5 times

TechMinerUK Most Recent 3 months, 3 weeks ago

Selected Answer: C

The answer is right however from recent experience microsoft have phased out the security and compliance center in favor of two seperate areas (security.microsoft.com and compliance.microsoft.com)

Not sure if the new exam reflects this change however it has been like this for a while

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

sabin001 10 months, 3 weeks ago

Correct Answer
Anti-phishing protection is part of Office 365 Advanced Threat Protection (ATP). To prevent phishing email messages from being deliver to your organization, you need to configure a threat management policy.

ATP anti-phishing is only available in Advanced Threat Protection (ATP). ATP is included in subscriptions, such as Microsoft 365 Enterpris Microsoft 365 Business, Office 365 Enterprise E5, Office 365 Education A5, etc.

Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policie

upvoted 2 times

Sr15 1 year, 4 months ago

whats the diff betwn a threat management policy and a spam policy?

upvoted 2 times

Jcbrow27 10 months, 4 weeks ago

threat is an attack like malware, phishing, ransomware, infected url and spam is a marketing email or similar.

upvoted 3 times

Turak64 1 year, 1 month ago

Spam isn't necessarily a threat, it can just be junk mail trying to sell you stuff. Threat Management, protects against phishing attemp
etc

upvoted 5 times

Question #10 *Topic 2*

Your company has a Microsoft 365 subscription. All identities are managed in the cloud.
The company purchases a new domain name.
You need to ensure that all new mailboxes use the new domain as their primary email address.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Run the Update-EmailAddressPolicy Windows PowerShell command

B. From the Exchange admin center, select mail flow, and then configure the email address policies.

C. From the Microsoft 365 admin center, select Setup, and then configure the domains.

D. Run the Set-EmailAddressPolicy Windows PowerShell command.

E. From the Azure Active Directory admin center, configure the custom domain names.

Correct Answer: *BD*
Email address policies define the rules that create email addresses for recipients in your Exchange organization whether this is Exchange on-premise or
Exchange online.
You can configure email address policies using the graphical interface of the Exchange Admin Center or by using PowerShell with the Set-EmailAddressPolicy cmdlet.
The Set-EmailAddressPolicy cmdlet is used to modify an email address policy. The Update-EmailAddressPolicy cmdlet is used to apply an email address policy to users.
Reference:
https://docs.microsoft.com/en-us/exchange/email-addresses-and-address-books/email-address-policies/email-address-policies?view=exchserver-2019

Community vote distribution
CE (76%) DE (19%) 5%

Razuli Highly Voted 1 year, 5 months ago
C + E as others specified, just tested
upvoted 22 times

PeterC 1 year, 5 months ago
Agree ->
https://docs.microsoft.com/en-us/microsoft-365/admin/email/change-email-address?view=o365-worldwide
upvoted 4 times

YuvaRajaVignesh 3 months, 3 weeks ago
But this changes the email address of current users as well.
Question is to make the new domain as email address of new users.
upvoted 1 times

lengySK 1 year, 1 month ago
answer C no, because blade SETUP doesn't include domain...its in SETTINGS
upvoted 3 times

Aps123 1 year ago
Look at PeterC provided link, also do practical in OO365. When you click on custom domains under setup, it takes you to settings >domains
upvoted 2 times

tf444 9 months, 2 weeks ago
You must be a global admin to perform these steps.

Go to the admin center at https://admin.microsoft.com.
Go to the Setup > Domains page.

On the Domains page, select Add domain.

Follow the steps to confirm that you own your domain. You'll be guided to get everything set up correctly with your domain in Microsoft 365.

Go to Users > Active users.

Select a user to edit their username and change it to the domain you just added.

upvoted 1 times

MartinTexel Highly Voted 1 year ago

Correct answers should be D and E
there is a real example:
Set-EmailAddressPolicy -Identity "Office 365 Groups" -EnabledEmailAddressTemplates "SMTP:@contoso.com","smtp:@contoso.onmicrosoft.com","smtp:@contoso.microsoftonline.com"

In Exchange Online, this example modifies the existing email adress policy named "Office 365 Groups" and sets the enabled email addr templates to use "@contoso.com" as the primary SMTP address and "@contoso.onmicrosoft.com" and "@contoso.microsoftonline.com proxy addresses.

https://docs.microsoft.com/en-us/powershell/module/exchange/set-emailaddresspolicy?view=exchange-ps

and in Azure AD:
Select Custom domain names.
Select the name of the domain that you want to be the primary domain.

Select the Make primary command. Confirm your choice when prompted.
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-manage

upvoted 12 times

XW_64 6 days, 5 hours ago

Tested and confirmed! E and D are correct!

upvoted 1 times

zacmzee 1 year ago

Nice one, tested to confirm!

upvoted 1 times

rfox321 1 year ago

It's simply wrong because the answer states: "In Windows" - You don't run these from windows..

upvoted 1 times

Davidchercm 8 months, 3 weeks ago

what you mean you don't run these from windows ?

upvoted 2 times

XW_64 Most Recent 6 days, 5 hours ago

Selected Answer: DE

E & D are correct! Admin please check and update

upvoted 1 times

KemalM 2 weeks, 3 days ago

Selected Answer: DE

D & E is correct.
it's not C, because to configure the domains you should go to "Settings", not to "Setup".

upvoted 2 times

Chaostix 1 month, 3 weeks ago

Selected Answer: CE

"that all new mailboxes " no change on existing mailboxes!

upvoted 2 times

Mkhadir 3 months, 3 weeks ago

Selected Answer: CE

C + E is a correct answer

upvoted 2 times

TechMinerUK 3 months, 3 weeks ago

Selected Answer: CE

I believe the answer is C + E since the question makes no reference to the organisation having a traditional AD connected to AzureAD.

This means we cannot use D since there is no on-premises Exchange server to setup an email address policy on (Exchange Online does not support email address policies)

That means to add a new domain and set it for new users we would add the domain i nthe 365 portal and then set it to the default dom in AzureAD via the blade. Because it is the default domain any new user accounts will have the domain set as their default username ar they have an Exchange Online license as their default email address domain as well (It won't change existing account usernames or em addresses though)

upvoted 1 times

TechMinerUK 4 months ago

Selected Answer: CE

C + E as whilst not ideal answers it seems as though the question is wrong as there are no email address policies in Exchange Online

upvoted 2 times

mikaiwhodakno 3 months, 3 weeks ago

Some comments come from the point of changing everyones email to the new domain, where the question very specifically states c new users. Individual users can be changed/added later, but that is outside of the scope of this question.

upvoted 1 times

charat 4 months, 1 week ago

Selected Answer: CE

C & E for the reasons stated below from other fellows

upvoted 2 times

bastien95 4 months, 1 week ago

D + E for me

upvoted 2 times

M_kuttan 4 months, 2 weeks ago

Selected Answer: CE

there is no email address policy for mailboxes in office 365

upvoted 2 times

Sh1rub10 4 months, 2 weeks ago

Selected Answer: CE

C + E as others specified

upvoted 2 times

gaem 4 months, 2 weeks ago

Selected Answer: DE

Answer is D + E

upvoted 1 times

itmaster 6 months, 1 week ago

Selected Answer: CE

C ==>
https://docs.microsoft.com/en-us/microsoft-365/admin/email/change-email-address?view=o365-worldwide#:~:text=Go%20to%20the%20Setup%20%3E%20Domains%20page
E ==>
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#:~:text=Then%20select%20Custom%20domain%20names%20%3E%20Add%20custom%20domain

upvoted 2 times

mrrc1987 7 months, 1 week ago

Selected Answer: CE

https://docs.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-manage#set-the-primary-domain-name-for-your-azure-ad-organization

upvoted 1 times

[Removed] 7 months, 4 weeks ago

I just tested this, you can change the default domain in Microsoft 365 Admin Center, and thus the default primary email address associated with users.

upvoted 1 times

[Removed] 7 months, 4 weeks ago

It's also worth noting this will not change the primary email address of the current user mailboxes but it will change newly created users that are created in Microsoft 365 Admin Center. The question only mentioned new users but I thought it was worth mentionin this.

upvoted 1 times

mfaisal786 8 months ago

B is wrong , because there is no option available to configure Email Address Policies in Exchange Online Admin Center...

upvoted 1 times

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that includes the users shown in the following table.

Name	Usage location	Membership
User1	United States	Group1, Group2
User2	*Not set*	Group2
User3	*Not set*	Group1
User4	Canada	Group1

Group2 is a member of Group1.

You assign a Microsoft Office 365 Enterprise E3 license to Group1.

How many Office 365 E3 licenses are assigned?

A. 1

B. 2

C. 3

D. 4

Correct Answer: *C*

Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied. Therefore, User2 will not be assigned a license.

When Azure AD assigns group licenses, any users without a specified usage location inherit the location of the directory. Therefore, User3 will be assigned a license and his usage location will be set to the location of the directory.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-group-advanced

Community vote distribution



Carlo5 Highly Voted 1 year, 3 months ago

The answer C is right. Based on my test, you cannot assign license to user 3 directly. But you can assgin to a security group. Users with location will inherit the license. You can find it in the AAD license page.

upvoted 16 times

azexiroyal 2 weeks, 2 days ago

user 2 not 3

upvoted 1 times

Kotor987 2 months ago

Can confirm.

upvoted 1 times

rfox321 1 year ago

Big round of applause for actually testing.. instead of impulsively providing an incorrect answer. Thank you!

upvoted 11 times

rafaelsilva01 Highly Voted 1 year, 5 months ago

C for sure

upvoted 14 times

Kotor987 Most Recent 2 months ago

Selected Answer: C

Tested. It's C.

upvoted 1 times

ConveneSupport 2 months, 1 week ago

Now Azure supports nested security access

upvoted 1 times

KrisDeb 1 month ago

Limitations and known issues
If you use group-based licensing, it's a good idea to familiarize yourself with the following list of limitations and known issues.

Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nest group, only the immediate first-level user members of the group have the licenses applied.

upvoted 2 times

Rudelke 3 months ago

Had this question 07.2022

upvoted 1 times

TechMinerUK 3 months, 3 weeks ago

Selected Answer: C

C is correct and I can confirm this as we have alot of customers who we used to assign licenses to via groups. If the user is in a group w a license assigned but doesn't have a usage location explicitly set it will default to the tenant location.

Likewise the answer is correct as group based licensing does not cascade nested security groups

upvoted 1 times

charat 4 months, 1 week ago

Selected Answer: C

"For group license assignment, any users without a usage location specified inherit the location of the directory. "

Therefore, C is the correct answer

upvoted 2 times

charat 4 months, 1 week ago

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign

upvoted 1 times

frankchen0609 6 months, 3 weeks ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign#:~:text=Step%201%3A%20Assign%20the%20required%20licenses,-Sign%20in%20to&text=Under%20All%20products%2C%20select%20both,list%20of%20users%20and%20groups.

upvoted 1 times

mfaisal786 8 months ago

C is right because nested group licensing is not supported..

upvoted 1 times

IamSherlocked 1 year, 3 months ago

Answer is C. (3 licenses)
It is not 2 because for group license assignment, any users without a usage location specified inherit the location of the directory.
It is not 4 because, If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.
Ref: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

upvoted 5 times

Luiza 1 year, 3 months ago

B.2
I tested. "License cannot be assigned to a user without a usage location specified."

upvoted 11 times

Joshycannon 10 months ago

They are not assigning to users...They are assigning to a group.

upvoted 4 times

melatocaroca 1 year, 4 months ago

User 1, groups and multiple licenses

So user 2 and user 3 will got a license
User 4 Canada and group 1
Usage location isn't allowed
Problem: Some Microsoft services aren't available in all locations because of local laws and regulations. Before you can assign a license a user, you must specify the Usage location property for the user. You can specify the location under the User > Profile > Edit section in Azure portal.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-resolve-problems
Answer B

upvoted 3 times

melatocaroca 1 year, 4 months ago

Correct myself For group license assignment, any users without a usage location specified inherit the location of the directory.
User 1, groups and multiple licenses first level group 1 will got licence
So user 2 and user 3 will got a license For group license assignment, any users without a usage location specified inherit the locatio
the directory.
User 4 Canada and group 1
So 3

upvoted 2 times

Maroslaw 1 year, 4 months ago

The answer is correct, C

upvoted 2 times

jeremyburrows 1 year, 4 months ago

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#:~:text=If%20you%20apply%20a%20license,groups%20that%20have%20securityEnabled%3DTRUE.&text=Inherited%20grou
20licenses%20cannot%20be%20modified%20directly%20on%20a%20user.
under known limitations is says nested groups not supported. So the count should be 2

upvoted 1 times

gladi 1 year, 5 months ago

Reading the others comments, I think that only will have license the users of group1. Not license for nested groups and no locations. C
2 licenses. Correct?

upvoted 1 times

gladi 1 year, 5 months ago

Update: The answer is 3. According to Microsoft: "Any user whose usage location is not specified inherits the location of the Azure A
organization." -- https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups

upvoted 7 times

johnpapoulias 1 year, 5 months ago

Only 2 users will get a license assigned. Usage location is needed in order to get a license assigned.

upvoted 2 times

johnpapoulias 1 year, 5 months ago

After a small research, it seems that the users contained in a group get the default directory locations when a license is assigned to
group.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#usage-location

Usage location
Some Microsoft services are not available in all locations. Before a license can be assigned to a user, the administrator has to specify
the Usage location property on the user. In the Azure portal, you can specify usage location in User > Profile > Settings.

For group license assignment, any users without a usage location specified inherit the location of the directory. If you have users in
multiple locations, make sure to reflect that correctly in your user resources before adding users to groups with licenses.

upvoted 7 times

lucidgreen 1 year, 6 months ago

3. I don't think nested groups are supported, still.

upvoted 1 times

sadsadweqr23424dsdqweqwe 1 year, 6 months ago

Is a license going to be assigned to a user without a location usage?

upvoted 2 times

chaoscreater 1 year, 3 months ago

Did you not read the answer?

upvoted 1 times

You have a Microsoft 365 subscription.
A new corporate security policy states that you must automatically send DLP incident reports to the users in the legal department.
You need to schedule the email delivery of the reports. The solution must ensure that the reports are sent as frequently as possible.
How frequently can you schedule the delivery of the reports?

A. hourly

B. monthly

C. weekly

D. daily

Correct Answer: *C*
From the Dashboard in the Security and Compliance center, you can view various reports including the DLP Incidents report. From there you can configure a schedule to email the reports. In the schedule configuration, there are two choices for the frequency: Weekly or Monthly. Therefore, to ensure that the reports are sent as frequently as possible, you need to select Weekly.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/create-a-schedule-for-a-report

lucidgreen Highly Voted 1 year, 6 months ago
Tested this. Answer is corrct.
upvoted 8 times

Puneet30 Highly Voted 1 year, 4 months ago
Exam Q on 15May21
upvoted 5 times

charat Most Recent 4 months, 1 week ago
05/22 exam. Great stuff ExamTopics!
upvoted 2 times

Wojer 10 months ago
I think you can do daily reports but the report will have information from a last 7 days
upvoted 2 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 3 times

jjong 1 year ago
came out today on my exam on 27-sep-21
upvoted 3 times

Ash473 1 year, 1 month ago
In today's exam
upvoted 2 times

RAJULROS 1 year, 4 months ago
This question came on 28May21
upvoted 3 times

PeterC 1 year, 5 months ago
shortest report frequency is weekly
upvoted 4 times

Question #13 *Topic 2*

Your company has a Microsoft 365 subscription.

You need to identify all the users in the subscription who are licensed for Microsoft Office 365 through a group membership. The solution must include the name of the group used to assign the license.

What should you use?

A. the Licenses blade in the Azure portal

B. Reports in the Microsoft 365 admin center

C. Active users in the Microsoft 365 admin center

D. Reports in Security & Compliance admin center

Correct Answer: *A*

In the Azure AD Admin Center, select Azure Active Directory then select Licenses to open the Licenses blade. From there you need to click on the 'Managed your purchased licenses link'. Select a license you want to view, for example Office 365 E3. This will then display a list of all users with that license. In the

'Assignment Paths' column, it will say 'Direct' for a license that has been assigned directly to a user or 'Inherited (Group Name)' for a license that has been assigned through a group.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

Community vote distribution

A (100%)

Ray81 Highly Voted 2 years, 7 months ago

A is correct, under licenses, go to All Products, you'll see group assignments

upvoted 29 times

WoneSix 2 years, 7 months ago

Not quite as simple as that, but yes, this is where you're find the information. Azure AD (not the Azure portal, as the question says, b
I'll not argue symantics), Licenses, Licensed Groups, then select the individual groups to find a) members, and b) licenses assigned t
A is correct.

upvoted 7 times

PhantomPhixer 2 years, 4 months ago

slight clarification, Licenses, Licensed Groups, then select the individual licenses to find the info as stated under Licensed users o
licensed groups..

upvoted 2 times

ctfalci Highly Voted 2 years, 2 months ago

Answer: A
Explanation
In the Azure AD Admin Center, select Azure Active Directory then select Licenses to open the Licenses blade.
From there you need to click on the 'Managed your purchased licenses link'. Select a license you want to view, for example Office 365 E
This will then display a list of all users with that license. In the 'Assignment Paths' column, it will say 'Direct' for a license that has been
assigned directly to a user or 'Inherited (Group Name)' for a license that has been assigned through a group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

upvoted 18 times

Cheekypoo Most Recent 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

TechMinerUK 3 months, 3 weeks ago

Selected Answer: A

A is correct as it is the most logical answer since the Microsoft 365 Admin center whilst it will show the users assigned a license it will n
name the group which they are licensed through

upvoted 1 times

trexar 6 months ago

Selected Answer: A

correct

upvoted 1 times

Aze 1 year, 8 months ago

A is correct

upvoted 3 times

mkoprivnj 1 year, 9 months ago

A for sure!

upvoted 2 times

mkoprivnj 1 year, 9 months ago

ctfalci great job!

upvoted 1 times

FcoGlezRoy 2 years, 4 months ago

Correct answer is A but will require AD P2 or EMS

upvoted 5 times

JaBe 2 years, 1 month ago

Nope, a basic E3 is fine. Just tested it - you do get the friendly "Get started with license management" and the link to a free trial etc. you can just click 'manage your purchased licenses' and access the Licensed users - groups panes.

upvoted 3 times

DUSHIWORLD 2 years, 7 months ago

Correct Answer is A.
https://www.enowsoftware.com/solutions-engine/assigning-office-365-licenses-by-ad-group-membership

upvoted 7 times

WoneSix 2 years, 7 months ago

I don't see this in the Azure portal - in Azure AD, there's a licenses blade, but it doesn't show any assignments. Anyone know what they' saying here?

upvoted 1 times

ctfalci 2 years, 3 months ago

https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Licenses

upvoted 3 times

Question #14 *Topic 2*

Your company has a Microsoft 365 subscription.
You upload several archive PST files to Microsoft 365 by using the Microsoft 365 compliance center.
A month later, you attempt to run an import job for the PST files.
You discover that the PST files were deleted from Microsoft 365.
What is the most likely cause of the files being deleted? More than one answer choice may achieve the goal. Select the BEST answer.

A. The PST files were corrupted and deleted by Microsoft 365 security features.

B. PST files are deleted automatically from Microsoft 365 after 30 days.

C. The size of the PST files exceeded a storage quota and caused the files to be deleted.

D. Another administrator deleted the PST files.

Correct Answer: *B*
You can use the Office 365 Import Service to bulk-import PST files to Office 365 mailboxes.
When you use the network upload method to import PST files, you upload them to an Azure blob container named ingestiondata. If there are no import jobs in progress on the Import page in the Security & Compliance Center), then all PST files in the ingestiondata container in Azure are deleted 30 days after the most recent import job was created in the Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/faqimporting-pst-files-to-office-365

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/faqimporting-pst-files-to-office-365 You can use the Office 365 Import Service to bulk-import PST files to Office 365 mailboxes.
When you use the network upload method to import PST files, you upload them to an Azure blob container named ingestiondata. If th are no import jobs in progress on the Import page in the Security & Compliance Center), then all PST files in the ingestiondata containe Azure are deleted 30 days after the most recent import job was created in the Security & Compliance Center. Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/faqimporting-pst-files-to-office-365
upvoted 19 times

rleijten Highly Voted 2 years, 7 months ago
Unless the PST-files were uploaded in februari, and a month later no 30 days had passed :)
upvoted 8 times

Vsurvase Most Recent 6 months, 1 week ago
I got this question on 26 March 2022 exam.
upvoted 1 times

Turak64 1 year, 1 month ago
It's questions like this that really put me off MS exams, who decides what the "best" answer is? What if an admin had deleted the file, th B is no longer the correct answer!
upvoted 4 times

Ash473 1 year, 1 month ago
In today exam
upvoted 1 times

melatocaroca 1 year, 4 months ago
Azure are deleted 30 days after the most recent import job was created in the Security & Compliance Center.
https://docs.microsoft.com/en-us/microsoft-365/compliance/importing-pst-files-to-office-365?view=o365-worldwide
upvoted 1 times

Puneet30 1 year, 4 months ago
Exam Q on 15May21
upvoted 3 times

mkoprivnj 1 year, 9 months ago

B for sure!

upvoted 3 times

DUSHIWORLD 2 years, 7 months ago

B

https://docs.microsoft.com/en-us/microsoft-365/compliance/faqimporting-pst-files-to-office-365

upvoted 6 times

Question #15 *Topic 2*

Your company has a main office and 20 branch offices in North America and Europe. Each branch connects to the main office by using a WAN link.
All the offices connect to the Internet and resolve external host names by using the main office connections.
You plan to deploy Microsoft 365 and to implement a direct Internet connection in each office.
You need to recommend a change to the infrastructure to provide the quickest possible access to Microsoft 365 services.
What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. For all the client computers in the branch offices, modify the MTU setting by using a Group Policy object (GPO).

B. In each branch office, deploy a proxy server that has user authentication enabled.

C. In each branch office, deploy a firewall that has packet inspection enabled.

D. In the branch offices, configure name resolution so that all queries for external host names are redirected to public DNS servers directly.

Correct Answer: *D*
Being a cloud service, Office 365 would be classed as an external host to the office computers.
All the offices connect to the Internet and resolve external host names by using the main office connections. This means that all branch office computers perform
DNS lookups and connect to the Internet over the WAN link.
Each branch office will have a direct connection to the Internet so the quickest possible access to Microsoft 365 services would be by using the direct Internet connections. However, the DNS lookups would still go over the WAN links to main office. The solution to provide the quickest possible access to Microsoft 365 services is to configure DNS name resolution so that the computers use public DNS servers for external hosts. That way DNS lookups for Office 365 and the connections to Office 365 will use the direct Internet connections.

test123123 Highly Voted 2 years, 8 months ago
D,
"You configured each local office with Internet access with a local ISP whose DNS servers use a local public IP address that identifies th location on the Internet. This ensures the best possible performance for users who access Microsoft 365 cloud services.

If you don't use a local ISP for each branch office, performance can suffer because network traffic must traverse an organization's backbone or data requests are serviced by remote front-end servers."
Ref: https://docs.microsoft.com/en-us/microsoft-365/enterprise/deploy-with-existing-infrastructure
upvoted 19 times

test123123 Highly Voted 2 years, 8 months ago
More*

Because Office 365 runs on the Microsoft Global Network, which includes front end servers around the world, there will often be a fron end server close to the user's location. By providing local Internet egress and by configuring internal DNS servers to provide local nam resolution for Office 365 endpoints, network traffic destined for Office 365 can connect to Office 365 front end servers as close as poss to the user

Ref:
https://docs.microsoft.com/en-us/office365/enterprise/office-365-network-connectivity-principles#BKMK_P2
upvoted 14 times

Vsurvase Most Recent 6 months, 1 week ago
I got this question on 26 March 22 exam.
upvoted 3 times

Nastha 9 months, 2 weeks ago
Local DNS and Internet egress is of critical importance for reducing connection latency and ensuring that user connections are made t the nearest point of entry to Microsoft 365 services. In a complex network topology, it is important to implement both local DNS and lo Internet egress together.

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide
upvoted 2 times

Ash473 1 year, 1 month ago
In today's exam
upvoted 4 times

mkoprivnj 1 year, 9 months ago

D for sure!

upvoted 6 times

ctfalci 2 years, 2 months ago

Answer: D
Explanation
Being a cloud service, Office 365 would be classed as an external host to the office computers. All the offices connect to the Internet ar
resolve external host names by using the main office connections. This means that all branch office computers perform DNS lookups a
connect to the Internet over the WAN link. Each branch office will have a direct connection to the Internet so the quickest possible acce
to Microsoft 365 services would be by using the direct Internet connections. However, the DNS lookups would still go over the WAN link
to main office. The solution to provide the quickest possible access to Microsoft 365 services is to configure DNS name resolution so th
the computers use public DNS servers for external hosts. That way DNS lookups for Office 365 and the connections to Office 365 will us
the direct Internet connections.

upvoted 8 times

PDR 2 years, 7 months ago

agree answer is D

The ideal would for each branch to have their own DNS server but from the options public DNS servers are most likely better (say most
because it doesnt specify which public DNS servers - it could be configured for DNS servers that are further /slower than the main offic
one!)

upvoted 6 times

Question #16 *Topic 2*

Your network contains an Active Directory forest named adatum.local. The forest contains 500 users and uses adatum.com as a UPN suffix.
You deploy a Microsoft 365 tenant.
You implement directory synchronization and sync only 50 support users.
You discover that five of the synchronized users have usernames that use a UPN suffix of onmicrosoft.com.
You need to ensure that all synchronized identities retain the UPN set in their on-premises user account.
What should you do?

A. From the Microsoft 365 admin center, add adatum.com as a custom domain name.

B. From Windows PowerShell, run the Set-ADDomain ג€"AllowedDNSSuffixes adatum.com command.

C. From Active Directory Users and Computers, modify the UPN suffix of the five user accounts.

D. From the Microsoft 365 admin center, add adatum.local as a custom domain name.

Correct Answer: *C*
The question states that only five of the synchronized users have usernames that use a UPN suffix of onmicrosoft.com. Therefore the other 45 users have the correct UPN suffix. This tells us that the adatum.com domain has already been added to Office 365 as a custom domain.
The forest is named adatum.local and uses adatum.com as a UPN suffix. User accounts in the domain will have adatum.local as their default UPN suffix. To use adatum.com as the UPN suffix, each user account will need to be configured to use adatum.com as the UPN suffix.
Any synchronized user account that has adatum.local as a UPN suffix will be configured to use a UPN suffix of onmicrosoft.com because adatum.local cannot be added to Office 365 as a custom domain.
Therefore, the reason that the five synchronized users have usernames with a UPN suffix of onmicrosoft.com is because their accounts were not configured to use the UPN suffix of contoso.com.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization

Community vote distribution
C (100%)

ctfalci Highly Voted 2 years, 1 month ago
Answer: C
Explanation
The question states that only five of the synchronized users have usernames that use a UPN suffix of onmicrosoft.com. Therefore the other 45 users have the correct UPN suffix. This tells us that the adatum.com domain has already been added to Office 365 as a custon domain.The forest is named adatum.local and uses adatum.com as a UPN suffix. User accounts in the domain will have adatum.local a their default UPN suffix. To use adatum.com as the UPN suffix, each user account will need to be configured to use adatum.com as the UPN suffix. Any synchronized user account that has adatum.local as a UPN suffix will be configured to use a UPN suffix of onmicrosoft.com because adatum.local cannot be added to Office 365 as a custom domain. Therefore, the reason that the five synchronized users have usernames with a UPN suffix of onmicrosoft.com is because their accounts were not configured to use the UP suffix of contoso.com.
upvoted 32 times

donathon 2 years ago
Yes, I can personally verify this because my environment has this issue. Once you change th UPN suffix to the domain that is verifie the issue will go away.
upvoted 7 times

DUSHIWORLD Highly Voted 2 years, 7 months ago
Correct Answer is C.
upvoted 7 times

LamestDuck 1 year, 10 months ago
They literally give it away with D, that's the problem but not the solution haha.
upvoted 2 times

SkullRage Most Recent 1 month, 1 week ago
Correct answer is C
upvoted 1 times

Moderator 2 months ago

Selected Answer: C

Still a valid question as of July 30th 2022.

upvoted 2 times

gaem 4 months, 1 week ago

Selected Answer: C

C correct answer

upvoted 2 times

jjong 1 year ago

in today's exam too. seems like whatever Ash473 encountered, i oso have.

upvoted 2 times

Ash473 1 year, 1 month ago

In today's exam

upvoted 2 times

syswiz85 1 year, 5 months ago

"The forest contains 500 users and uses adatum.com as a UPN suffix"

If users are synchronised to Azure AD and they don't have a custom domain name in their UPN, this means either a) the custom domai has not been set in Azure AND/OR b) the UPN suffix is incorrect on-premise. Seeing as the question is saying that five of the accounts a affected only, we can only assume the other 45 accounts have the correct UPNs with @adatum.com. Agreed that the wording of the question is confusing but C IS THE ONLY CORRECT ANSWER based on the above.

upvoted 2 times

jelley 1 year, 6 months ago

Team 'C', why you may ask:
For instance you have 2 domains on-prem "adatum.de" and "adatum.com", only 1 of those domains is actually added as a custom dom in o365 (the "adatum.com" one).
If you create any accounts on-prem with a UPN containing "adatum.com" they will replicate the UPN to o365 (when AAD has been setu With any accounts created On-prem containing the "adatum.de" domain they will turn to "adatum.onmicrosoft.com" as the domain is unknown.
Thus you should modify the UPN on-prem to achieve this goal

upvoted 3 times

estarisbourne 1 year, 8 months ago

should this not be A? We kind of need to address the adatum.local issue before we do anything else right? we should make it adatum.c if available so that it can be routable on the inter webs? I think those 5 users were the distraction to sie fundamentals

upvoted 1 times

bingomutant 1 year, 8 months ago

ignore above - there is no suggestion in the question that the remaining 450 users are to be synced - so from the wording you can only focus on the 5 - C.

upvoted 2 times

bingomutant 1 year, 8 months ago

this is a staged migration. The question tells you to make sure ALL users retain the on-prem address. So it is wrong to focus on the 5 incorrect ones in the current batch. You are told to stop this problem occurring for ALL users. A.

upvoted 2 times

mkoprivnj 1 year, 9 months ago

C for sure!

upvoted 3 times

Noppawat 1 year, 9 months ago

The question say "The forest contains 500 users and uses adatum.com as a UPN suffix."
And the question mentioned only 5 users accounts, not mention anything for the rest of accounts. Then I go for 'A', no change at on-premise, but change setting on Azure AD.

upvoted 1 times

ayyildizrdm 1 year, 9 months ago

correct

upvoted 1 times

scotths 1 year, 10 months ago

I also recon c. The 'a' upn suffix is the trick... It's not saying it's assign to all users. Just that's its there

upvoted 1 times

skadoura 1 year, 11 months ago

Answer C, because adatum.local AD domain cannot be added to Office 365 as a custom domain

upvoted 2 times

HOTSPOT -

Your company has a Microsoft Office 365 subscription that contains the groups shown in the following table.

Name	Members
Group1	User1, User2
Group2	User3

You have the licenses shown in the following table.

License	Included service	Assigned to
Microsoft 365	Microsoft Exchange Online	Group1
Microsoft 365	Microsoft SharePoint Online	User1, User2, User3

Another administrator removes User1 from Group1 and adds Group2 to Group1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 is licensed for SharePoint Online.	○	○
User2 is licensed for SharePoint Online.	○	○
User3 is licensed for SharePoint Online.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 is licensed for SharePoint Online.	○	○
User2 is licensed for SharePoint Online.	○	○
User3 is licensed for SharePoint Online.	○	○

User1, User2 and User3 have each been assigned a SharePoint license directly. Therefore, they are all licensed for SharePoint Online.

Changing the group memberships will only affect whether or not they are licensed for Exchange Online because the Exchange Online licenses are assigned to

Group1.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-licensing-whatis-azure-portal

mkoprivnj Highly Voted 1 year, 9 months ago

Y, Y, Y is correct. All users are licensed for SPO!

upvoted 11 times

init2winit Highly Voted 1 year, 5 months ago

Trick question, Y,Y,Y

upvoted 6 times

honeyman123 Most Recent 3 months, 3 weeks ago

Y, Y, Y is correct.

Just fyi: Nested groups are there as a new feature via dynamic membership rules. :)

upvoted 1 times

Bren 4 months, 1 week ago

Trying to get my head around this Im assuming by adding 1 group to another it stops both groups from operating thus group 1 and gr 2 is no longer working?

upvoted 1 times

Rudelke 3 months ago

None of that. Grup nesting does not work for licensing. What you do inside them (add, remove whatever) is irrelevant.

For this question Groups are just Microsoft shenanigans. If you look at actual questions groups are irrelevant as users are assigned licenses directly. They just messing with you.

upvoted 1 times

Nilz76 7 months ago

YYY. All 3 members have explicit membership. Group-based licensing currently does not support groups that contain other groups (nes groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues

upvoted 2 times

[Removed] 7 months, 4 weeks ago

That was a good tricky question, my mind was stuck on Exchange Online when they were talking about sharepont.
Just curious, if they were asking which users would be licensed for Exchange Online instead, would that just be User2, since User1 was removed from group 1 and Microsoft doesn't support nested groups for licensing? Does someone know that for sure?

upvoted 1 times

Durden871 7 months ago

I always start with the questions and then work backwards. Makes it easier to understand what to look for.

upvoted 1 times

extrankie 9 months ago

direct question with unnecessary information

upvoted 4 times

bingomutant 1 year, 9 months ago

The SPO licenses are assigned to users directly - not to Groups - so its YYY as removing user from group or nesting groups simply make no difference

upvoted 4 times

[Removed] 2 years, 2 months ago

Double question again

upvoted 6 times

Question #18 *Topic 2*

Your company has on-premises servers and a Microsoft Azure Active Directory (Azure AD) tenant.
Several months ago, the Azure AD Connect Health agent was installed on all the servers.
You review the health status of all the servers regularly.
Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure Active Directory Connect
Servers list.
You suspect that another administrator removed Server1 from the list.
You need to ensure that you can view the health status of Server1.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. From Windows PowerShell, run the Register-AzureADConnectHealthSyncAgent cmdlet.

B. From Azure Cloud shell, run the Connect-AzureAD cmdlet.

C. From Server1, change the Azure AD Connect Health services Startup type to Automatic (Delayed Start).

D. From Server1, change the Azure AD Connect Health services Startup type to Automatic.

E. From Server1, reinstall the Azure AD Connect Health agent.

Correct Answer: *AE*
question states that another administrator removed Server1 from the list. To view the health status of Server1, you need to re-register the AD Connect Health
Sync Agent. You can do this manually by running the Register-AzureADConnectHealthSyncAgent cmdlet. Alternatively, you can reinstall the Azure AD
Connect Health agent. The Azure AD Connect Health agent is registered as part of the installation.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

Community vote distribution
AE (100%)

ctfalci Highly Voted 2 years, 2 months ago
Answer: A E
Explanation
question states that another administrator removed Server1 from the list. To view the health status of Server1, you need to re-register AD Connect Health Sync Agent. You can do this manually by running theRegister-AzureADConnectHealthSyncAgentcmdlet. Alternativel you can reinstall the Azure AD Connect Health agent. The Azure AD Connect Health agent is registered as part of the installation.
upvoted 28 times

Jokke71 Highly Voted 2 years, 7 months ago
After deleting a service instance from Azure AD Connect Health service, if you want to start monitoring the same server again, uninstal reinstall, and register the Health Agent on that server.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations
upvoted 9 times

Moderator Most Recent 2 months ago
Selected Answer: AE
Still a valid question (July 30th 2022).
upvoted 2 times

mikl 1 month, 3 weeks ago
Thank you :)
upvoted 1 times

spg987 1 year, 1 month ago
It is my exam today
upvoted 5 times

mikl 1 year, 7 months ago

A and E seems correct.

upvoted 3 times

mkoprivnj 1 year, 9 months ago

A & E for sure!

upvoted 5 times

Tarek 2 years, 6 months ago

There are various reasons why AAD Connect Health monitoring agent doesn't work anymore. Potential reasons are:

Server has been deleted
Server has been marked as inactive in AAD Connect Data Retention Policy
There are two options to fix this problem

Install newest version of monitoring agent
Re-register monitoring agent
https://samilamppu.com/2019/04/15/how-to-fix-unmonitored-azure-ad-connect-health-status/

upvoted 4 times

VP11 2 years, 6 months ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

upvoted 3 times

Question #19 *Topic 2*

You have a Microsoft 365 subscription.
You suspect that several Microsoft Office 365 applications or services were recently updated.
You need to identify which applications or services were recently updated.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. From the Microsoft 365 admin center, review the Message center blade.

B. From the Office 365 Admin mobile app, review the messages.

C. From the Microsoft 365 admin center, review the Products blade.

D. From the Microsoft 365 admin center, review the Service health blade.

Correct Answer: *AB*
The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where
Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.
The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.
Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app?view=o365-worldwide

ctfalci Highly Voted 2 years, 2 months ago
Explanation
The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated i
the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenanc
or other important announcements.
The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.
Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide
https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app?view=o365-worldwide
upvoted 22 times

mkoprivnj Highly Voted 1 year, 9 months ago
A & B for sure!
upvoted 10 times

Matt789 Most Recent 1 year, 4 months ago
Definite exam question
upvoted 5 times

Puneet30 1 year, 4 months ago
Exam Q
upvoted 5 times

lucidgreen 1 year, 6 months ago
The mobile app part gave it away for me. Both those answers pointed to the same place.
upvoted 3 times

mikl 1 month, 3 weeks ago
Thank you :)
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a Microsoft Office 365 tenant.
You suspect that several Office 365 features were recently updated.
You need to view a list of the features that were recently updated in the tenant.
Solution: You use Monitoring and reports from the Compliance admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Depending on what your organization's Office 365 subscription includes, the Dashboard in Security & Compliance includes several widgets, such as Threat
Management Summary, Threat Protection Status, Global Weekly Threat Detections, Malware, etc. The Compliance admin center in Microsoft 365 contains much of the same information but also includes additional entries focusing on alerts, data insights.
The Monitoring and reports section from the Compliance admin center does not display a list of the features that were recently updated in the tenant so this solution does not meet the goal.
To meet the goal, you need to use Message center in the Microsoft 365 admin center.
Reference:
https://docs.microsoft.com/en-us/office365/admin/manage/message-center?view=o365-worldwide

Community vote distribution
B (100%)

Sh1rub10 4 months, 3 weeks ago
Selected Answer: B
Go to Message Center instead
upvoted 2 times

ProfesorF 3 months, 3 weeks ago
Thankyou
upvoted 1 times

DRAG DROP -

Your network contains an on-premises Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. The on-premises domain contains a server named Server1 that runs Windows Server 2016 and 200 client computers that run Windows 10.

Your company purchases a Microsoft 365 subscription.

On Server1, you create a file share named Share1. You extract the Microsoft Office Deployment Tool (ODT) to Share1.

You need to deploy Microsoft 365 Apps for enterprise and the French language pack from Share1 to the Windows 10 computers.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

- Create an XML configuration file.
- On Server1, run `setup.exe` and specify the /configure parameter.
- On every client computer, run `setup.exe` and specify the /configure parameter.
- On Server1, run `setup.exe` and specify the /packager parameter.
- On every client computer, run `setup.exe` and specify the /download parameter.
- On Server1, run `setup.exe` and specify the /download parameter.

Answer Area

Correct Answer:

Actions

- On Server1, run `setup.exe` and specify the /configure parameter.
- On Server1, run `setup.exe` and specify the /packager parameter.
- On every client computer, run `setup.exe` and specify the /download parameter.

Answer Area

- Create an XML configuration file.
- On Server1, run `setup.exe` and specify the /download parameter.
- On every client computer, run `setup.exe` and specify the /configure parameter.

Note:

Step 1: Create an XML configuration file with the source path and download path for the installation files.

Step 2: On the deployment server, run the ODT executable in download mode and with a reference to the XML configuration file.

Step 3: Create another XML configuration file with the source path to the installation files.

Step 4: On the client computer, run the ODT executable in configure mode and with a reference to the XML configuration file.

Reference:

https://docs.microsoft.com/en-us/DeployOffice/overview-of-the-office-2016-deployment-tool

nitvit610 Highly Voted 1 year, 4 months ago

The answer in the notes is correct but the screenshot is incorrect.
The XML configuration file must be created before running setup.exe /download on Server1.

Correct order is:
1. Create XML configuration file.
2. On Server1, run setup.exe /download with the configuration file.
3. On each client machine run setup.exe /configure with the configuration file.

upvoted 59 times

PDR 1 year, 3 months ago

why?
I dont think it matters really. You could do it first and it wouldnt matter but you dont have to. It is referenced as an input parameter when you run setup.exe so is pulled in then and used to set configuration choices during setup , it doesnt care when it was made. The setup.exe file download is the same regardless.

upvoted 1 times

FumerLaMoquette 1 year, 3 months ago

Nitvit610 is correct. The order is important because when you run setup.exe /download, you need to specify the XML file, which tells the setup utility which o365 apps you want to download. Refer to https://docs.microsoft.com/en-us/deployoffice/overview-office-deployment-tool#download-the-installation-files-for-microsoft-365-apps, step 2

upvoted 7 times

TechMinerUK 3 months, 3 weeks ago

I concur with nitvit610, Justin1 and FumerLaMoquette.

We use ODT to deploy from a server to client systems regularly and the order is:
1. Create XML configuration file.
2. On Server1, run setup.exe /download with the configuration file.
3. On each client machine run setup.exe /configure with the configuration file.

This is because in order to download the correct configuration of Office to be deployed the /download command must specify XML e.g. if you want to deploy BusinessApps

You then run the /configure comand on each client system which will pull the software from the share you have configured

upvoted 2 times

Justin1 Highly Voted 1 year, 3 months ago

The answer should be as follows:

1. Create and configure the XML file (specify the configuration you want)
2. Run setup.exe /download on the server (office will then be downloaded to the server)
3. Run setup.exe /configure on each client

There's no need to create a 2nd XML file as the notes claim, you will save all the files required on the shared drive so using the same XML file on the client machine that you used on the server will work because the client machines will have access to that file path.

upvoted 10 times

donb21 Most Recent 1 month, 3 weeks ago

answer should be creating a xml file > download > install in target server

upvoted 1 times

Cheekypoo 2 months ago

Was in my exam today 05/08/22

upvoted 1 times

Moderator 2 months ago

Still a valid question (July 30th 2022).

upvoted 1 times

charat 4 months, 1 week ago

On exam 05/22. Given answer is correct on this one.

upvoted 1 times

Stiobhan 4 months, 2 weeks ago

It might not matter what gets done first, but the Microsoft way is to create the XML config file first. So nitvit610 is correct and in an exa that is how you would sequence it. https://docs.microsoft.com/en-us/DeployOffice/overview-of-the-office-2016-deployment-tool

upvoted 1 times

Mthaher 5 months ago

https://docs.microsoft.com/en-us/deployoffice/overview-office-deployment-tool#install-microsoft-365-apps

upvoted 2 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

MartiFC 1 year, 2 months ago

nitvit610 Is correct your answer!

upvoted 2 times

momonoke 1 year, 2 months ago

I dont get it..
So many mistakes so far in examtopics.com..
As I failed the Exam last week, I begin to ask myself if Microsoft wanted it the same wrong way during the test..
Because I am absolutely sure, that I answered the Questions the correct way.

upvoted 1 times

leirbag 1 year, 1 month ago

yeah, dont study the answers.

upvoted 6 times

RAJULROS 1 year, 4 months ago

last week exam question

upvoted 4 times

Khazetul1 1 year, 4 months ago

Agree with nitvit610.

upvoted 6 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You add Device1 to an Active Directory group.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a
Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection, not an Active Directory Group. Therefore, this solution does not meet the requirements.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

VanillaWes Highly Voted 2 years, 10 months ago
I looked at the explanation and didn't notice anything about adding to a group. I also think just saying that ad it to a group is a very generic statement. I'm leaning towards this one being No.
upvoted 31 times

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection, not an Active Directory Group. Therefore, this solution does not meet the requirements.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable
upvoted 24 times

Eggsamine Most Recent 11 months, 2 weeks ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 4 times

SandyZ 1 year, 6 months ago
The answer should be NO.
I wrote the https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/ back in 2017 before we migrated our site msendpointmgr, I didn't write anything about adding a device to AD group for co-management. The old post is no longer valid anyway have changed the serial post to"how to configure PKI", not Co-management.
upvoted 3 times

Neshiri 1 year, 6 months ago
the answer is no
upvoted 1 times

lucidgreen 1 year, 7 months ago

Add it to a group, huh? I wish that's all I could do every time...
I think it's a typo.
upvoted 3 times

dwerdler 1 year, 8 months ago
Dead link: https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/
upvoted 1 times

alecrobertburns 1 year, 8 months ago
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune
upvoted 2 times

mkoprivnj 1 year, 9 months ago
B for sure!
upvoted 2 times

MSROCKS 1 year, 11 months ago
NO! most be the correct answer :)
upvoted 2 times

VTHAR 1 year, 11 months ago
The correct answer is NO. It doesn't meet the goal.
upvoted 2 times

FNyirongo 1 year, 12 months ago
The answer there should be no
upvoted 2 times

mkcom 2 years, 2 months ago
https://docs.microsoft.com/en-us/intune/enrollment/windows-enroll#enable-windows-10-automatic-enrollment
upvoted 1 times

Benoit_HAMET 2 years, 3 months ago
This should be no
There is no group relation when implementing co-management; only thing is if you want to have co-management enabled only for 1 device you need to define a device collection in SCCM - memberhsip can be a direct assignement, no need for group whatsoever
upvoted 1 times

skajam66 2 years, 3 months ago
There's a lot of vagueness in this question but I am going for answer B - no. My reasoning is this: if you assume 1) SCCM 1902, 2) Windo 10 1903, 3) the line "You configure a pilot for co-management" means that all the SCCM configuration has been done and 4) the line "Y add Device 1 to an Active Directory group" means that the group in question is the pilot group (aka collection) set up in SCCM, then all that is not enough. You also need to configure Intune wherein, as part of that configuration, the pilot group is specified for auto-enrollment.
As nothing is mentioned about the Intune side of the configuration, I am going in favour of answer B...
upvoted 1 times

Benjam 2 years, 3 months ago
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto enrolled
in Microsoft Intune. You need to add Device1 to the Device Collection, not an Active Directory Group. Answer is B
upvoted 2 times

Scooter454 1 year, 6 months ago
We done this. Key work is PILOT! The SCCM collection is membership based on a group. A is correct.
upvoted 1 times

PPPan 2 years, 5 months ago
IMO, the answer is no.
The scenario: “synced” to Microsoft Azure Active Directory (Azure AD).
Case 1 – Assume hybrid Azure AD
User in MDM user scope allows auto enroll device to Intune, actually, it is not add device to group.
Case 2- if not setup hybrid Azure AD, this case not for this scenario.
upvoted 1 times

Question #23 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a
Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

DJHASH786 Highly Voted 2 years, 9 months ago
The correct solution, so the answer is A
upvoted 40 times

VTHAR 1 year, 11 months ago
Agreed. The correct answer is A. YES It does meet the goal.
upvoted 3 times

VP11 2 years, 6 months ago
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable
upvoted 2 times

melatocaroca 1 year, 4 months ago
Automatic enrollment into Intune - Enables automatic client enrollment in Intune for existing Configuration Manager clients. This option allows you to enable co-management on a subset of clients to initially test co-management, and rollout co-management using a phased approach. If a device is unenrolled by the user, on the next evaluation of the policy, it will re-enroll.
upvoted 1 times

ctfalci 2 years, 2 months ago
Answer: A
Explanation
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable
upvoted 20 times

depmatic Highly Voted 2 years, 8 months ago
Answer is yes, indeed.
upvoted 7 times

Eggsamine Most Recent 11 months, 2 weeks ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 2 times

Bitek123 1 year, 7 months ago

Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are autoenrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

upvoted 1 times

mkoprivnj 1 year, 9 months ago

A for sure!

upvoted 2 times

MSROCKS 1 year, 11 months ago

This shoud be YES

upvoted 1 times

FNyirongo 1 year, 12 months ago

I can understand better on this Question than Q22

upvoted 1 times

Lynxy 2 years, 3 months ago

This question has split so many, so far I found both answers to be true?!

upvoted 1 times

STFN2019 2 years, 2 months ago

its a yes, previous question. as long as you have your devices in collection in SCCM then Intune will pick this up

upvoted 1 times

JeepScratch 2 years ago

Have no doubt, just carefully read: https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients.
And see step 4.
Automatic enrollment into Intune - Enables automatic client enrollment in Intune for existing Configuration Manager clients. This option allows you to enable co-management on a subset of clients to initially test co-management, and rollout co-management usir phased approach. If a device is unenrolled by the user, on the next evaluation of the policy, it will re-enroll.
Pilot - Only the Configuration Manager clients that are members of the Intune Auto Enrollment collection are automatically enrolled Intune.
All - Enable automatic enrollment for all Windows 10, version 1709 or later, clients.

upvoted 1 times

Benoit_HAMET 2 years, 3 months ago

This should be yes
piloting co-management is using device collection which can use direct assignmenet

upvoted 1 times

shark1 2 years, 3 months ago

Yes. maybe, anyone? https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/collections/create-collections

upvoted 2 times

Benjam 2 years, 3 months ago

Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto enrolled
in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune.
You will then be able to manage Device1 using Microsoft Intune.
Answer is A

upvoted 4 times

applejoe6 2 years, 4 months ago

There is no mention of enrollment for Intune. I am leaning towards "no"

Enable Windows 10 automatic enrollment
Automatic enrollment lets users enroll their Windows 10 devices in Intune. To enroll, users add their work account to their personally owned devices or join corporate-owned devices to Azure Active Directory. In the background, the device registers and joins Azure Activ

Directory. Once registered, the device is managed with Intune. https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#enable-windows-10-automatic-enrollment

upvoted 2 times

MichealAlex5 2 years, 4 months ago

The answer is A

upvoted 1 times

Tarek 2 years, 6 months ago

YES

Enable co-management starting in version 1906
https://docs.microsoft.com/en-us/configmgr/comanage/tutorial-co-manage-clients

upvoted 3 times

espnadmin 2 years, 7 months ago

This is for MS-101 exam. Stever is right. Configure co-management w/ Intune needs the computer in a group (Ad group)

upvoted 1 times

Jokke71 2 years, 7 months ago

This is a difficult one but I'm leaning towards Yes. There is much more to setting up co-management then what is mentioned here but assigning a collection as a Pilot group is part of it.
Reference: https://docs.microsoft.com/en-us/configmgr/comanage/tutorial-co-manage-clients

upvoted 2 times

Stever 2 years, 8 months ago

The answer is no. Doing this would not allow you to manage it from Config Manager and Intune, just Config Manager

upvoted 4 times

lucidgreen 1 year, 6 months ago

The current version of MECM allows you to use a collection to auto-enroll devices in Intune once co-management is configured.
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You create a device configuration profile from the Intune admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a
Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection.
You do not need to create a device configuration profile from the Intune admin center. Therefore, this solution does not meet the requirements.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection.
You do not need to create a device Configuration profile from the Intune admin
center. Therefore, this solution does not meet the requirements.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable
upvoted 8 times

Eggsamine Most Recent 11 months, 2 weeks ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 2 times

junior6995 1 year ago
Did someone get this question on MS-100? It feels like this question should be in MS-101 instead
upvoted 2 times

Turak64 1 year, 1 month ago
This feels like it should be a question for MS-101...
upvoted 4 times

adaniel89 1 year, 6 months ago
To manage the device on intune, you need to enroll the device
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll
Answer is no
upvoted 3 times

mkoprivnj 1 year, 9 months ago
B for sure!

upvoted 4 times

gardist 2 years ago

add Device1 to an active Directory Groupe will meet the goal.

upvoted 1 times

Takloy 1 year, 8 months ago

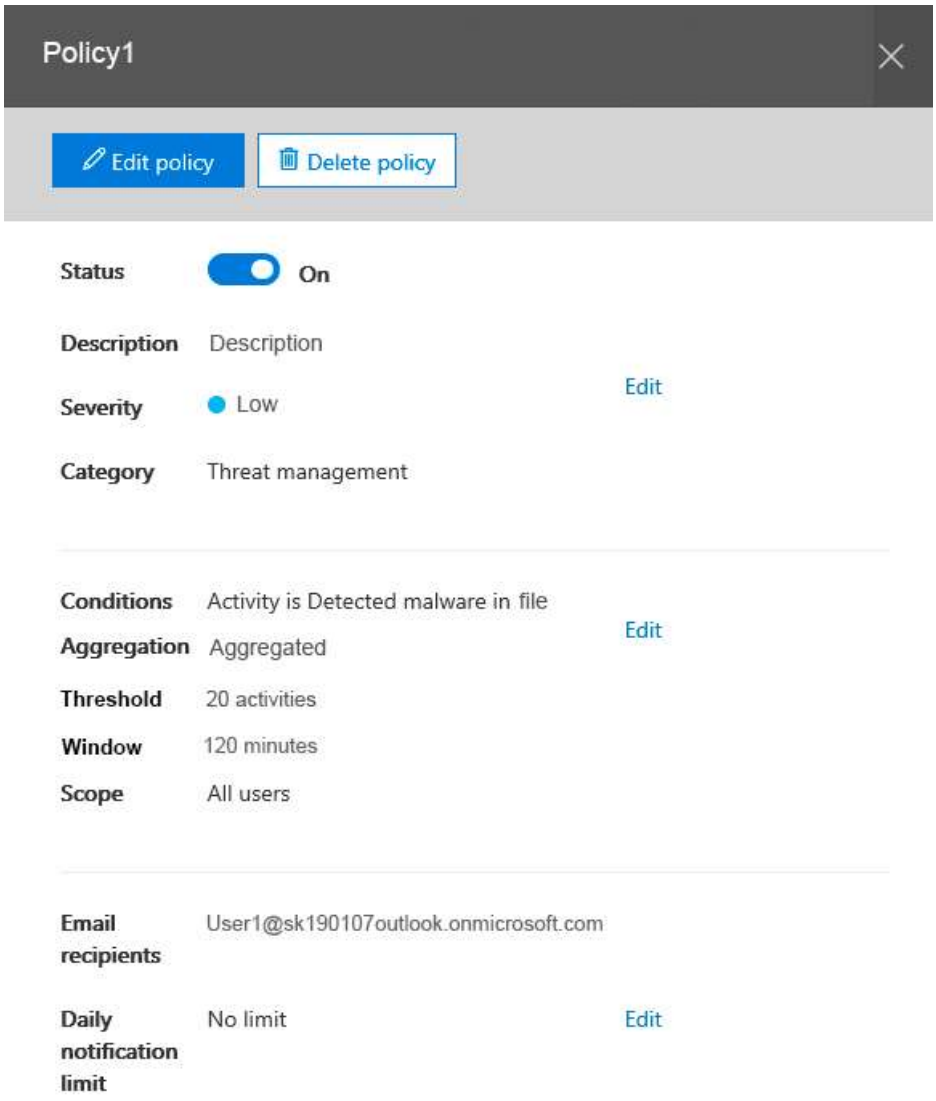
add to device collection

upvoted 7 times

HOTSPOT -

You have a Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

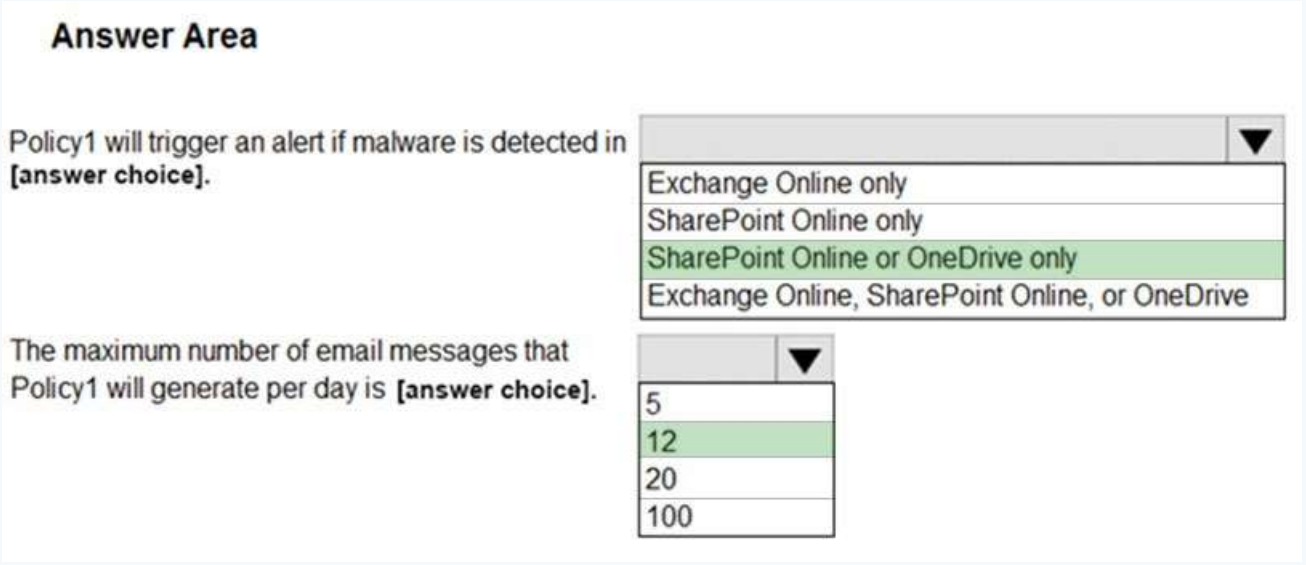
Policy1 will trigger an alert if malware is detected in **[answer choice]**.

- Exchange Online only
- SharePoint Online only
- SharePoint Online or OneDrive only
- Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is **[answer choice]**.

- 5
- 12
- 20
- 100

Correct Answer:



The 'Activity is' setting is configured as 'Detected malware in file'. This setting means the policy is applied to files stored in SharePoint or OneDrive.

The Aggregation settings has a 120 minute window. This means that if there 20 detections in 120 minutes, an email will be generated.

Therefore, the maximum number of emails generated in 24 hours is 12.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

itmp Highly Voted 2 years, 4 months ago

Pay attention, similar question in multiple MS exams.

1.There are to distinct activities you can chose from:
- Detected malware in an email message (ExchangeOnline)
- Detected malware in file (OneDrive & SharePoint)

2.The policy triggers when there are 20 activities within 120min (2hours)
So every 2hours, the policy checks and if there are more than 20 activities, it sends 1 alert.
Since we have 24hours/day, the policy can send a maximum of 1alert/2hours or 12alerts/24hours.

Answer1 = SharePoint & OneDrive only.
Answer2 = 12.

upvoted 105 times

Moji1 Highly Voted 2 years, 9 months ago

I think the answer is not correct because when you select "Detect malware in file", you will see the explanation which says "Office 365 detected malware in either a SharePoint or OneDrive file". If you want a policy which protect Exchange, I think we need to select "Detec malware in an email message"

upvoted 44 times

zeeess99 2 years, 7 months ago

This explaination is correct

upvoted 2 times

Sachie_Brown 2 years, 5 months ago

I agree with this.

upvoted 2 times

praveen97 2 years, 3 months ago

Agree. "Detect malware in file" alert activity is for SharePoint, OneDrive and MS Teams files only.

upvoted 2 times

AADapson 1 year, 5 months ago

This particular activity only covers for SharePoint and OneDrive. There is another option that covers for Email

upvoted 2 times

melatocaroca 1 year, 3 months ago

They do not mention the plans that they have, so with normal plans you can set sharepoint and one drive

https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-attachments-policies?view=o365-worldwide
https://www.nakivo.com/microsoft-office-365-backup/microsoft-office-365-advanced-threat-protection-overview/
upvoted 2 times

FallenShroud1 Most Recent 3 months ago
This question is still relevant, It was on my MS 101 test in 6/22
upvoted 1 times

trexar 6 months ago
Actually they have on Daily Notification Limit:
1,5,10,25,50,100,150,200 or no limit
upvoted 1 times

Jcbrow27 10 months, 4 weeks ago
i tested and the answer is correct only apply for SharePoint and OneDrive
upvoted 2 times

fofo1960 12 months ago
For those who are not good at math
in 24 Hours there are 1440 Minutes
The calculation is 1440 / 120 =12
upvoted 5 times

lengySK 1 year, 1 month ago
correct
upvoted 1 times

[Removed] 1 year, 3 months ago
OneDrive and SharePoint
https://www.stephenhackers.co.uk/office-365-alert-policy-detected-malware-in-file-onedrive-or-sharepoint/
upvoted 1 times

PattiD 1 year, 9 months ago
Copied from Sec&Compliance Portal: "Office 365 detected malware in either a SharePoint or OneDrive file" - So SharePoint & OneDrive MSGS.
upvoted 6 times

lucidgreen 1 year, 6 months ago
If that's the case, SharePoint and OneDrive make sense.
upvoted 1 times

mkoprivnj 1 year, 9 months ago
4 & 2 for sure!
upvoted 1 times

mkoprivnj 1 year, 9 months ago
(24*60)/120=12
upvoted 1 times

csribeiro12 1 year, 10 months ago
Resposta correta é SharePoint e OneDrive
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide
upvoted 2 times

scottims 1 year, 11 months ago
Sharepoint or OneDrive only
This is taken from the policy creation wizard..

Choose an activity, conditions and when to trigger the alert
You can only choose one activity but you can add conditions to refine what we'll detect.
What do you want to alert on?

* Activity is
Detected malware in file
Office 365 detected malware in either a SharePoint or OneDrive file.
upvoted 4 times

kev001 1 year, 10 months ago
below message appears when creating the policy as scottims has pasted above.
Office 365 detected malware in either a SharePoint or OneDrive file.
upvoted 2 times

ctfalci 2 years, 2 months ago

SharePoint / One Drive only
12
100% Confirmed!

upvoted 14 times

rambo1990 2 years, 2 months ago

HI Are these questions related to MS-100? I do not see these in the study guide. Please advice. Thanks,

upvoted 2 times

VTHAR 1 year, 11 months ago

It does NOT because it was in my MS-101 exam and the correct answer is SharePoint/OneDrive ONLY and 12.

upvoted 2 times

Benjam 2 years, 3 months ago

The `Activity is' setting is configured as `Detected malware in file'. This setting means the policy is applied to files stored in SharePoint or OneDrive.
The Aggregation settings has a 120 minute window. This means that if there 20 detections in 120 minutes, an email will be generated. Therefore, the maximum number of emails generated in 24 hours is 12.

upvoted 2 times

PPPan 2 years, 5 months ago

Detect malware in file -> Office 365 detected malware in either a SharePoint or OneDrive file.
Windows 120 mins -> max 12 notification per day

upvoted 3 times

Cabelo 2 years, 5 months ago

The maximum number of email messages notifications that is possible for this question is 100, I confirmed this in my tenant. I can cho
1 5 10 25 50 100 150 200 and unlimited.

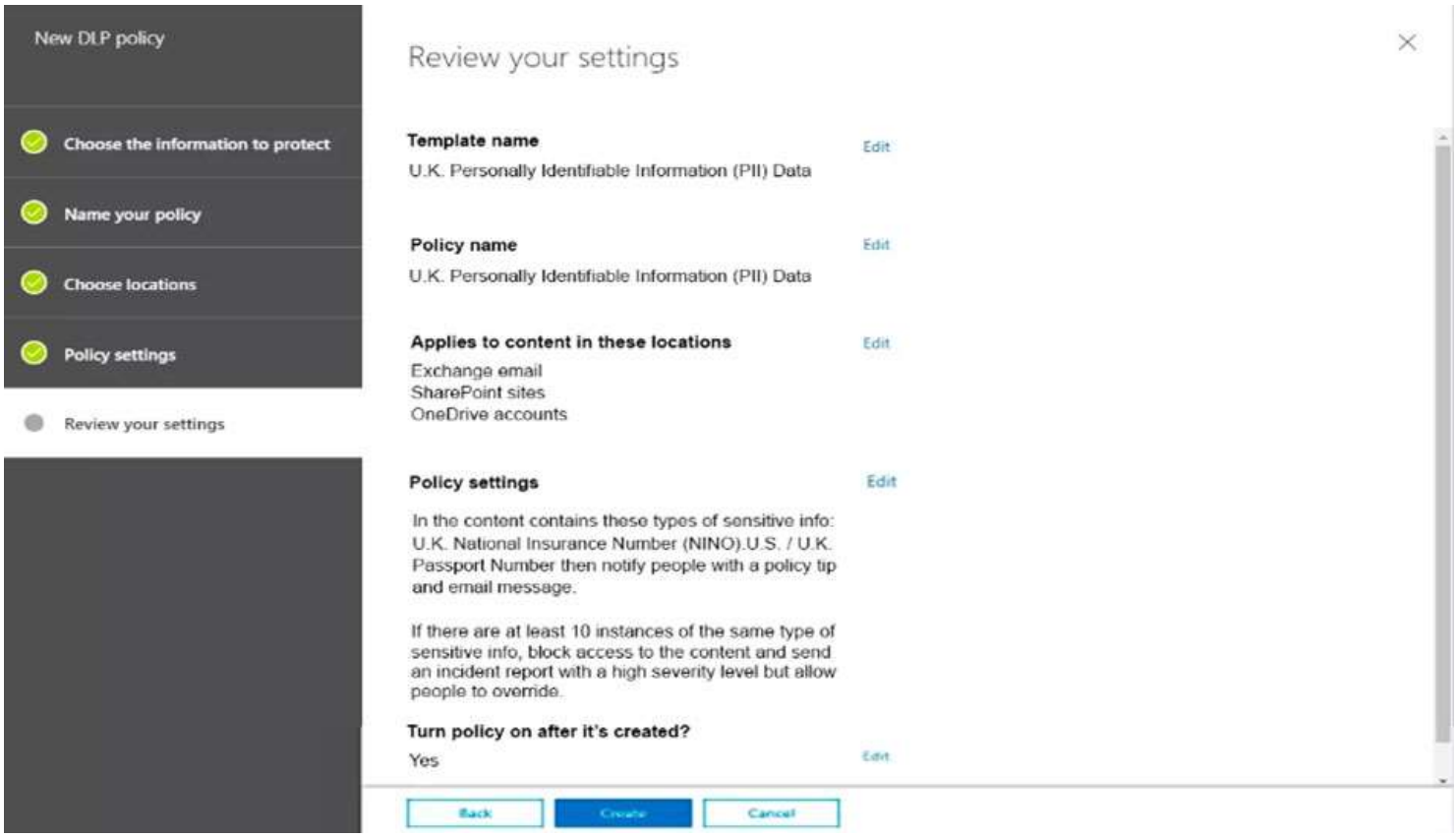
upvoted 1 times

HOTSPOT -

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based in the information presented in the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [**answer choice**].

- allowed
- blocked without warning
- blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [**answer choice**].

- allowed
- blocked without warning
- blocked, but the user can override the policy

Correct Answer:

Answer Area

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [**answer choice**].

- allowed
- blocked without warning
- blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [**answer choice**].

- allowed
- blocked without warning
- blocked, but the user can override the policy

The text in the Policy Settings section of the exhibit explains what will happen.

If a user sends between 1 and 10 instances of the sensitive info (passport number), then a notification email and will be sent to the user and a policy tip will be displayed. The email will not be blocked though. Therefore, it will be allowed.
If a user sends more than 10 instances of the sensitive info (passport number), the email will be blocked and a high-severity alert generated. However, the user can override the block.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

airairo Highly Voted 1 year, 4 months ago
The given answers are correct.
upvoted 15 times

Eggsamine Most Recent 11 months, 2 weeks ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 3 times

InformationOverload 1 year, 1 month ago
If you choose the email notification and policy tip, it can allow users to override a rule by reporting a false positive or providing a busin justification
upvoted 1 times

momonoke 1 year, 2 months ago
If a user sends more than 10 instances of the sensitive info (passport number), the email will be blocked and a high-severity alert generated.

Yes, but the note doesn't explain why..
The setting states, that the access will be blocked, if we have "..more than 10 instances of the sensitive info..".
But why is the user able to override it. That makes this setting and its description senseless.
upvoted 2 times

TechMinerUK 3 months, 3 weeks ago
I can only speak from personal experience with DLP policies however I think the second statement is a bit muddled as the policy tip the element which can be over-ridden however it sounds like what is being configured is as follows:
1. Policy tip shows without any blocking
2. Policy tip shows in block mode but user can over-ride by providing a justification.

It seems the question wording is just a bit unusual in how it's conveying this however the functionality is there as it is similar to the overriding for document labelling
upvoted 1 times

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant.

Your company implements Windows Information Protection (WIP).

You need to modify which users and applications are affected by WIP.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To modify which users are affected by WIP, configure: [▼]
- The Azure AD app registration
- The Azure AD device settings
- The MAM User scope
- The mobile device management (MDM) authority

To modify which applications are affected by WIP, configure: [▼]
- App configuration policies
- App protection policies
- Compliance policies
- Device configuration profiles

Correct Answer:

Answer Area

To modify which users are affected by WIP, configure: [▼]
- The Azure AD app registration
- The Azure AD device settings
- The MAM User scope
- The mobile device management (MDM) authority

To modify which applications are affected by WIP, configure: [▼]
- App configuration policies
- App protection policies
- Compliance policies
- Device configuration profiles

Microsoft Intune has an easy way to create and deploy a Windows Information Protection (WIP) policy. You can choose which apps to protect, the level of protection, and how to find enterprise data on the network. The devices can be fully managed by Mobile Device Management (MDM), or managed by Mobile

Application Management (MAM), where Intune manages only the apps on a user's personal device.

The MAM User scope determines which users are affected by WIP. App protection policies are used to configure which applications are affected by WIP.

Reference:

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

syswiz85 Highly Voted 1 year, 5 months ago

I see nothing in the skills measured for this exam about WIP....

upvoted 11 times

Razuli 1 year, 4 months ago

And the training Microsoft provide doesn't include all the stuff covered but I do remember this in the exam

upvoted 6 times

Turak64 1 year, 1 month ago

This happens a lot with MS exams and it drives me nuts. This really should be a question for the MS-101 exam!

upvoted 5 times

fofo1960 12 months ago

There are alot of Exchange Online questions also here

upvoted 1 times

PlumpyTumbler Highly Voted 1 year, 4 months ago

MS-101 question.

upvoted 6 times

mikl Most Recent 1 month, 3 weeks ago

Beside the fact that this might belong to MS-101, I do believe its correct answers.

upvoted 1 times

Eggsamine 11 months, 2 weeks ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 1 times

Question #28 *Topic 2*

You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.
You need to prevent the users from bypassing the DLP policy.
What should you configure?

A. actions

B. exceptions

C. incident reports

D. user overrides

Correct Answer: *D*
A DLP policy can be configured to allow users to override a policy tip and report a false positive.
You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and
Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

Community vote distribution
D (100%)

ctfalci Highly Voted 2 years, 2 months ago
Answer: D
Explanation
A DLP policy can be configured to allow users to override a policy tip and report a false positive. You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sens information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library th allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook Excel, PowerPoint, and Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies
upvoted 20 times

kevinmwest2112 Highly Voted 2 years ago
MS-101 question
upvoted 8 times

VTHAR 1 year, 11 months ago
Yes ... It is.
upvoted 3 times

mmraouf Most Recent 1 week, 3 days ago
Starting in July 2022, Microsoft is deprecating Windows Information Protection (WIP). Microsoft will continue to support WIP on suppor versions of Windows. New versions of Windows won't include new capabilities for WIP, and it won't be supported in future versions of Windows. For more information, see Announcing sunset of Windows Information Protection.
upvoted 1 times

gaem 4 months, 2 weeks ago
Selected Answer: D
User Override

upvoted 1 times

Eggsamine 11 months, 2 weeks ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 2 times

B1G_B3N 1 year, 7 months ago

The answer is an exception, why would creating an over ride policy stop a user from overriding or bypassing a DLP. The whole point of override is to ALLOW them to do it not DENY them.

upvoted 1 times

Chipper 1 year, 3 months ago

I don't think "override" just means it just allows users to over ride it. I think it means that they can be allowed to over ride the policy also make is so the user cannot over ride it to send the content.

upvoted 1 times

mkoprivnj 1 year, 9 months ago

D for sure!

upvoted 3 times

HenriksDisciple 6 months ago

are all your 660 comments "___ for sure!"? Your comments don't really add anything except your opinion.

upvoted 3 times

Noppawat 1 year, 9 months ago

Answer: D
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide
See "User overrides" setting in a demonstration picture.

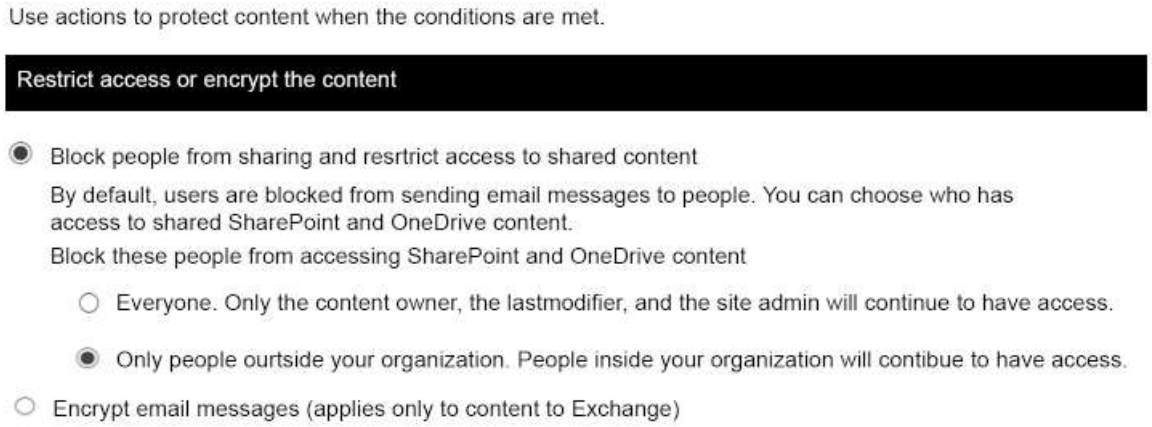
upvoted 4 times

Larency 2 years, 2 months ago

exception

upvoted 2 times

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.
Policy1 is configured as shown in the exhibit.



You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.
What should you configure?

A. an action

B. a group

C. a condition

D. an exception

Correct Answer: *D*
You need to add an exception. In the Advanced Settings of the DLP policy, you can add a rule to configure the Conditions and Actions. There is also an 'Add
Exception' button. This gives you several options that you can select as the exception. One of the options is 'except when recipient domain is'. You need to select that option and enter the domain name contoso.com.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work

birzorirko Highly Voted 1 year, 4 months ago
D is the way.
upvoted 9 times

zaicnupagadi 6 months ago
They want the D
upvoted 6 times

Landy360 Highly Voted 1 year ago
"Only people ourtside of your organization..."
upvoted 5 times

Eggsamine Most Recent 11 months, 2 weeks ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 1 times

Eggsamine 11 months, 2 weeks ago
DLP is on MS-101 and not MS-100 is it not? There have also been some questions for WIP which again is MS-101. Can these questions f
MS-101 be removed from this dump or are these questions actually coming up on the exam?
upvoted 3 times

TechMinerUK 3 months, 3 weeks ago

Microsoft do have a habit of throwing in a few curve balls into exams from past experience where you would expect them to be in different exams. It's best to be aware of them "Just in case"

upvoted 2 times

manwithplan 1 month, 3 weeks ago

This is correct. When I did the MD100 exam, there were quite a few MD101 questions in the exam.

upvoted 1 times

Your company uses on-premises Windows Server File Classification Infrastructure 9FCI). Some documents on the on-premises file servers are classifies as
Confidential.
You migrate the files from the on-premises file servers to Microsoft SharePoint Online.
You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded files based on the Confidential classification.
What should you do first?

A. From the SharePoint admin center, create a managed property.

B. From the SharePoint admin center, configure hybrid search.

C. From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

D. From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.

Correct Answer: *A*
Your organization might use Windows Server FCI to identify documents with personally identifiable information (PII) such as social security numbers, and then classify the document by setting the Personally Identifiable Information property to High, Moderate, Low, Public, or Not PII based on the type and number of occurrences of PII found in the document. In Office 365, you can create a DLP policy that identifies documents that have that property set to specific values, such as High and Medium, and then takes an action such as blocking access to those files.
Before you can use a Windows Server FCI property or other property in a DLP policy, you need to create a managed property in the SharePoint admin center.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties

SMHH Highly Voted 2 years, 8 months ago
Correct answer is A
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties#before-you-create-t
dlp-policy
upvoted 56 times

WoneSix 2 years, 7 months ago
SMHH is right - from his link, "Before you can use a Windows Server FCI property or other property in a DLP policy, you need to crea
managed property in the SharePoint admin center."
upvoted 7 times

praveen97 2 years, 3 months ago
Agree with SMHH and the article clearly says that Managed property has to be added to SharePoint Search schema in SP Admin Cer
upvoted 3 times

VTHAR 1 year, 11 months ago
Agreed! Correct answer is A.
upvoted 5 times

Ama100 Highly Voted 2 years, 6 months ago
A is the correct answer:

Before you can use a Windows Server FCI property or other property in a DLP policy, you need to create a managed property in the SharePoint admin center. Here's why.

In SharePoint Online and OneDrive for Business, the search index is built up by crawling the content on your sites. The crawler picks up content and metadata from the documents in the form of crawled properties. The search schema helps the crawler decide what conten and metadata to pick up. Examples of metadata are the author and the title of a document. However, to get the content and metadata from the documents into the search index, the crawled properties must be mapped to managed properties. Only managed properties kept in the index. For example, a crawled property related to author is mapped to a managed property related to author.

https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o365-worldwic
upvoted 18 times

ctfalci 2 years, 2 months ago

Answer: A
Explanation
Your organization might use Windows Server FCI to identify documents with personally identifiable information (PII) such as social security numbers, and then classify the document by setting the Personally Identifiable Information property to High, Moderate, Lo Public, or Not PII based on the type and number of occurrences of PII found in the document. In Office 365, you can create a DLP po that identifies documents that have that property set to specific values, such as High and Medium, and then takes an action such as blocking access to those files.
Before you can use a Windows Server FCI property or other property in a DLP policy, you need to create a managed property in the SharePoint admin center.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties
upvoted 7 times

charat Most Recent 4 months, 2 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o365-worldwic

Here's a working link for the MS article
upvoted 1 times

Durden871 7 months ago
This cannot possibly be an MS-100 question.
upvoted 1 times

Eggsamine 11 months, 2 weeks ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 3 times

Eggsamine 11 months, 2 weeks ago
DLP is on MS-101 and not MS-100 is it not? There have also been some questions for WIP which again is MS-101. Can these questions f MS-101 be removed from this dump or are these questions actually coming up on the exam?
upvoted 1 times

Durden871 7 months ago
On One hand, it should theoretically make the 101 easier since we're going through these questions now, but on the other, it's push back me taking the 100 and honestly, it's creating frustration because I study the material as much as I can and use these as a guideline as to where I am. Getting questions that don't seem relevant hurts the confidence of me scheduling it.
upvoted 1 times

Duyons 1 year, 7 months ago
MS-101 question
upvoted 7 times

mkoprivnj 1 year, 9 months ago
A for sure!
upvoted 3 times

k2kimmy 1 year, 10 months ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o365-worldwide#before-you-create-the-dlp-policy

to ensure that you apply DLP policy one needs to create a managd property first so i think its A
upvoted 1 times

AADapson 1 year, 11 months ago
File as been migrated to SharePoint online, configuring manage properties SPO Admin center is not going to apply DLP.

DLP configured from Security Compliance is going to apply to all SPO sites and files
upvoted 1 times

Jayatheerthan 1 year, 11 months ago
to be specific "implement data loss prevention (DLP) policies for the uploaded files based on the classification"
upvoted 1 times

Jayatheerthan 1 year, 11 months ago
It says" uploaded files" . This means they have already have Managed property created and uploaded the content.
upvoted 2 times

ctfalci 2 years, 2 months ago
Answer: A
Explanation
Your organization might use Windows Server FCI to identify documents with personally identifiable information (PII) such as social

security numbers, and then classify the document by setting the Personally Identifiable Information property to High, Moderate, Low, Public, or Not PII based on the type and number of occurrences of PII found in the document. In Office 365, you can create a DLP policy that identifies documents that have that property set to specific values, such as High and Medium, and then takes an action such as blocking access to those files.
Before you can use a Windows Server FCI property or other property in a DLP policy, you need to create a managed property in the SharePoint admin center.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-orother-properties

upvoted 3 times

shark1 2 years, 3 months ago

It's FCI, it's reupload, it's Managed Property. https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o365-worldwide#before-you-create-the-dlp-policy

upvoted 1 times

Raj2020 2 years, 3 months ago

Answer is : A
Refer Ama100 comments and https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o365-worldwide#create-a-dlp-policy-that-uses-an-fci-property-or-other-property

upvoted 2 times

hmirza 2 years, 3 months ago

Based on the following I believe C is correct

https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o365-worldwide#create-a-dlp-policy-that-uses-an-fci-property-or-other-property

upvoted 1 times

hitmk5 2 years, 3 months ago

In the link you provided: First, they follow the steps above to create a managed property in SharePoint Online, which maps to the crawled property created automatically from the FCI property.
Answer is: A

upvoted 3 times

kazaki 2 years, 3 months ago

The answer is C
https://docs.microsoft.com/en-us/powershell/module/exchange/new-dlpcompliancerule?view=exchange-ps

upvoted 1 times

Sonia33 2 years, 3 months ago

No, answer is A, you should FIRST create a managed property in Sharepoint Online and then, use New-Dlpcomplicancerule in PS because it is not supported in the portal.

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o36 worldwide

Read the section "Before you create the DLP policy".

upvoted 2 times

FaresJG 2 years, 3 months ago

This exchange online related not SharePoint !
U just have to fully read the link u posted to understand it.

upvoted 1 times

Josey001 1 year, 5 months ago

Udemy Practice exam for MS 100 has the answer as C: Other practice tests have the answer as A or alternatively C.For a novice, very confusing especially as just one or tow incorrect answer in the real exam could be difference between a PASS or FAIL.This is not the question/answer that differs with other practice tests: surely they must have the correct answers from the real exam. otherwise why are we here?

upvoted 1 times

Question #31 *Topic 2*

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You have three applications App1, App2, App3. The Apps use files that have the same file extensions.

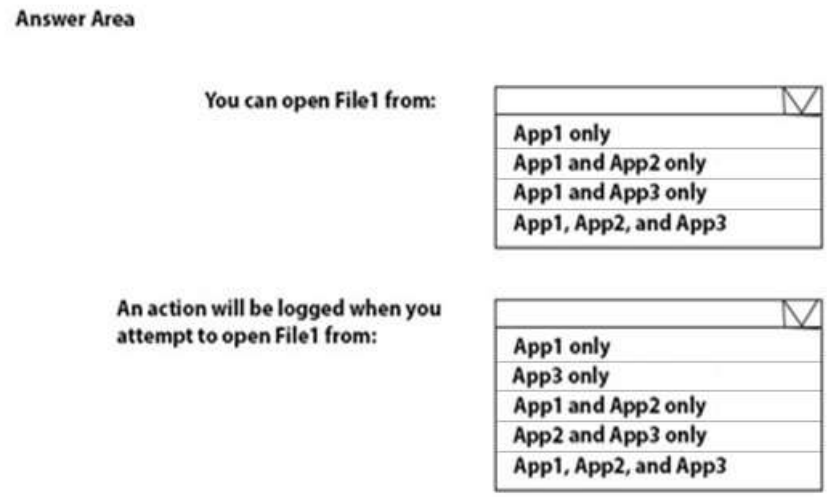
Your company uses Windows Information Protection (WIP). WIP has the following configurations:

- Windows Information Protection mode: Silent
- Protected apps: App1
- Exempt apps: App2

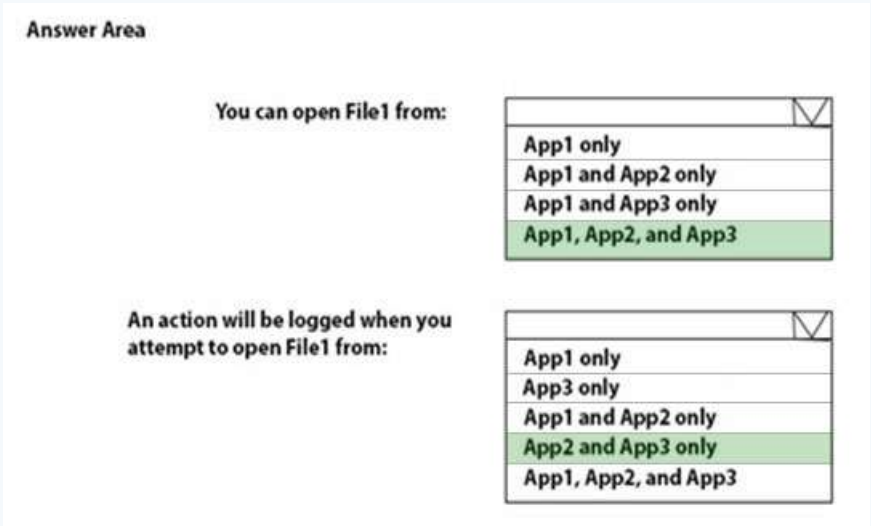
From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

Hot Area:



Correct Answer:



Exempt apps: These apps are exempt from this policy and can access corporate data without restrictions.

Windows Information Protection mode: Silent: WIP runs silently, logging inappropriate data sharing, without stopping anything that would've been prompted for employee interaction while in Allow overrides mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still stopped.

Reference:

https://docs.microsoft.com/en-us/intune/apps/windows-information-protection-policy-create https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

saasaa Highly Voted 2 years, 7 months ago

Silent mode detects and logs inappropriate actions, but doesn't block them.
SO, for the first selection, App1, App2 and App3 can be used to open the file.

Its scope doesn't include App1 because the File1 is created on App1.
Apps2 is also not included because it's exempted.
So, the attempt to open the file, which is to be logged, is only the one from App3.

This is mu understanding. Please correct me if I'm wrong.
upvoted 67 times

STFN2019 2 years, 2 months ago
Perfect. Box1: all apps, Box2: App3 only
upvoted 16 times

Rosco 2 years, 4 months ago
I think everyone is wrong. I believe inappropriate actions "sharing data" ie. cut and paste are allowed but logged in Silent. Opening i an unprotected app would be an unallowed action and would still be blocked in silent mode I believe. no?
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/protect-enterprise-dat using-wip
upvoted 6 times

sailerjerry Highly Voted 2 years, 8 months ago
You can open an app from app1,2 or 3 as it is in silent mode. This will only log, not alert or block user.
Log will be generated on app 3 only. It wont log on protected app or exempt app.
upvoted 27 times

donb21 Most Recent 1 month, 3 weeks ago
Box 1 should be 1,2,3 and Box2 should be only App3
upvoted 2 times

DenisRossi 3 months, 3 weeks ago
MS-101 question
upvoted 2 times

Eggsamine 11 months, 2 weeks ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 3 times

MomoLomo 1 year, 1 month ago
So user can open file from 1.2.3 cause it's in silent mode and agree on that
as for the logs
https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create

When working with WIP-enabled apps and WIP-unknown apps, we recommend that you start with Silent or Allow Overrides while verif with a small group that you have the right apps on your protected apps list. After you're done, you can change to your final enforceme policy, Block.

WIP runs silently, logging inappropriate data sharing, without blocking anything that would have been prompted for employee interac while in Allow Override mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, still stopped.

it says to make sure you have the right apps on your protect list and silent logs contain inappropriate data sharing

which means apps that are blocked and unknown aka not on the protect list
upvoted 2 times

Aysan 1 year, 4 months ago
Ms-101question
upvoted 4 times

Mr01z0 1 year, 4 months ago
Per Microsoft:

"Silent. Windows Information Protection runs silently. It logs inappropriate data sharing without blocking anything that would've prompted employee interaction in Allow Overrides mode. Unallowed actions, like apps trying to access a network resource or Windows Information Protection protected data, are allowed but audited. Silent mode is good choice for more open IT environments or where la groups of users, like testers or application developers, have legitimate reasons to perform actions that might be blocked under other circumstances. Silent mode is also good to use when an organization is thinking about implementing Allow Overrides or Hide Override mode, because the event log will offer information about the number of overridden or blocked events that implementing Windows Information Protection will cause."

this phrase "the event log will offer information about the number of overridden or blocked events" suggests that the exempt app doe not get logged at all.

Only events where a block would occur or a user overrides the block will be logged.
upvoted 3 times

init2winit 1 year, 5 months ago

is this on the test?
upvoted 1 times

YounesDump 1 year, 6 months ago
i think that skajam66 is right ;
upvoted 1 times

Parvezg 1 year, 7 months ago
I believe it should be only App1 and App2 can open because App3 is out of protection/exemption so not allowed to open any file. And, will be generated for such type of actions for App1 only because that is the protected app.
upvoted 2 times

Duyons 1 year, 7 months ago
MS-101 question - MS-100 does not cover WIP
upvoted 6 times

Turak64 1 year, 1 month ago
it shoudn't, but this is a MS exam... they tend to pull this sort of thing
upvoted 1 times

Takloy 1 year, 9 months ago
so what's the correct answer?
upvoted 1 times

mkoprivnj 1 year, 9 months ago
1, 2, 3 & 2, 3.
upvoted 4 times

palani75 1 year, 11 months ago
You Can open File1 from App1,App2, and App3
An action will be logged when you attempt to open File1 from: App3 only

WIP Silent mode will not block any action but will log inappropriate data sharing, giving you the opportunity to monitor your WIP enab apps but also apps you did not add to your WIP policy.
upvoted 10 times

Jayatheerthan 1 year, 11 months ago
Silent mode. The Windows Information Protection-protected work files can be moved or copied to the user's personal local OneDrive sy folder, the files will sync without issue, and an audit log event will be generated.
upvoted 1 times

LucWave 2 years ago
WIP runs silently, logging inappropriate data sharing, without stopping anything that would've been prompted for employee interactio while in Allow overrides mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, still stopped.
Unallowed actions in silent are blocked so I think App 3 can't access the file.

For the log, i'm not sure that events for "exempt app" are logged so if someone can provide a link with the answer, it would be greatly appreciated!
upvoted 1 times

Your company has 10 offices.

The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.

You discover that one of the offices has the following:

- Computers that have several preinstalled applications
- Computers that use nonstandard computer names
- Computers that have Windows 10 preinstalled
- Computers that are in a workgroup

You must configure the computers to meet the following corporate requirements:

- All the computers must be joined to the domain.
- All the computers must have computer names that use a prefix of CONTOSO.
- All the computers must only have approved corporate applications installed.

You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.

A. a provisioning package

B. wipe and load refresh

C. Windows Autopilot

D. an in-place upgrade

Correct Answer: *A*

By using a provisioning package, IT administrators can create a self-contained package that contains all of the configuration, settings, and apps that need to be applied to a device.

Incorrect Answers:

C: With Windows Autopilot the user can set up pre-configured devices without the need consult their IT administrator.

D: Use the In-Place Upgrade option when you want to keep all (or at least most) existing applications.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

subbuhotmail Highly Voted 1 year, 2 months ago

In this question, they no where mentioned about AAD. So its all on premises and it wont be Windows Autopilot. Answer will be a PPKG package which is a provisioning package only.

upvoted 5 times

PDR 1 year, 2 months ago

exactly this , doesnt even mention if they have AAD, Intune at all . Specifically says Join AD and not AAD , so to use autopilot would require setting up a 365 tenant, licencing, then setting up co-management , then AD joining, having the AD Device records sync to A to Hybrid Join and Intune autoenroll etc etc . ALOT more work than Provisioning package solution (even if it is ultimately the better solution, it is not correct in this question)

upvoted 4 times

PDR 1 year, 2 months ago

and by not correct in this question, I mean Autopilot is not correct

upvoted 2 times

BoxGhost Most Recent 5 months, 2 weeks ago

I was sure this was autopilot but then realised one of the points is some machines are joined to a workgroup. Therefore A is the only answer that can work in all of those scenarios.

upvoted 2 times

Eggsamine 11 months, 2 weeks ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 1 times

stoneface 9 months ago

You've asking the same question. So, in this case this is completely related to MS-100.
upvoted 2 times

xofowi5140 11 months, 2 weeks ago
https://www.examtopics.com/discussions/microsoft/view/25336-exam-ms-101-topic-10-question-2-discussion/

https://www.examtopics.com/discussions/microsoft/view/15621-exam-ms-100-topic-1-question-32-discussion/
upvoted 1 times

lengySK 1 year, 1 month ago
It looks like a question from MD100
A: https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages
upvoted 4 times

Azuz 1 year, 2 months ago
A
Windows provisioning makes it easy for IT administrators to configure end-user devices without imaging. Using Windows provisioning, IT administrator can easily specify desired configuration and settings required to enroll the devices into management and then apply t configuration to target devices in a matter of minutes. It is best suited for small- to medium-sized businesses with deployments that ra from tens to a few hundred computers.

A provisioning package (.ppkg) is a container for a collection of configuration settings. With Windows 10, you can create provisioning packages that let you quickly and efficiently configure a device without having to install a new image.

Provisioning packages are simple enough that with a short set of written instructions, a student or non-technical employee can use the to configure their device. This can result in a significant reduction in the time required to configure multiple devices in your organizatio
upvoted 2 times

goape 1 year, 3 months ago
100% A
upvoted 3 times

JordanJammer 1 year, 3 months ago
It's a little unclear from the comments what the true answer is. Is the given answer of A correct?
upvoted 2 times

melatocaroca 1 year, 4 months ago
Correct Answer: C

Answer A: Wrong, can be used to deploy but will take longer time than autopilot, Autopilot with Lenovo, HP or Dell will bring you the corporate image and customer BIOS, so with an Microsoft 365 subscription and one Azure Tenant you will need just login

package needs to be downloaded and deployed, Computers that are in a workgroup, Windows 10 preinstalled, no version, preinstalled applications solution to redeploy the computers

A provisioning package contains specific configurations/settings and assets that can be provided through a removable media or simply downloaded to the device.
When multiple provisioning packages are available for device provisioning, the combination of package owner type and package rank l defined in the package manifest is used to resolve setting conflicts. The pre-defined package owner types are listed below in the order lowest to highest owner type precedence:

1. Microsoft
2. Silicon Vendor
3. OEM
4. System Integrator
5. Mobile Operator
6. IT Admin

upvoted 2 times

nitvit610 1 year, 4 months ago
Surely C Autopilot is an option?
You can select what software is deployed, standard naming convention with CONTOSO-xxxxxxx, and join to domain with hybrid AD join
upvoted 1 times

melatocaroca 1 year, 3 months ago
Yes, you can, and you can also provide to your own wim image to your preferred vendor,
upvoted 1 times

tungbache 1 year, 5 months ago
ms - 101 question ?
upvoted 2 times

Bobalo 1 year, 2 months ago

Pretty sure I had this one on my MS-101 exam.

upvoted 1 times

james1 1 year, 7 months ago

Provisioning package for sure - https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-package
lists all of the requirements

upvoted 4 times

mkoprivnj 1 year, 9 months ago

A for sure!

upvoted 2 times

Alvaroll 2 years ago

1-32 https://www.examtopics.com/exams/microsoft/ms-100/view/7/

upvoted 4 times

Learner3000 2 years, 2 months ago

Could be "Wipe and load refresh"?
Due to is needed to remove the preinstalled applications in order to met the "only approved apps installed"

upvoted 2 times

JaBe 2 years, 2 months ago

a provisioning package can remove pre-installed software.
"Set up device [...] Assign device name, enter product key to upgrade Windows, configure shared used, remove pre-installed softwar
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

upvoted 10 times

You have a Microsoft 365 subscription.
You recently configured a Microsoft SharePoint Online tenant in the subscription.
You plan to create an alert policy.
You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.
What should you do first?

A. Enable Microsoft Office 365 Cloud App Security.

B. Deploy Windows Defender Advanced Threat Protection (Windows Defender ATP).

C. Enable Microsoft Office 365 Analytics.

Correct Answer: *B*
An alert policy consists of a set of rules and conditions that define the user or admin activity that generates an alert, a list of users who trigger the alert if they perform the activity, and a threshold that defines how many times the activity has to occur before an alert is triggered.
In this question, we would use the ג€Malware detected in fileג€ activity in the alert settings then configure the threshold (5 detections) and the time window (10 minutes).
The ability to configure alert policies based on a threshold or based on unusual activity requires Advanced Threat Protection (ATP).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Community vote distribution
A (63%) B (38%)

Ronald82 Highly Voted 3 years ago
Yes ATP, but here you guys mention the wrong ATP, it should be called either Office 365 ATP, or Microsoft 365 ATP. Windows Defender A will not take care of malicious files within SharePoint Online.
upvoted 42 times

VTHAR 1 year, 11 months ago
Yes, it should be Office 365 ATP.
upvoted 5 times

mikl 1 month, 3 weeks ago
Which is named : Microsoft Defender for Office 365 now.
upvoted 1 times

Cyclops74 Highly Voted 2 years, 9 months ago
I agree with both remarks: indeed you can enable malware detection in Cloud App Security, but you need an Office 365 ATP license. Sin that is not mentioned, in this case the answer should be A. See: https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detectio policy
upvoted 14 times

simoen Most Recent 2 weeks, 1 day ago
Selected Answer: A
cloud app security
upvoted 1 times

pozzetttt 4 weeks, 1 day ago
Selected Answer: A
The answer is A:
You can test it!
Cloud App Security Portal--> Control--> Policies--> Activity type equals "Malware detected in file'
upvoted 1 times

ados8 2 months, 2 weeks ago
Selected Answer: A
Many years in this needs to be correct with B with appropriate name Microsoft Defender for Office 365.

upvoted 3 times

mikl 1 month, 3 weeks ago

I tend to agree.

upvoted 1 times

aaron_roman 2 months, 4 weeks ago

Selected Answer: A

it should be a

upvoted 1 times

aaron_roman 3 months ago

Selected Answer: A

it should be A based on:
https://docs.microsoft.com/en-us/defender-cloud-apps/editions-cloud-app-security-o365
"Threat Detection Anomaly detection and behavioral analytics"

upvoted 1 times

TechMinerUK 3 months, 3 weeks ago

Selected Answer: B

B is correct however it is not Windows Defender ATP (Now named Microsoft Defender for Endpoint) but rather Microsoft Defender for Office 365 (Previously named Office 365 ATP).

Windows Defender ATP would have never worked in this scenario since it is a client antivirus/anti-malware solution and Defender for Cloud Apps monitors connecting cloud apps e.g. abnormal data upload/download or new OAuth app connections

upvoted 2 times

DenisRossi 3 months, 3 weeks ago

Selected Answer: B

B is the correct, stop voting A.

upvoted 2 times

mikaiwhodakno 3 months, 3 weeks ago

Sorry but that is not correct. Look at the wording, Windows Defender ATP protects endpoints and PCs, it does not protect Sharepoin online, therefore the correct answer is A. This is commonly confused with the various products known as Cloud App Security, or Offi 365 ATP (now Microsoft Defender for Office 365), which WILL scan and protect Sharepoint.

upvoted 2 times

DenisRossi 3 months, 2 weeks ago

I see, you are right! I've made a mistake with the names!!!
Thank you!

upvoted 1 times

gaem 3 months, 3 weeks ago

Selected Answer: B

B is the right answer.
Stop voting A

upvoted 1 times

mikaiwhodakno 3 months, 3 weeks ago

Sorry but that is not correct. Look at the wording, "Windows Defender ATP" protects endpoints and PCs, it does not protect Sharepo online, therefore the correct answer is A. This is commonly confused with the various products known as Cloud App Security, or Offi 365 ATP (now Microsoft Defender for Office 365), which WILL scan and protect Sharepoint. The "Windows" naming gives it away as t wrong answer.

upvoted 1 times

gaem 4 months, 2 weeks ago

Selected Answer: B

ATP is the answer

upvoted 1 times

mikaiwhodakno 3 months, 3 weeks ago

A is the answer: https://www.examtopics.com/discussions/microsoft/view/11495-exam-ms-101-topic-2-question-66-discussion/

upvoted 1 times

UltraMAGA 4 months, 3 weeks ago

The Answer is B, and the reason it is B is:
"Tip

Originally launched as Windows Defender ATP, in 2019, this EDR product was renamed Microsoft Defender ATP.

At Ignite 2020, we launched the Microsoft Defender for Cloud XDR suite, and this EDR component was renamed Microsoft Defender fo
Endpoint. "
Source:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows

upvoted 1 times

joergsi 8 months, 1 week ago

Please check:
https://docs.microsoft.com/en-us/defender-cloud-apps/editions-cloud-app-security-o365

Office 365 Cloud App Security is a subset of Microsoft Defender for Cloud Apps that provides enhanced visibility and control for Office 3
Office 365 Cloud App Security includes threat detection based on user activity logs, discovery of Shadow IT for apps that have similar functionality to Office 365 offerings, control app permissions to Office 365, and apply access and session controls.

upvoted 1 times

davem90 10 months, 2 weeks ago

Selected Answer: A

Microsoft Cloud App Security is now called Microsoft Defender for Cloud Apps.

Defender for Cloud Apps supports malware detection for the following apps:
Box
Dropbox
Google Workspace
Office 365 (requires a valid license for Microsoft Defender for Office 365 P1)

https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

upvoted 3 times

Durden871 7 months ago

I doubt recent changes are reflected in the test, but I could be wrong.

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 1 times

TimurKazan 1 year, 1 month ago

Tricky question from MS. At first I would have chosen Microsoft 365 Defender
, but there is no such answer. In addition, alert policy allows minum interval of 60 minutes. Checked it in Cloud App Security, and it allo
to set it with required settings. I go with A

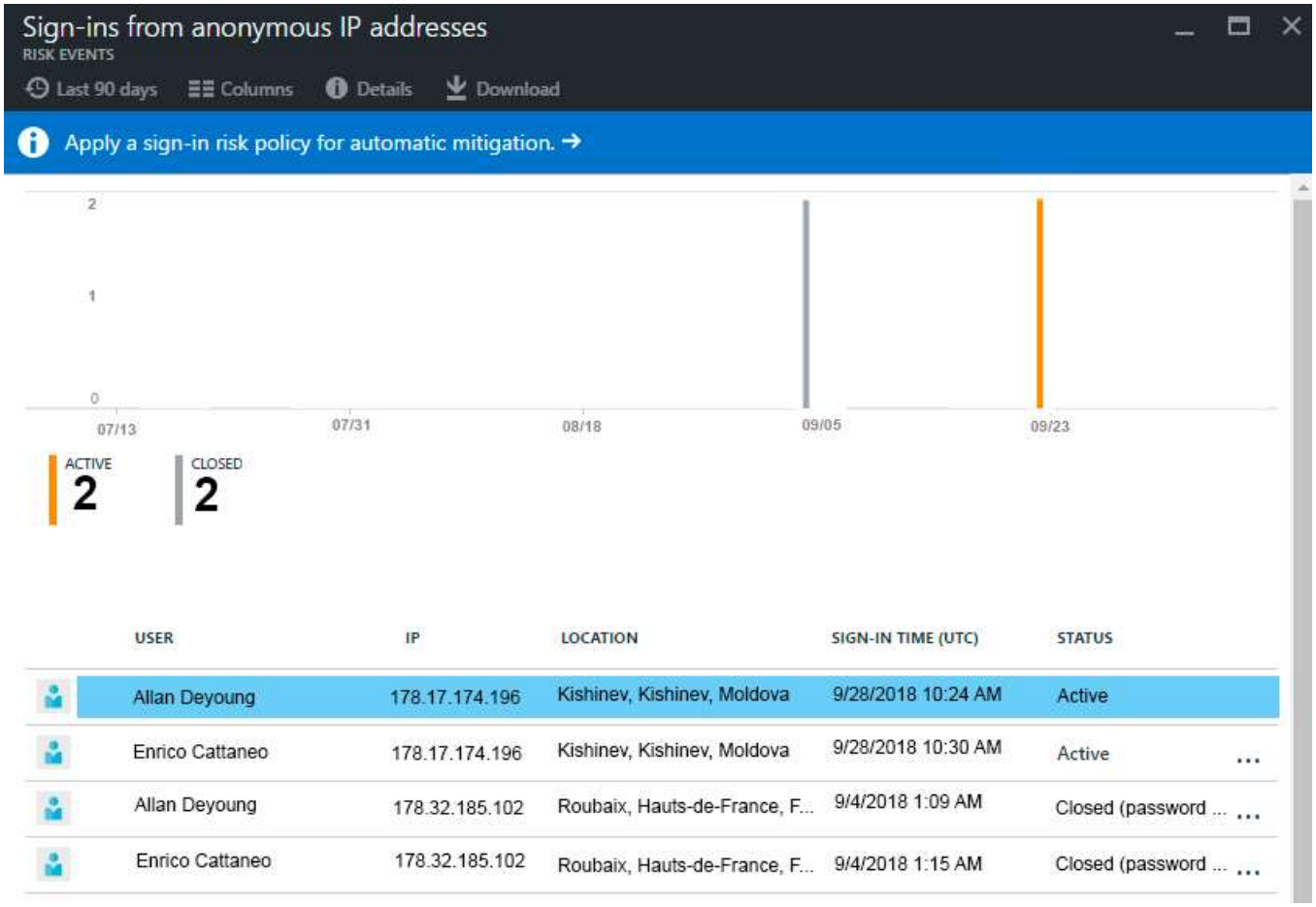
upvoted 2 times

Davidchercm 1 year, 1 month ago

similar discussion found here : https://www.examtopics.com/discussions/microsoft/view/11495-exam-ms-101-topic-2-question-66-discussion/

upvoted 1 times

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit.



You need to reduce the likelihood that the sign-ins are identified as risky.

What should you do?

A. From the Security & Compliance admin center, add the users to the Security Readers role group.

B. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.

D. From the Security & Compliance admin center, create a classification label.

Correct Answer: *B*

A named location can be configured as a trusted location. Typically, trusted locations are network areas that are controlled by your IT department. In addition to

Conditional Access, trusted named locations are also used by Azure Identity Protection and Azure AD security reports to reduce false positives for risky sign-ins.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Community vote distribution

B (100%)

mikl 1 month, 3 weeks ago

Selected Answer: B

Seems ok.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

upvoted 1 times

gxsh 1 year, 1 month ago

Correct!

upvoted 1 times

melatocaroca 1 year, 4 months ago

Difference between active and closed are location so, ANSWER B is correct

From the Conditional access blade in the Azure Active Directory admin center, create named locations.

RISK DETECTION AND REMEDIATION

New country This detection is discovered by Microsoft Cloud App Security (MCAS).
Activity from anonymous IP address This detection is discovered by Microsoft Cloud App Security (MCAS).

Reference
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

upvoted 3 times

Jol 1 year, 3 months ago

Agree!

upvoted 1 times

Manojch 1 year, 4 months ago

correct

upvoted 3 times

DRAG DROP -

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

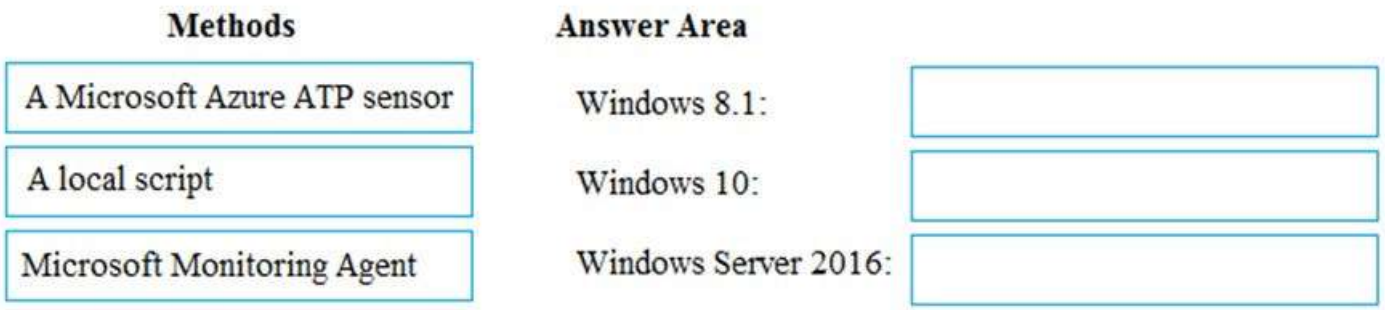
Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Windows Defender Advanced Threat Protection (ATP). The solution must avoid installing software on the devices whenever possible.

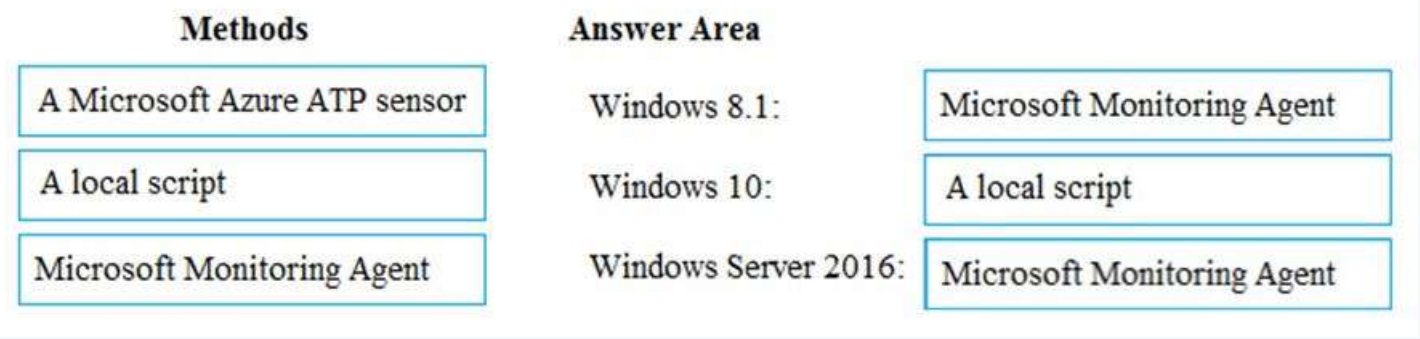
Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1:

To onboard down-level Windows client endpoints to Microsoft Defender ATP, you'll need to:

Configure and update System Center Endpoint Protection clients.

Install and configure Microsoft Monitoring Agent (MMA) to report sensor data to Microsoft Defender ATP

Box 2:

For Windows 10 clients, the following deployment tools and methods are supported:

Group Policy -

System Center Configuration Manager

Mobile Device Management (including Microsoft Intune)

Local script -

Box 3:

Windows Server 2016 can be onboarded by using Azure Security Centre. When you add servers in the Security Centre, the Microsoft Monitoring Agent is installed on the servers.

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-

threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat- protection

ctfalci Highly Voted 2 years, 2 months ago

Box 1:
To onboard down-level Windows client endpoints to Microsoft Defender ATP, you'll need to:
Configure and update System Center Endpoint Protection clients. Install and configure Microsoft Monitoring Agent (MMA) to report se data to Microsoft Defender
ATP Box 2:
For Windows 10 clients, the following deployment tools and methods are supported:
Group Policy System Center Configuration Manager Mobile Device Management (including Microsoft Intune) Local script.
Box 3:
Windows Server 2016 can be onboarded by using Azure Security Centre. When you add servers in the Security Centre, the Microsoft Monitoring Agent is installed on the servers.

upvoted 15 times

RNG60FR Highly Voted 1 year, 9 months ago

This cannot be an MS-100 exam question.

upvoted 11 times

Turak64 1 year, 1 month ago

Correction, it *shouldn't* be a MS-100 question but this is Microsoft. I've done enough MS certs now, to know they are always addin questions that are totally out of scope.

upvoted 6 times

H_ngM_n Most Recent 3 days, 7 hours ago

i agree

upvoted 1 times

H_ngM_n 3 days, 7 hours ago

with windows server 2016 using local script

upvoted 1 times

mmraouf 1 week, 1 day ago

1-MMA
2-Local Script
3-Local Script
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-downlevel?view=o365-worldwide
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide#prerequisites-for-windows-server-2016

upvoted 1 times

aaron_roman 3 months ago

Box 1 - MMA
Box 2 &3 Local script to comply with the requirement "avoid installing software when possible"

upvoted 1 times

mikaiwhodakno 3 months, 3 weeks ago

The "avoid installing software when possible", combined with local script available from 2012 R2-newer means local script for Win10 ar 2016, and install MMA for Win8. The real question though is which version of the test do we get and which answer does the test actuall accept as correct?
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide

upvoted 1 times

TechMinerUK 3 months, 3 weeks ago

I'm not sure I agree with this as from personal experience you do not need to install the Microsoft Monitoring Agent to onboard Server 2012 R2, Server 2016, Server 2019 or Server 2022 systems.

In the past to onboard server systems we have used the same method as onboarding AD joined Windows systems which is creating a G that runs the onboarding script which would be an answer which meets the requirement of not installing any software.

This is backed up by the documentation here: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide

Note it says:
The previous implementation of onboarding Windows Server 2012 R2 and Windows Server 2016 required the use of Microsoft Monitor Agent (MMA).

The new unified solution package makes it easier to onboard servers by removing dependencies and installation steps.

Because of this I would say that Windows 8.1 needs the MMA however Server 2016 and Windows 10 do not from my experience
upvoted 3 times

neeewbi 4 months ago
What's right?
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide#endpoint-onboarding-tools
upvoted 2 times

forummj 4 months, 1 week ago
I don't agree with the answer or those suggesting using MMA more than once.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide

The above link clearly has Local Scripts for Server & 10 situations, and MMA for 8.1.

In order to "avoid installing software" where possible, this would be the best solution for me.
upvoted 4 times

Wojer 9 months, 3 weeks ago
Now its possible to onboard win 2016 and 2012r2 with installation package and after that onboard package
upvoted 1 times

JAPo123 1 year, 1 month ago
in ms-100 exam last friday.
upvoted 7 times

JAPo123 1 year, 1 month ago
In exam last friday.
upvoted 2 times

melatocaroca 1 year, 4 months ago
Windows 10 deployment supported tools and methods:
• Group Policy
• Microsoft Endpoint Configuration Manager
• Mobile Device Management (including Microsoft Intune)
• Local script
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide
Install and configure Microsoft Monitoring Agent (MMA) to report sensor data to Microsoft Defender for Endpoint
• Windows 7 SP1 Enterprise
• Windows 7 SP1 Pro
• Windows 8.1 Pro
• Windows 8.1 Enterprise
Windows Defender ATP on legacy operating system requires installation of an agent
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/protecting-windows-server-with-windows-defender-atp/ba-p/267114

Windows 2016 Windows Defender Antivirus is built-in Windows Defender ATP on legacy operating system requires installation of an ag
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/protecting-windows-server-with-windows-defender-atp/ba-p/267114
upvoted 1 times

jroxas 1 year, 5 months ago
I saw this question on MS-101.
upvoted 5 times

Candice79 1 year, 5 months ago
This seems like a question for the MS 500 not the MS 100.
upvoted 5 times

Rstilekar 1 year, 8 months ago
Seems not a right question and any explainations either. Ques looks outdated
upvoted 2 times

PattiD 1 year, 9 months ago
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/onboard-downlevel#install-and-configur
microsoft-monitoring-agent-mma-to-report-sensor-data-to-microsoft-defender-for-endpoint
upvoted 1 times

HOTSPOT -

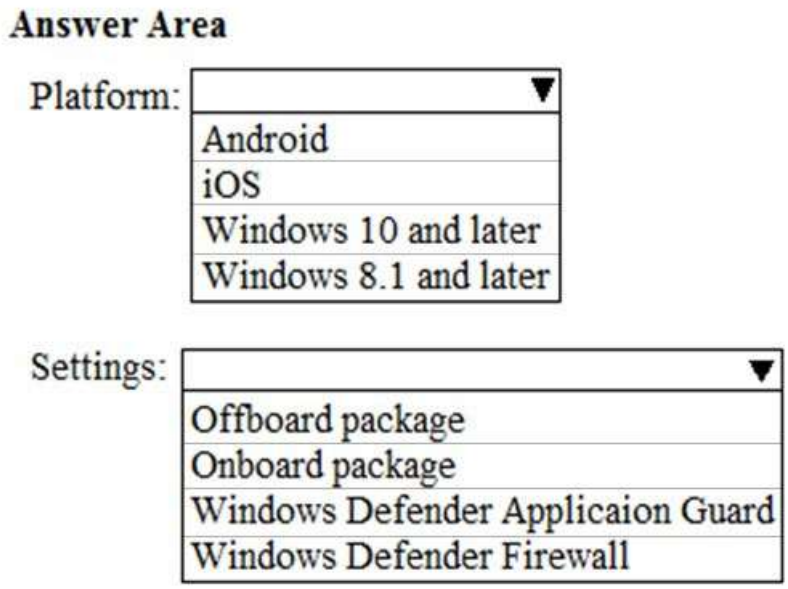
You have a Microsoft 365 subscription.

You need to implement Windows Defender Advanced Threat Protection (ATP) for all the supported devices enrolled devices enrolled on mobile device management (MDM).

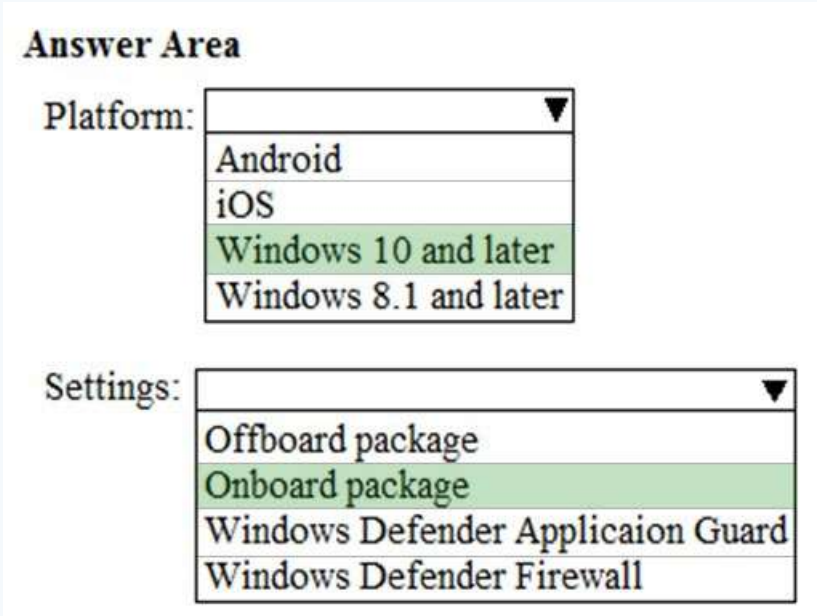
What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



You can integrate Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) with Microsoft Intune as a Mobile Threat Defense solution.

Integration can help you prevent security breaches and limit the impact of breaches within an organization. Microsoft Defender ATP works with devices that run

Windows 10 or later.

When you establish a connection from Intune to Microsoft Defender ATP, Intune receives a Microsoft Defender ATP onboarding configuration package from

Microsoft Defender ATP. This package is deployed to devices by using a device configuration profile.

Reference:

https://docs.microsoft.com/en-us/intune/advanced-threat-protection

ctfalci Highly Voted 2 years, 1 month ago

You can integrate Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization. Microsoft Defender ATP works with devices that run Windows 10 or later.
When you establish a connection from Intune to Microsoft Defender ATP, Intune receives a Microsoft Defender ATP onboarding configuration package from Microsoft Defender ATP. This package is deployed to devices by using a device configuration profile.
Reference:
https://docs.microsoft.com/en-us/intune/advanced-threat-protection

upvoted 8 times

jage01 Most Recent 7 months ago

On-board via Intune - it is supported only for Win10.
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

Onboard Android devices
There isn't a configuration package for devices that run Android.

Onboard iOS/iPadOS devices
There isn't a configuration package for devices that run iOS/iPadOS.

upvoted 3 times

Davidchercm 9 months ago

platform is to be all and the setting is onboard package

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

upvoted 1 times

forummj 4 months, 1 week ago

There is no "all" option.

upvoted 1 times

melatocaroca 1 year, 4 months ago

They ask to use mobile device management for all the supported devices enrolled devices enrolled on and implement Windows Defend
Advanced Threat Protection (ATP), so
Windows 10 and onboarding package match

Onboard Windows 10 devices using Mobile Device Management tools
Onboard Windows 10 devices using Group Policy
Onboard Windows 10 devices using Microsoft Endpoint Configuration Manager
Onboard Windows 10 devices using a local script
Onboard non-persistent virtual desktop infrastructure (VDI) devices

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-mdm?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide
Android
iOS
Linux
macOS
https://www.inthecloud247.com/microsoft-defender-atp-for-mobile/

upvoted 1 times

RAJULROS 1 year, 4 months ago

is this question still valid with the recent changes in Intune?

upvoted 1 times

RNG60FR 1 year, 9 months ago

This cannot be an MS-10 Exam question.

upvoted 1 times

bog23 1 year, 6 months ago

yes, o365

upvoted 2 times

airairo 1 year, 4 months ago

it is MS 101

upvoted 2 times

mkoprivnj 1 year, 9 months ago

W10 + onboarding package.

upvoted 3 times

madsa 1 year, 10 months ago

All these questions are MS-101 related, which I already approved, a very hard exam by the way. Makes no sense.

upvoted 4 times

Kabir93 2 years ago

I have seen questions related to Microsoft Intune which is a topic for MS-101 exam (Enterprise Mobility and Security), why there are several questions for Intune when it does not fall in MS100

upvoted 4 times

VTHAR 1 year, 11 months ago

yes. it was asked in exam.

upvoted 3 times

Kabir93 2 years ago

I have seen questions related to Microsoft Intune which is a topic for MS-100 exam (Enterprise Mobility and Security), why there are several questions for Intune when it does not fall in MS100

upvoted 4 times

Turak64 1 year, 1 month ago

Because that's how Microsoft roll...

upvoted 2 times

JohnO1971 2 years, 5 months ago

Microsoft Defender ATP works with devices that run Windows 10 or later, and with Android devices.

upvoted 2 times

JohnO1971 2 years, 5 months ago

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

upvoted 1 times

PhantomPhixer 2 years, 4 months ago

but there is no mention of any specific extra items to onboard android. so it looks like the question refers to what you need to do onboard win 10, which is the onboard package referenced in the answer and the link

upvoted 1 times

madmouse256 2 years, 5 months ago

WDATP works with plenty OSes but you should use different onboarding methods for this - https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/onboard-downlevel

upvoted 2 times

yoloserg 2 years, 6 months ago

win 8.1 support Defender ATP. why chosen "Windows 10 and later"?

upvoted 3 times

madmouse256 2 years, 5 months ago

If you want to on-board via Intune - it is supported only for Win10. For prevision versions you should install MMA. So if you have this answers - you should pickup "Onboarding package", and it will technically work only with Win10

upvoted 6 times

Question #37 *Topic 2*

You have a Microsoft 365 tenant.
You have a line-of-business application named App1 that users access by using the My Apps portal.
After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.
You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.
What should you do?

A. From Microsoft Cloud App Security, modify the impossible travel alert policy.

B. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.

C. From the Azure Active Directory admin center, modify the conditional access policy.

D. From Microsoft Cloud App Security, create an app discovery policy.

Correct Answer: *A*
Impossible travel detection identifies two user activities (is a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second.
We need to modify the policy so that it applies to App1 only.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Community vote distribution
B (80%) A (20%)

joelfrancisco Highly Voted 2 years, 11 months ago
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Impossible travel is on anomaly detection policy see link
upvoted 27 times

WoneSix 2 years, 7 months ago
Thanks, joel - that's the link that should ahve been referenced in the answer. :-(
upvoted 1 times

asdkjhbfc Highly Voted 2 years, 4 months ago
Hi guys and gals,
I tested this answer in my tenant and i've come to a conclusion; Answer A. Is in fact the correct answer. "Modify the impossible travel al policy"
See the how-to over here: http://www.rebeladmin.com/2018/09/step-step-guide-manage-impossible-travel-activity-alert-using-azure-cloud-app-security/ (i am not this guy thogh)
The fact remains that with an anomaly detection - impossible travel you cannot select a specific app to monitor for impossible travel (yo CAN select a Cloud app but there's no option to monitor for impossible travel)
Also see this: https://docs.microsoft.com/nl-nl/cloud-app-security/cloud-discovery-anomaly-detection-policy
There no option to monitor for impossible travel here. I've tested this in my tenant and the option does not present itself.
upvoted 17 times

shaan6810 1 year, 9 months ago
You're contradicting yourself here. You say the answer is A, then mention that you cannot select a specific app for it.
upvoted 1 times

Josey001 1 year, 5 months ago
Here answer is A: Udemy practice tests answer is B: Other practice tests i piad for answre
is again A.Are any of these practice tests worth bothering with, so many differing answers,
i have found over half a dozen answers to questions that differ from other practice tests i have paid for.Test prep training has ove dozen answers in one exam that differe from
both here & Udemy
upvoted 3 times

lucidgreen 1 year, 6 months ago
asdkjhbfc said that you cannot link an app in anomaly policy but you can in impossible travel policy.

upvoted 2 times

T10T Most Recent 1 month, 3 weeks ago

Selected Answer: B

The answer is B.

It's a trick question, they are misleading you with "impossible travel". Yes, there is a default "Impossible Travel" policy, but even if you modify you cannot restrict it to a single application.

You would have to create a new "Cloud Discovery anomaly detection policy", which includes the "impossible travel" as part of its scope then create a filter for "App1".

upvoted 3 times

Storm 3 months, 1 week ago

Answer has to be B
A. You cannot Modify Impossible travel alert policy
B. That will work
C. You cannot setup email alert in conditional access policy
D. The app is allready discovered. Thus dosen't make any sense.

https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy#impossible-travel
find : Scope anomaly detection policies in the link

upvoted 2 times

Chris1972 3 months, 2 weeks ago

all of the above

upvoted 1 times

DenisRossi 3 months, 3 weeks ago

Selected Answer: B

B is the correct.
1 - Never change a default policy, always create a new custom policy.
2 - The question ask to notify only if the App1 has a impossible travel alert, this is possible creating a new anomaly detection policy and setting the filter option with the App1 name.

upvoted 4 times

MirS 3 months, 1 week ago

Ans: B, refer to https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy#impossible-travel

upvoted 1 times

TechMinerUK 3 months, 2 weeks ago

I concur with DenisRoss.
When possible you shouldn't be editing the default policies as you are essentially narrowing down the protection they give based or the new configuration.

Any specific granular policies should be created additionally to the default policy to add more protection rather than removing it fro all other apps.

Because the question here is about only targeting App1 you should create an additional anomaly detection policy which is just targetted at App1 for impossible travel.

Yes, changing the default policy would work however it would not be the best solution since it is reducing the protection for other a

upvoted 1 times

salla 7 months ago

Selected Answer: A

tested

upvoted 1 times

rockey90 7 months ago

the answer is A
explanation :
1-from (Microsoft 365 admin center > security) it pops up a new window
2-you scroll down and click on (more resources)
3-you chose (microsoft defender for clouds Apps)
4- you navigate in (control>policies)
5-you scroll down to (impossible travel) and then modify it by adding the email address

upvoted 1 times

T10T 1 month, 3 weeks ago

It's a trick question because you are just looking for "Impossible Travel" in the GUI, when in fact that feature is included in the Anom detection policy. You will need to create a new policy and filter for App1.

upvoted 1 times

mikaiwhodakno 3 months, 3 weeks ago

But there is no option there as stated in the question to only protect App1, therefore B is the answer.

upvoted 2 times

AlexLiourtas 8 months, 3 weeks ago

Selected Answer: B

tested, ans B

upvoted 1 times

kanag1 8 months, 3 weeks ago

Selected Answer: A

Answer "A"is correct.
Policy Type : Anomaly detection
Exact Policy name : Impossible travel.
There are several "anomaly detection" polices available and dont need to configure all of them to achieve what is asked for (Refer the li in answer for all policy details). , As the question looks for the exact policy name, the answer is : Impossible travel Policy.

upvoted 1 times

mikaiwhodakno 3 months, 3 weeks ago

But there is no option there as stated in the question to only protect App1, therefore B is the answer. The question is regarding the App1, not the user(s) using the App1.

upvoted 2 times

AZalan 1 year, 2 months ago

There is already default "Impossible travel" policy and to apply it to a specific user who uses App1. change Scope to "specific users & groups" and "filter" the specific user. So ANS=A

upvoted 1 times

rebadow 1 year, 3 months ago

It has to be A, the question states that the policy is already created.
The task is to simply modify the existing policy so that it alerts.

Choosing B is if there was no policy in place, and even then the answer would be iffy, since when you create an anomaly detection polic you also choose what kind, one does not cover all.

upvoted 3 times

BGM_YKA 1 year, 4 months ago

I think there is some confusion here... the question is asking how to add email alerts to the already created conditional access policy fo App1 that uses Conditional Access App Control.

I think the correct answer should be modify the MCAS Session Policy based on the conditional access policy... But that's not an option.

C. is wrong since alerting is not part of conditional access policy

A. maybe since it's the only MCAS modify where B. and D. are MCAS create

upvoted 1 times

lucidgreen 1 year, 6 months ago

Always create a custom policy. Never modify default policies.

upvoted 3 times

lucidgreen 1 year, 6 months ago

Let me clarify. You don't want to restrict your default policies to a single app. So best to create a new one.

upvoted 4 times

[Removed] 1 year, 8 months ago

B - https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy
You cant edit an existing policy, just create one. Also, impossible travel is under anomaly detection.

upvoted 3 times

JeepScratch 1 year, 8 months ago

Nonsense, you can edit the default policy BUT then you only limit for the specific user which is not smart. So create a new one..right ans = B

upvoted 2 times

bingomutant 1 year, 9 months ago

definitely D beyond all doubt

upvoted 2 times

mkoprivnj 1 year, 9 months ago

B but not sure!

upvoted 2 times

Question #38 *Topic 2*

Your network contains an on-premises Active Directory domain.
Your company has a security policy that prevents additional software from being installed on domain controllers.
You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP).
What should you do? More than once choice may achieve the goal. Select the BEST answer.

A. Deploy an Azure ATP standalone sensor, and then configure port mirroring.

B. Deploy an Azure ATP standalone sensor, and then configure detections.

C. Deploy an Azure ATP sensor, and then configure detections.

D. Deploy an Azure ATP sensor, and then configure port mirroring.

Correct Answer: *C*
If you're installing on a domain controller, you don't need a standalone ATP sensor. You need to configure the detections to detect application installations. With an ATP sensor (non-standalone), you don't need to configure port mirroring.
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5 https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning#choosing-the-right-sensor-type-for-your-deployment

Community vote distribution
A (100%)

Piper Highly Voted 2 years, 11 months ago
This I am quite sure is wrong, a standalone sensor is the only option with port mirroring. Because you cant install agents on DC's, the answer provided is wrong (in my opinion). I am happy if someone wishes to challenge that.
upvoted 46 times

Alvaroll 2 years ago
Completely agree.
https://practical365.com/security/azure-atp-intro/
"If you don't want to deploy the Azure ATP Sensor directly on your domain controllers, you can instead deploy the Azure ATP Standal Sensor on a separate server. The standalone sensor monitors traffic that you direct to it by using port mirroring on your network switches."
upvoted 5 times

VTHAR 1 year, 11 months ago
Yes. Correct answer is A. Same question in MS-101.
upvoted 8 times

[Removed] 1 year, 8 months ago
Agreed
upvoted 1 times

mshorty Highly Voted 2 years, 8 months ago
I agree with @PlasticMind. Azure ATP Sensor will be installed on DC which is in this case not allowed (answers C and D). Azure ATP standalon sensor with port mirroring must be the correct answer (A). See here https://docs.microsoft.com/en-us/azure-advanced-threa protection/atp-capacity-planning#choosing-the-right-sensor-type-for-your-deployment
upvoted 9 times

Arlecchino Most Recent 3 weeks, 6 days ago
Selected Answer: A
A is the way imo
upvoted 1 times

aaron_roman 3 months ago
Selected Answer: A
no doubt A
upvoted 1 times

sliix 7 months, 4 weeks ago

Selected Answer: A

This is the answer. Trust me bro :)

upvoted 2 times

AlexLiourtas 7 months, 3 weeks ago

source: "dude trust me"

upvoted 14 times

tf444 9 months, 2 weeks ago

If you're installing on a domain controller, you don't need a standalone ATP sensor. You need to configure the detections to detect application installations. With an ATP sensor (non-standalone), you don't need to configure port mirroring.
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning#choosing-the-right-sen

upvoted 1 times

mikaiwhodakno 3 months, 3 weeks ago

As stated in the question: Your company has a security policy that prevents additional software from being installed on domain controllers.

No install means it is installed elsewhere and monitors this server, answer A.

upvoted 2 times

08twitch 10 months ago

Selected Answer: A

Update answer to A

upvoted 3 times

AlexLiourtas 10 months, 1 week ago

Selected Answer: A

A, you cannot install on active directory due to policy

upvoted 1 times

zacmzee 1 year ago

I'll go with A, since in the question it states "Your company has a security policy that prevents additional software from being installed o domain controllers." That being said you can install Azure ATP standalone sensor on domain controller.

upvoted 1 times

Panku 1 year ago

Answer should be A
We cannot install additional software on the domain controllers. Azure ATP Standalone Sensor is a full agent installed on a dedicated server that can monitor traffic from multiple domain controllers. This is an alternative to those that do not wish to install an agent direc on a domain controller.

upvoted 2 times

jeffyeh 1 year, 1 month ago

From here looks like the "Azure ATP Sensor" is feasible to install on DC. So I'll go with C.

https://docs.microsoft.com/en-us/defender-for-identity/install-step4

upvoted 1 times

mikaiwhodakno 3 months, 3 weeks ago

but the question states clearly:
Your company has a security policy that prevents additional software from being installed on domain controllers.

upvoted 1 times

lengySK 1 year, 1 month ago

I think correct is A

upvoted 1 times

Azreal_75 1 year, 2 months ago

Does a stand-alone sensor even exist now? I can;t see any reference to it in the MS install guides?

upvoted 2 times

mkuczynski 1 year, 3 months ago

It's a tricky question. We need to install ATP to fulfill the security policy. In this way C is correct answer.

upvoted 1 times

ubt 1 year, 3 months ago

When reviewing the below link, doesn't it point towards C as being correct?
https://docs.microsoft.com/en-us/defender-for-identity/install-step4

upvoted 2 times

mikaiwhodakno 3 months, 3 weeks ago

Your company has a security policy that prevents additional software from being installed on domain controllers.

upvoted 1 times

Gus01 1 year, 5 months ago

Answer C is Correct
https://docs.microsoft.com/en-us/defender-for-identity/install-step4
The installation wizard automatically checks if the server is a domain controller or a dedicated server. If it's a domain controller, the Defender for Identity sensor is installed. If it's a dedicated server, the Defender for Identity standalone sensor is installed.

upvoted 2 times

mikaiwhodakno 3 months, 3 weeks ago

Your company has a security policy that prevents additional software from being installed on domain controllers.

upvoted 1 times

Davood 1 year, 6 months ago

Correct answer is C.

upvoted 1 times

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.
You perform a proof of concept (PoC) deployment of Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP-related data to be stored in the United States.
You plan to onboard all the devices to Windows Defender ATP data in Europe.
What should you do first?

A. Create a workspace

B. Offboard the test devices

C. Delete the workspace

D. Onboard a new device

Correct Answer: *B*
When onboarding Windows Defender ATP for the first time, you can choose to store your data in Microsoft Azure datacenters in the European Union, the United
Kingdom, or the United States. Once configured, you cannot change the location where your data is stored.
The only way to change the location is to offboard the test devices then onboard them again with the new location.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/data-storage-privacy#do-i-have-the-flexibility-to-select-where-to-store- my-data

Community vote distribution
B (100%)

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
When onboarding Windows Defender ATP for the first time, you can choose to store your data in Microsoft Azure datacenters in the European Union, the United Kingdom, or the United States. Once configured, you cannot change the location where your data is stored
The only way to change the location is to offboard the test devices then onboard them again with the new location.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defenderatp/data-storage-privacy
upvoted 19 times

Duyons Highly Voted 1 year, 7 months ago
Not an MS-100 question but MS-101.
upvoted 9 times

Moderator Most Recent 1 month, 2 weeks ago
Selected Answer: B
Valid question (30th july 2022)
upvoted 1 times

mkoprivnj 1 year, 9 months ago
B for sure!
upvoted 4 times

donathon 1 year, 11 months ago
Correct link: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/minimum-requirements#network-and-data-storage-and-configuration-requirements
upvoted 2 times

FcoGlezRoy 2 years, 4 months ago
Can somebody explain why not D? I do not see the need of removing previously onboarded devices. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/onboard-configure
Also data location behave is changing but I think that Europe devices just define a logical unit grouping the devices.
upvoted 3 times

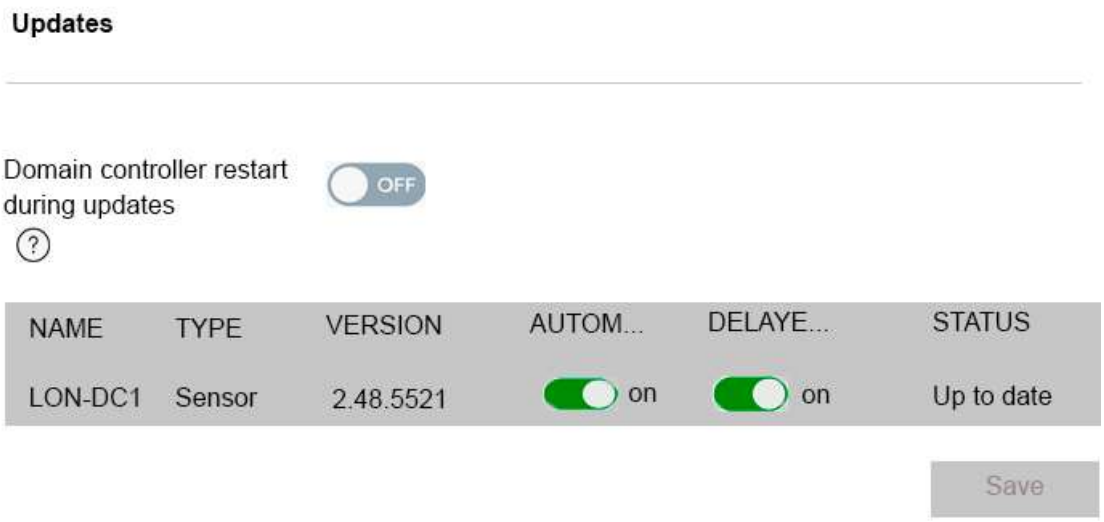
BRad96 2 years, 3 months ago

It states "You plan to onboard all devices data to Europe". So you need to remove the devices from the USA servers first

upvoted 6 times

You implement Microsoft Azure Advanced Threat Protection (Azure ATP).
You have an Azure ATP sensor configured as shown in the following exhibit.

Updates -



How long after the Azure ATP cloud service is updated will the sensor update?

A. 1 hour

B. 7 days

C. 48 hours

D. 12 hours

E. 72 hours

Correct Answer: *E*
The exhibit shows that the sensor is configure for Delayed update.
Given the rapid speed of ongoing Azure ATP development and release updates, you may decide to define a subset group of your sensors as a delayed update ring, allowing for a gradual sensor update process. Azure ATP enables you to choose how your sensors are updated and set each sensor as a Delayed update candidate.
Sensors not selected for delayed update are updated automatically, each time the Azure ATP service is updated. Sensors set to Delayed update are updated on a delay of 72 hours, following the official release of each service update.
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update

HobGoblinTank Highly Voted 2 years, 11 months ago
I believe this is now 72 hours - https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update
upvoted 27 times

VTHAR 1 year, 11 months ago
Yes, this question is outdated and was in MS-101 exam. You need to select 72 hours which is the only correct answers in the options Possible answer like 24 hours/1 day since the version is 2.48 are excluded there (possibly to avoid confusion).
upvoted 3 times

dailyup 1 year, 5 months ago
This question has shown in MS-100 and E is 24 hours. The correct answer is 72 hours.
upvoted 1 times

Goofer Highly Voted 2 years, 7 months ago
Answer E is changed in the exam to 72 hours
upvoted 10 times

Rlcky Most Recent 1 year ago

Answer is E. Feature Enhancement: 72 hour delayed sensor update
Changed option to delay sensor updates on selected sensors to 72 hours (instead of the previous 24-hour delay)

upvoted 1 times

Matajare 1 year, 3 months ago

The version in which it is updated every 72 hours is 2.62. The version that appears in the question is 2.48 ... so 24 hours
https://docs.microsoft.com/en-us/defender-for-identity/whats-new#azure-atp-release-262

upvoted 1 times

lucidgreen 1 year, 6 months ago

Moral of the story is, it used to be 24. Now it's 72. I think if I see the question on the exam and 72 isn't there, I'm picking 24.

upvoted 3 times

mikl 1 year, 6 months ago

72 hours.

Source : https://docs.microsoft.com/en-us/defender-for-identity/whats-new

"Feature Enhancement: 72 hour delayed sensor update
Changed option to delay sensor updates on selected sensors to 72 hours (instead of the previous 24-hour delay) after each release upd
of Azure ATP. See Azure ATP sensor update for configuration instructions."

upvoted 2 times

rRefJr 1 year, 7 months ago

"Sensors not selected for delayed update are updated automatically, each time the Defender for Identity service is updated. Sensors se
Delayed update are updated on a delay of 72 hours, following the official release of each service update." - Ans 72 Hours

upvoted 1 times

ezapper2 1 year, 8 months ago

delayed update is 72 hours

upvoted 1 times

mkoprivnj 1 year, 9 months ago

72h. Answer E is changed in the exam to 72 hours. I confirm: It's now 72 hours --> https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update

upvoted 3 times

scottims 2 years ago

Meant to add the link
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new

upvoted 1 times

scottims 2 years ago

As per the possible solutions, D=24 hours is correct. The delay is currently 72-hours but that is not a choice here.

Feature Enhancement: 72 hour delayed sensor update
Changed option to delay sensor updates on selected sensors to 72 hours (instead of the previous 24-hour delay) after each release upd
of Azure ATP. See Azure ATP sensor update for configuration instructions.

upvoted 1 times

Ben22 2 years, 2 months ago

Answer is 72 hours
Explanation:
The exhibit shows that the sensor is configure for Delayed update.
Given the rapid speed of ongoing Azure ATP development and release updates, you may decide to define a subset group of your sensors as a delayed update ring, allowing for a gradual sensor update process. Azure ATP enables you to choose how your sensors are updated and set each sensor as a Delayed update candidate.
Sensors not selected for delayed update are updated automatically, each time the Azure ATP service is updated. Sensors set to Delayed update are updated on a delay of 72 hours, following the official release of each service update.

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update

upvoted 4 times

ctfalci 2 years, 2 months ago

Answer: E
Explanation

The exhibit shows that the sensor is configure forDelayed update.
Given the rapid speed of ongoing Azure ATP development and release updates, you may decide to define a subset group of your senso
as a delayed update ring, allowing for a gradual sensor update process. Azure ATP enables you to choose how your sensors are update
and set each sensor as a Delayed update candidate.

Sensors not selected for delayed update are updated automatically, each time the Azure ATP service is updated. Sensors set to Delayed update are updated on a delay of 72 hours, following the official release of each service update.
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new

upvoted 5 times

zordss 2 years, 5 months ago

guys, look at the vers. in the screenshot. 25 is correct for v2.48.

upvoted 2 times

TonySuccess 2 years, 3 months ago

Ff that's the case then when in the exam I assume the version will be updated, this question was likely extracted before the update. 72.

upvoted 1 times

itmp 2 years, 5 months ago

version is 2.48 so it is 24hours - no one talks about new versions ..

upvoted 6 times

Jhill777 2 years, 4 months ago

On this link it says 72 hours and the version in the screenshot is 2.35.
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update

upvoted 2 times

praveen97 2 years, 3 months ago

72 hours delay is correct

upvoted 1 times

KingJulian 2 years, 7 months ago

Release update: Azure ATP release 2.62
Changed option to delay sensor updates on selected sensors to 72 hours (instead of the previous 24-hour delay) after each release upd of Azure ATP.
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new#azure-atp-release-262

upvoted 2 times

depmatic 2 years, 8 months ago

I confirm: It's now 72 hours --> https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update

upvoted 6 times

Question #41 *Topic 2*

Your company has a Microsoft 365 E3 subscription.
All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).
You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.
What should you use?

A. Subscription Activation

B. Windows Update

C. Windows Autopilot

D. an in-place upgrade

Correct Answer: *C*
When initially deploying new Windows devices, Windows Autopilot leverages the OEM-optimized version of Windows 10 that is preinstalled on the device, saving organizations the effort of having to maintain custom images and drivers for every model of device being used. Instead of re-imaging the device, your existing
Windows 10 installation can be transformed into a ג€business-readyג€ state, applying settings and policies, installing apps, and even changing the edition of
Windows 10 being used (e.g. from Windows 10 Pro to Windows 10 Enterprise) to support advanced features.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

Community vote distribution
A (100%)

TommyTommy Highly Voted 2 years, 11 months ago
A should be the correct one?
upvoted 55 times

PeterC 1 year, 4 months ago
Off course A - Subscription Activation
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 13 times

ctfalci 2 years, 2 months ago
Answer: C
Explanation
When initially deploying new Windows devices, Windows Autopilot leverages the OEM-optimized version of Windows 10 that is preinstalled on the device, saving organizations the effort of having to maintain custom images and drivers for every model of device being used. Instead of re-imaging the device, your existing Windows 10 installation can be transformed into a "business-ready" state, applying settings and policies, installing apps, and even changing the edition of Windows 10 being used (e.g. from Windows 10 Pro to Windows 10 Enterprise) to support advanced features.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot
upvoted 4 times

adaniel89 1 year, 4 months ago
Correct answer is A
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 4 times

VTHAR 1 year, 11 months ago
Wrong! Correct answer is A. This was also in MS-101 exam. Microsoft has been trying so hard to let the world know how easy it is switch from Win10 Pro to Ent by just assigning license, log off and log on. https://youtu.be/bk9wWc7x_m4
upvoted 25 times

Jayatheerthan 1 year, 11 months ago
Yes, this is there in MS-101 and the answer is A: Windows Autopilot

upvoted 1 times

Jayatheerthan 1 year, 11 months ago

In MS-101 the answer is A:Windows Autopilot. Here the answer is C.

upvoted 1 times

VTHAR 1 year, 11 months ago

What I'm trying to say is it was in my MS-101 exam and I have passed. Good luck with your answer.

upvoted 4 times

Takloy 1 year, 8 months ago

@VTHAR I agree with you on this one. It should be a matter of subscription activation and switch the license from Pro to Ent. I have actually done that and can't recall doing an autopilot just to switch the edition. In addition, question stated less downtim for the users, if you do autopilot, there will definitely be more down time due to the nature of autopilot.

upvoted 4 times

Cyclops74 Highly Voted 2 years, 10 months ago

Indeed, answer is A:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

upvoted 31 times

Rudelke Most Recent 3 months ago

Selected Answer: A

Windows itself is nowadays more or less unaware of enterprice license since you assign it per user in M365.
Enterprice license changes nothing in Windows functionality. It only allows you to take some actions that technically were plausible all along (for instance use W10 as VM on serwer).

upvoted 1 times

Gokhan83 3 months, 2 weeks ago

Selected Answer: A

Go for A: https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

upvoted 1 times

Gokhan83 3 months, 2 weeks ago

https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#how-it-works

upvoted 1 times

TechMinerUK 3 months, 2 weeks ago

Selected Answer: A

A is the correct answer as it allows the edition to be upgraded on client workstations without any per system intervention which would cause significant disruption for the end users.

By assigning a Windows 10/11 Enterprise licene via AzureAD any workstations which are hybrid joined/joined to AzureAD will automatically be upgraded to Windows 10/11 Enterprise.

The other options present either fail to do the above or upgrade the edition of Windows but at a significant downtime cost to the user (place upgrade/AutoPilot)

upvoted 1 times

Conkerzin 4 months, 2 weeks ago

A is Correct

upvoted 1 times

Ibraheem 5 months, 2 weeks ago

A ---correct answer

upvoted 1 times

Pr9 7 months, 3 weeks ago

Selected Answer: A

A. Subscription Activation

upvoted 1 times

Mea988 7 months, 3 weeks ago

Selected Answer: A

It's A, you just need to assign the new license, like we did in our org

upvoted 1 times

ExamTraining24 8 months, 1 week ago

Selected Answer: A

100% A
upvoted 1 times

AlexLiourtas 8 months, 3 weeks ago

Selected Answer: A

tested, ans A
upvoted 1 times

Pantoniou 9 months, 2 weeks ago

Selected Answer: A

Answer: A
upvoted 1 times

lengySK 1 year, 1 month ago

correct A - subscription activation
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 1 times

Comp_technician 1 year, 4 months ago

Answer is A

With Windows 10, version 1703 both Windows 10 Enterprise E3 and Windows 10 Enterprise E5 are available as online services via subscription. Deploying Windows 10 Enterprise in your organization can now be accomplished with no keys and no reboots.
upvoted 1 times

Shanjevan 1 year, 4 months ago

A . Subscription Activation - User logon triggers a silent edition upgrade, with no reboot required.
upvoted 1 times

Davood 1 year, 6 months ago

Correct answer is C.
upvoted 1 times

Razuli 1 year, 4 months ago

Why is it, please explain. A seems correct and I have done it many times
upvoted 2 times

lucidgreen 1 year, 6 months ago

Since they have A3 licenses, A is a no-brainer.
C would be the case if you wanted to do more than just change the license. AutoPilot would also take much more time and incur some unnecessary downtime while things get installed.
upvoted 3 times

HOTSPOT -

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

The device compliance policies have the assignment shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

Device 1:

No because Device1 is in group3 which has Policy1 assigned which requires BitLocker.

Device 2:

No because Device2 is in group3 which has Policy1 assigned which requires BitLocker. Device2 is also in Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.

Device3:

Yes because Device3 is in Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.

Reference:

https://blogs.technet.microsoft.com/cbernier/2017/07/11/windows-10-intune-windows-bitlocker-management-yes/

zeeess99 Highly Voted 2 years, 7 months ago

Answer is
Device 1 > No
Device 2 > No
Device 3 > Yes

upvoted 78 times

balouchi1964 Highly Voted 2 years, 4 months ago

Explanation:
Device 1:
No because Device1 is in group3 which has Policy1 assigned which requires BitLocker.
Device 2:
No because Device2 is in group3 which has Policy1 assigned which requires BitLocker. Device2 is also in Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.
Device3:
Yes because Device3 is in Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.
Reference:
https://blogs.technet.microsoft.com/cbernier/2017/07/11/windows-10-intune-windows-bitlocker-management-yes/

upvoted 16 times

donb21 Most Recent 1 month, 3 weeks ago

Should be NNY right,

upvoted 1 times

Rudelke 3 months ago

I love it how this answer is simple to answer even if you know little about compliance and Intune
BUT
during exam tables will not be layed out nicely. Insted they'll be in separate tabs forcing you to jump back and forthe between them. In other words this question does not test your knowledge. Instead it tests your resiliance to bull****.

upvoted 2 times

lengySK 1 year, 1 month ago

correct

upvoted 2 times

Ana22 1 year, 3 months ago

Had this in my MS-101 exam. Given answer is correct.

upvoted 3 times

mikl 1 year, 6 months ago

NO
NO
YES

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor

"If you have deployed multiple compliance policies, Intune uses the most secure of these policies."

upvoted 2 times

MrDre 1 year, 7 months ago

No, No, Yes for me.

upvoted 2 times

mkoprivnj 1 year, 9 months ago

No, No, Yes.

upvoted 4 times

ctfalci 2 years, 2 months ago

Device 1:
No because Device1 is in group3 which has Policy1 assigned which requires BitLocker.
Device 2:
No because Device2 is in group3 which has Policy1 assigned which requires BitLocker. Device2 is also in Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.
Device3:
Yes because Device3 is n Group2 which has Policy2 assigned but the BitLocker requirement is not configured in Policy2.

upvoted 6 times

jhawkins28 1 year, 11 months ago

Agreed! MS states: If a compliance policy evaluates against the same setting in another compliance policy, then the most restrictive compliance policy setting applies.
Therefore, Policy 2 would apply to Device 2 and require Bitlocker.

upvoted 4 times

jhawkins28 1 year, 11 months ago

Sorry meant to say: Therefore, Policy 1 would apply to Device 2 and require Bitlocker.

upvoted 1 times

TonySuccess 2 years, 3 months ago

Agree with Shark, No, No, Yes.

upvoted 3 times

shark1 2 years, 3 months ago

No
No. The BitLocker is evaluate due to If a compliance policy evaluates against the same setting in another compliance policy, then the m
restrictive compliance policy setting applies.
Yes

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot#if-multiple-policies-are-assigned-to-the-same
user-or-device-how-do-i-know-which-settings-gets-applied

upvoted 7 times

VTHAR 1 year, 11 months ago

Agreed. Answer is NO NO YES.

upvoted 2 times

rso 2 years, 4 months ago

If you have deployed multiple compliance policies, Intune uses the most secure of these policies.

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor

upvoted 5 times

zeeess99 2 years, 7 months ago

i feel the answer should be:
Device 1 --> No
Device 2 --> Yes
Device 3 --> No

Can someone please confirm and comment about their thought of the correct answer ?

upvoted 2 times

Jhill777 2 years, 4 months ago

Device 2 is also part of Group 3 that requires bitlocker. Not compliant.

upvoted 2 times

Durden871 7 months, 1 week ago

It's no, no, yes. Curious how you got "no" On 3? 1 and 2 both have a policy that requires bit locker. In Device 2, if one requires and th
other is not configured, the requirement is still enforced.

3 belongs to a policy that doesn't require Bitlocker to be enabled.

upvoted 2 times

HOTSPOT -

Your company has a Microsoft 365 tenant.

You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

The device type restrictions are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

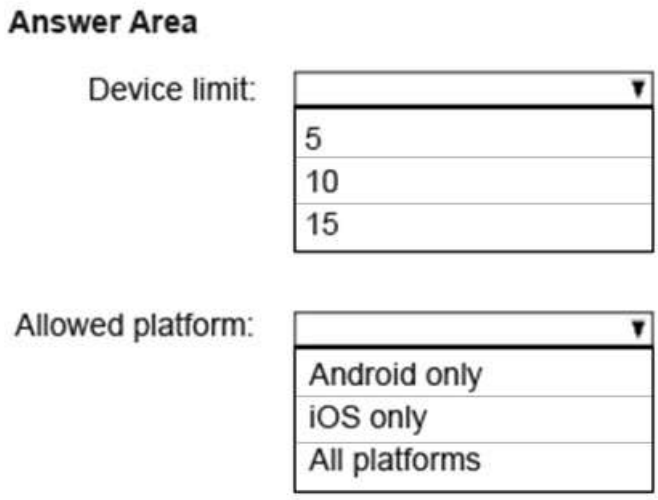
The device limit restrictions are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

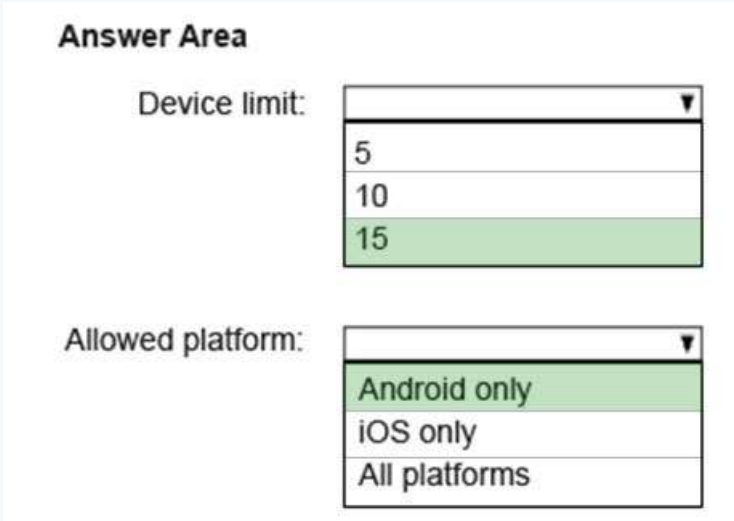
What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



When multiple policies are applied to groups that users are a member of, only the highest priority (lowest number) policy applies.

In this case, the Engineering users are assigned two device type policies (the default policy and the priority 2 policy). The priority 2 policy has a higher priority than the default policy so the Engineers' allowed platform is Android only.

The engineers have two device limit restrictions policies applied them. The priority1 policy is a higher priority than the priority2 policy so the priority1 policy device limit (15) applies.

Reference:

https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set

ctfalci Highly Voted 2 years, 2 months ago

When multiple policies are applied to groups that users are a member of, only the highest priority (lowest number) policy applies.
In this case, the Engineering users are assigned two device type policies (the default policy and the priority 2 policy). The priority 2 poli
has a higher priority than the default policy so the Engineers' allowed platform is Android only.
The engineers have two device limit restrictions policies applied them. The priority1 policy is a higher priority than the priority2 policy s
the priority1 policy device limit (15) applies.
Reference:
https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set

upvoted 20 times

VP11 Highly Voted 2 years, 7 months ago

https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set
Priority is used when a user exists in multiple groups that are assigned restrictions. Users are subject only to the highest priority restriction assigned to a group that they are in. For example, Joe is in group A assigned to priority 5 restrictions and also in group B assigned to priority 2 restrictions. Joe is subject only to the priority 2 restrictions.

upvoted 13 times

kravielex Most Recent 3 months ago

Correct

upvoted 1 times

Parvezg 1 year, 7 months ago

It should be 15 and Android only -
Priority is used when a user exists in multiple groups that are assigned restrictions. Users are subject only to the highest priority restriction assigned to a group that they are in. For example, Joe is in group A assigned to priority 5 restrictions and also in group B assigned to priority 2 restrictions. Joe is subject only to the priority 2 restrictions. When you create a restriction, it's added to the list jus
above the default.

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority

upvoted 5 times

mkoprivnj 1 year, 9 months ago

Android only + 15.

upvoted 3 times

Prianishnikov 1 year, 10 months ago

What is the correct answer?

upvoted 3 times

VTHAR 1 year, 11 months ago

Why is this question here since this related to EMS? It was in my MS-101 exam.

upvoted 7 times

minajahan 2 years, 7 months ago

I guess the reason being, these limitations are explicitly mentioned for Engineering department...?

upvoted 1 times

Question #44 *Topic 2*

Your network contains an Active Directory domain named contoso.com. The domain contains 1000 Windows 8.1 devices.
You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices.
You need to recommend a Windows 10 deployment method.
What should you recommend?

A. Wipe and load refresh

B. Windows Autopilot

C. a provisioning package

D. an in-place upgrade

Correct Answer: *A*
To deploy a custom image, you must use the wipe and load refresh method. You cannot deploy a custom image by using an in-place upgrade, Windows Autopilot or a provisioning package.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

Community vote distribution
A (100%)

ZakS Highly Voted 2 years, 10 months ago
I think the ans is A - Wipe and Load Refresh.
upvoted 43 times

PlasticMind 2 years, 9 months ago
since this question specifically states that a custom image of windows needs to be deployed, wipe-and-load refresh i.e. the tradition
method of deployment is the onl feasible option here. Please refer to:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
upvoted 12 times

ctfalci 2 years, 2 months ago
Answer: A
Explanation
To deploy a custom image, you must use the wipe and load refresh method. You cannot deploy a custom image by using an in-place upgrade, Windows Autopilot or a provisioning package.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
upvoted 10 times

melatocaroca 1 year, 4 months ago
You can deploy a custom image for in-place upgrade, using

MDT, Microsoft deployment-toolkit,
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

system configuration manager,
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-cm/upgrade-to-windows-10-with-configuraton-manage

Windows Autopilot,
https://www.techrepublic.com/article/using-autopilot-to-upgrade-existing-devices-to-windows-10/

provisioning package. need to upgrade to windows 10 first
upvoted 1 times

VTHAR 1 year, 11 months ago
Yes, answer is A. Wipe and Load refresh
upvoted 3 times

melatocaroca 1 year, 3 months ago

To deploy a custom image, you must use the wipe and load refresh method.
The process is normally initiated in the running operating system. User data and settings are backed up and restored later as part o
the deployment process. The target can be the same as for the new computer scenario.
upvoted 2 times

itmp Highly Voted 2 years, 5 months ago
Answer is definitely A.

Refresh:
"Redeploy a device by saving the user state, wiping the disk, then restoring the user state."
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#computer-refresh

In-Place: "CUSTOM images are not needed and CANNOT be used"
Autopilot: no mention about Azure/Intune
Provisioning package: for configuration, settings, and apps.
upvoted 13 times

itmp 2 years, 4 months ago
And another one for reference:
"In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade"

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployme
toolkit
upvoted 4 times

miry117 Most Recent 2 months, 1 week ago
Selected Answer: A
Wipe and Load is the best option.
upvoted 1 times

Davood 1 year, 6 months ago
Correct answer is A.
upvoted 1 times

lucidgreen 1 year, 6 months ago
No time or user constraints. No Intune. No talk of an available device management service...
A!
If IT could do what they wanted with every machine, it would always be wipe and refresh. Why? Because it is always the best option giv
a choice -- next to provisioning with a wipe and refresh. Clean out all the gremlins!
upvoted 2 times

mkoprivnj 1 year, 9 months ago
A for sure!
upvoted 3 times

choy1977 1 year, 10 months ago
I thought A on this one and was surprised to see that the revealed answer is D? has it been confirmed as A?
upvoted 2 times

Purist 1 year, 5 months ago
well, at the time of me reading this, yes
upvoted 1 times

k2kimmy 1 year, 10 months ago
Ans is A https://www.interfacett.com/videos/windows-10-deployment-wipe-and-load-in-place-and-provisioning/
upvoted 1 times

Martyvdb 1 year, 10 months ago
Key words: 'Custom Image' and 'Active Directory'
Can't be Auto pilot because AD (and Win 8 also)
Can't be in-place, because 'custom image'
Wipe...
upvoted 4 times

mikl 1 year, 6 months ago
Totally agree.
upvoted 1 times

csribeiro12 1 year, 10 months ago
Resposta correta é A:
Por que o upgrade não aceita imagens personalizadas

https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#in-place-upgrade
upvoted 1 times

Jayatheerthan 1 year, 11 months ago
Think the answer is D. https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#in-place-upgrade
upvoted 2 times

ctfalci 2 years, 2 months ago
Answer: A
Explanation
To deploy a custom image, you must use the wipe and load refresh method. You cannot deploy a custom image by using an in-place upgrade, Windows Autopilot or a provisioning package.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
upvoted 7 times

Benjam 2 years, 3 months ago
To deploy a custom image, you must use the wipe and load refresh method. You cannot deploy a custom image by using an in-place upgrade, Windows Autopilot or a provisioning package.
Correct Answer is A
upvoted 3 times

andpi 2 years ago
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#dynamic-provisioning
upvoted 1 times

DJHASH786 2 years, 4 months ago
Correct answer is D
The exercise is to upgrade the PC's that are on a domain with less work to do.
So you can create a custom Win 10 image and then use setup.exe to do the in place upgrade.
I passed the Win 10 exam and this was one of the same questions.
upvoted 2 times

T_B 2 years, 3 months ago
No, custom images cannot be used with in place upgrade:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
"custom images are not needed and cannot be used because the upgrade process is unable to deal with conflicts between apps in t
old and new operating system"
upvoted 3 times

MichealAlex5 2 years, 4 months ago
Te answer is wipe and load fresh.
upvoted 1 times

Hakimi 2 years, 5 months ago
The answer is correct To deploy a custom image, you must use the wipe and load refresh method. You cannot deploy a custom image b
using an in-place upgrade, Windows Autopilot
upvoted 2 times

Ama100 2 years, 6 months ago
*sorry, D is the correct answer
upvoted 2 times

You use Microsoft System Center Configuration manager (Current Branch) to manage devices.

Your company uses the following types of devices:

- Windows 10
- Windows 8.1
- Android
- iOS

Which devices can be managed by using co-management?

A. Windows 10 and Windows 8.1 only

B. Windows 10, Android, and iOS only

C. Windows 10 only

D. Windows 10, Windows 8.1, Android, and iOS

Correct Answer: *C*

You can manage only Windows 10 devices by using co-management.

When you concurrently manage Windows 10 devices with both Configuration Manager and Microsoft Intune, this configuration is called co-management. When you manage devices with Configuration Manager and enroll to a third-party MDM service, this configuration is called coexistence.

Reference:

https://docs.microsoft.com/en-us/configmgr/comanage/overview

Marz Highly Voted 2 years, 9 months ago

Only Windows 10 is supported: https://docs.microsoft.com/en-us/configmgr/comanage/overview

upvoted 50 times

djlink 2 years, 1 month ago

co-management: It enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune.

Ref: https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/choose-a-device-management-solution#bkmk_intune

upvoted 3 times

ctfalci Highly Voted 2 years, 2 months ago

Answer: C

Explanation

You can manage only Windows 10 devices by using co-management.

When you concurrently manage Windows 10 devices with both Configuration Manager and Microsoft Intune, this configuration is calle co-management. When you manage devices with Configuration Manager and enroll to a third-party MDM service, this configuration is called coexistence.

Reference:

https://docs.microsoft.com/en-us/configmgr/comanage/overview

upvoted 12 times

Cafarelli Most Recent 11 months, 2 weeks ago

Answer C.

MS KB says : "Co-management enables you to concurrently manage Windows 10 or later devices by using both Configuration Manager and Microsoft Intune."

https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#prerequisites

upvoted 1 times

lucidgreen 1 year, 6 months ago

It's asking which devices can be manage using co-management, not "while" using it.

Only Windows 10 can be managed using co-management.

upvoted 2 times

mikl 1 year, 6 months ago

Answer is C - Windows 10 only.

https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#prerequisites

upvoted 2 times

Parvezg 1 year, 7 months ago

Its Windows 10 and later
Paths to co-management. There are two main paths to reach to co-management:

Existing Configuration Manager clients: You have Windows 10 devices that are already Configuration Manager clients. You set up hybri
Azure AD, and enroll them into Intune.

New internet-based devices: You have new Windows 10 devices that join Azure AD and automatically enroll to Intune. You install the
Configuration Manager client to reach a co-management state.

Prerequisites
Co-management has these prerequisites in the following areas:

Licensing
Configuration Manager
Azure Active Directory (Azure AD)
Microsoft Intune
Windows 10
Permissions and roles

https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#prerequisites

upvoted 1 times

estarisbourne 1 year, 8 months ago

When you concurrently manage Windows 10 devices with both Configuration Manager and Microsoft Intune, this configuration is calle
co-management. When you manage devices with Configuration Manager and enroll to a third-party MDM service, this configuration is
called coexistence

upvoted 1 times

estarisbourne 1 year, 8 months ago

Windows 10
Upgrade your devices to Windows 10, version 1709 or later. For more information, see Adopting Windows as a service.

Important

Windows 10 mobile devices don't support co-management.
Folks suggesting co-management is useful for anything outside of Windows 10 past the specific criteria is wrong for that and are
confusing folks. ONLY WIN 10 is supported. Do not confuse co-management with Intune capabilities!

question asks about co-management abilities not Intune abilities.

upvoted 1 times

banditben86 1 year, 9 months ago

https://www.exam4training.com/which-devices-can-be-managed-by-using-co-management-3/#:~:text=Windows%2010,%20Windows%208.1,%20Android,%20and%20iOS.%20You,and%20Microsoft%20Intune,%20this%20configu
on%20is%20called%20co-management.

upvoted 1 times

paddyh 1 year, 9 months ago

Windows 10 only , as for the given answer should this be co-existence

upvoted 1 times

mkoprivnj 1 year, 9 months ago

Windows 10 only, so I would say C.

upvoted 1 times

mkoprivnj 1 year, 9 months ago

Only Windows 10.

upvoted 1 times

Prianishnikov 1 year, 10 months ago

Only Win 10 devices

upvoted 1 times

madsa 1 year, 10 months ago

Fcnet is 100% correct, co-management means managing devices with Endpoint and SCCM, meaning all platforms, this is another MS-1
exam question and the answer is on the MS-101 exam reference book. Correct answer D

upvoted 1 times

hchafloque 2 years ago

With "Co-manage" you can use both, intune and CCM). The other definition es Co-existence, and is the option to use CCM or Intune.
upvoted 1 times

Benjam 2 years, 3 months ago
Microsoft Answer is - C. Windows 10 only
upvoted 5 times

TonySuccess 2 years, 3 months ago
Also went for C, and looking at the comments and references am confident.
upvoted 2 times

scottims 2 years ago
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#windows-10
Windows 10 is a requirement for co-managment.
upvoted 2 times

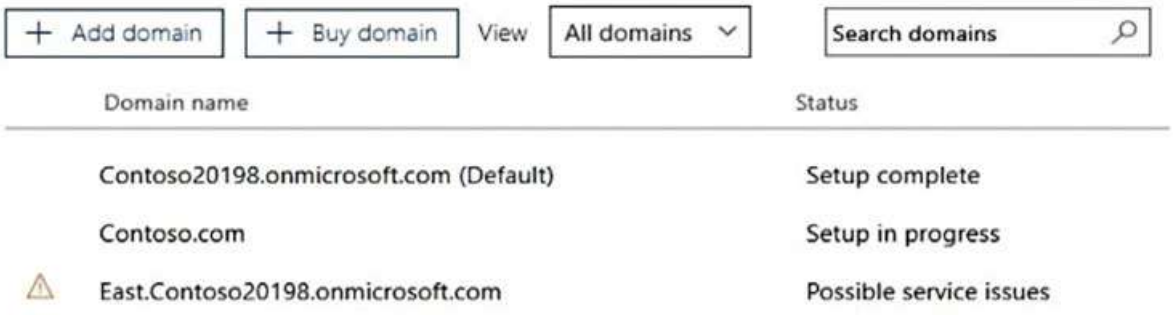
Fcnet 2 years, 4 months ago
The answer is D.
Co management means you manage from Intune AND Sccm the same device, yes in this scenario Windows 10 is a requirement. But in case that means you have both solutions. What that means : you can manage Win10, Android and IOs from Intune, And Win81 and Wi With Sccm. With the comanagement in place only Win 10 is comanaged, other devices either thru Intune or SCCM (not from both) are managed too . So the answer D is the right answer.
upvoted 3 times

Sonia33 2 years, 4 months ago
No, because it is asking which devices can be managed using co-management. Only Windows 10 devices can be "co-managed", Windows 8.1, Android and iOs cannot. You manage them from SCCM or from Intune, but using these two technologies is not co-management. Co-management must be enabled in SCCM and affects W10 only.
upvoted 1 times

Sonia33 2 years, 4 months ago
"Co-management requires Windows 10 version 1709 or later. Once you update Windows and configure auto-enrollment, your cli are automatically enrolled to co-management."
https://docs.microsoft.com/en-gb/mem/configmgr/comanage/quickstart-upgrade-win10
upvoted 1 times

HOTSPOT -

You company has a Microsoft 365 subscription that contains the domains shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

An administrator can create usernames that contain the **[answer choice]**.

- Contoso20198.onmicrosoft.com domain only
- Contoso20198.onmicrosoft.com domain and all its subdomains only
- Contoso20198.onmicrosoft.com and East.Contoso20198.onmicrosoft.com domains only
- Contoso20198.onmicrosoft.com, East.Contoso20198.onmicrosoft.com, and Contoso.com domains

Exchange Online can receive inbound email messages sent to the **[answer choice]**.

- Contoso20198.onmicrosoft.com domain only
- Contoso20198.onmicrosoft.com domain and all its subdomains only
- Contoso20198.onmicrosoft.com and East.Contoso20198.onmicrosoft.com domains only
- Contoso20198.onmicrosoft.com, East.Contoso20198.onmicrosoft.com, and Contoso.com domains

Correct Answer:

Answer Area

An administrator can create usernames that contain the **[answer choice]**.

- Contoso20198.onmicrosoft.com domain only
- Contoso20198.onmicrosoft.com domain and all its subdomains only
- Contoso20198.onmicrosoft.com and East.Contoso20198.onmicrosoft.com domains only
- Contoso20198.onmicrosoft.com, East.Contoso20198.onmicrosoft.com, and Contoso.com domains

Exchange Online can receive inbound email messages sent to the **[answer choice]**.

- Contoso20198.onmicrosoft.com domain only
- Contoso20198.onmicrosoft.com domain and all its subdomains only
- Contoso20198.onmicrosoft.com and East.Contoso20198.onmicrosoft.com domains only
- Contoso20198.onmicrosoft.com, East.Contoso20198.onmicrosoft.com, and Contoso.com domains

Only the Contoso20198.onmicrosoft.com domain has a status of Setup Complete. The other two statuses mean that the domain setup is not complete or has issues that need to be corrected before they can be used.

Reference:

https://support.office.com/en-gb/article/what-do-domain-statuses-mean-in-office-365-3ecf1fef-3b31-497c-98bc-e57e2413b4e5

kevinwu128 Highly Voted 1 year, 5 months ago

1st box answer is definitely C

2nd box is theoretically A, but should be C. Service issues can mean other dns issues that don't relate to mail, or MX records that are us with 3rd party spam filters.

upvoted 33 times

Arargnum 1 year, 5 months ago

I agree with Kevin, a number of the client i look after do not have the DNS records for lynnc and other services therefore they have t message of possible issues however because MX records are setup correctly email works fine. correct answer in this case should be and C

upvoted 7 times

Justin1 Highly Voted 1 year, 3 months ago

So I tested and it should be C and A

You can add a subdomain to the .onmicrosoft.com domain and even with the status being "possible service issues" I was still able to create a user with that domain

On the other hand, it won't be possible to add any services to this subdomain as you don't have the ability to add DNS records to the .onmicrosoft.com domain, and thereby any subdomain you try and create will give you DNS records (MX, TXT, CNAME) that you have no way of adding.

upvoted 16 times

Moderator Most Recent 1 month, 2 weeks ago

Valid Question (30th july 2022)

upvoted 1 times

donb21 1 month, 3 weeks ago

answer I agree is C and A

upvoted 1 times

TechMinerUK 4 months ago

After checking this on my tenant I believe the answers are C and A.

This is because you can add subdomain.%COMPANY%.onmicrosoft.com and it will be verified however you cannot add records for anything to be routed for it. Because it is verified it means you can add it to users as their user name

It is A for part two as contoso.com is not setup so you can't yet receive mail from it and the subdomain has no routing to the tenant despite being verified

upvoted 2 times

Stiobhan 4 months ago

I am pretty certain that the reason the sub domain is having issues is because the parent domain is not fully setup? So therefore the answers would be correct!

upvoted 1 times

PmgCosta 5 months ago

I tested, its possible to add a sufix to your default tenant domain

Example examtopics.onmicrosoft.com (default)

If you try to add ms100.examtopics.onmicrosoft.com the domain are vaild and stay verifed automaticaly

upvoted 1 times

PmgCosta 5 months ago

Prefix (not sufix)

upvoted 1 times

waterlego 5 months, 2 weeks ago

Still valid, April 2022 - variation on it though.

upvoted 2 times

Lukeford89 5 months, 4 weeks ago

Can anyone confirm 100 % in the exam that the answer given would be correct> what is Microsofts view?

upvoted 1 times

mfaisal786 8 months ago

It's C and A, you can create users using domain which have status "possible service issues" but not with "Setup in progress"

upvoted 3 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

xofowi5140 11 months, 2 weeks ago

Is not possible to add onmicrosft.com subdomain.

"Refresh the page or try again later

Failed to get the options for managing DNS records for domain sub.xxxxxxxxx.onmicrosoft.com. The domain was removed from your account. Close the wizard, refresh your browser and try again."

upvoted 1 times

fofo1960 12 months ago

I love reading these comment, but hate it when it seems like a fight with no clue about the correct answer :(

upvoted 8 times

rfox321 1 year ago

Has anyone taken the exam passed and answered this so we know what is most likely the correct answers??

upvoted 2 times

zul_n 1 year ago

i'd say A and A - similar to the answers given.

All explanations here are correct, but considering Microsoft is weird as ....., it is best to assume those 'possible issues' cause issues in creating users.

upvoted 2 times

lengySK 1 year, 1 month ago

I think C C

upvoted 2 times

PDR 1 year, 1 month ago

I think C and A although you could be pedantic and say that C and C given that in theory you can 1. assign the domain as a user name t users and 2. you could , set up internal DNS with mx records allowing for the routing of emails to the east. subdomain if you had a hyb exchange setup (using connectors to route directly the EXO) - but of course that isnt the answer they are looking for.

upvoted 1 times

Turak64 1 year, 1 month ago

That's the problem with some of these questions, MS doesn't provide enough info or the question is too ambiguous. Ultimately it's t "microsoft" answer they're after.

upvoted 1 times

Question #47 *Topic 2*

Your company has 20 employees. Each employee has a mailbox hosted in Outlook.com.
The company purchases a Microsoft 365 subscription.
You plan to migrate all the mailboxes to Microsoft 365.
You need to recommend which type of migration to use for the mailboxes.
What should you recommend?

A. staged migration

B. cutover migration

C. minimal hybrid migration

D. IMAP migration

Correct Answer: *D*
To migrate mailboxes from Outlook.com to Office 365, you need to use the IMAP migration method.
After you've added your users to Office 365, you can use Internet Message Access Protocol (IMAP) to migrate email for those users from their IMAP-enabled email servers.
In the Microsoft 365 admin center, go to Setup > Data migration to start migrating IMAP enabled emails. The email migrations page is pre-configured for migrations from Gmail, Outlook, Hotmail and Yahoo. You can also enter your own IMAP server name and connection parameters to migrate from an email service that is not listed.
References:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/imap-migration-in-the-admin-center

MichaelJS Highly Voted 1 year, 9 months ago
Microsoft seems to think it is IMAP
"After you have setup two-step verification, you can also obtain an app password that you will have to use in order to use Internet Message Access Protocol (IMAP) migration to copy email from your Outlook.com or Hotmail.com account to your Microsoft 365 or Offi 365 for business account. If your Microsoft 365 or Office 365 admin is moving email messages from your Outlook.com or Hotmail.com account to Microsoft 365 or Office 365 on your behalf, you'll need to give him your app password."

Ref: https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrating-your-outlook-com-account
upvoted 12 times

rfox321 12 months ago
Correct - https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration
upvoted 1 times

SkullRage Most Recent 1 month ago
I Think D is the correct answer, because of the move from Outlook.com.
You can use the Internet Message Access Protocol (IMAP) to migrate user email from Gmail, Exchange, Outlook.com, and other email systems that support IMAP migration. When you migrate the user's email by using IMAP migration, only the items in the users' inbox o other mail folders are migrated. Contacts, calendar items, and tasks can't be migrated with IMAP, but they can be by a user.
upvoted 1 times

waterlego 5 months, 2 weeks ago
Still valid, April 2022 - Larger number (above 150) was used though so different answer.
upvoted 3 times

Ibraheem 5 months, 2 weeks ago
IMAP is correct ---- You can use the Internet Message Access Protocol (IMAP) to migrate user email from Gmail, Exchange, Outlook.com and other email systems that support IMAP migration.

From below doc
https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration
upvoted 2 times

trexar 7 months, 2 weeks ago
You can use the Internet Message Access Protocol (IMAP) to migrate user email from Gmail, Exchange, Outlook.com, and other email systems that support IMAP migration
upvoted 2 times

Jcbrow27 10 months, 3 weeks ago
https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrating-your-outlook-com-account

D is correct!
upvoted 2 times

spg987 1 year, 1 month ago
It is on today's exam
upvoted 2 times

lengySK 1 year, 1 month ago
I think correct is IMAP. Copied from Skillpipe:

Source of email server: Cutover - Exchange 2010 or later
IMAP - Any IMAP-accessible email server
upvoted 2 times

momonoke 1 year, 2 months ago
I would also say cutover.
Any other opinion + Explanation?
upvoted 1 times

lucidgreen 1 year, 6 months ago
Because it's not in Exchange, the only answer is IMAP.
upvoted 3 times

mkoprivnj 1 year, 9 months ago
i'll bet on cutover method!
upvoted 2 times

JamieWilson 1 year, 10 months ago
Cutover Migration should work as outlook.com has activesync and ews?
upvoted 3 times

Johana 1 year, 9 months ago
I went for cutover as well
upvoted 2 times

rfox321 12 months ago
https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration - Just google it dude
upvoted 1 times

Question #48 *Topic 2*

Your network contains an on-premises Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.
The on-premises network contains a file server named Server1. Server1 has a share named Share1 that contains company documents.
Your company purchases a Microsoft 365 subscription.
You plan to migrate data from Share1 to Microsoft 365. Only data that was created or modified during the last three months will be migrated.
You need to identify all the files in Share1 that were modified or created during the last 90 days.
What should you use?

A. Server Manager

B. Microsoft SharePoint Migration Tool

C. Resource Monitor

D. Usage reports from the Microsoft 365 admin center

Correct Answer: *B*
You can use the Microsoft SharePoint Migration Tool to migrate files from a file server to SharePoint Online.
The Microsoft SharePoint Migration Tool has a number of filters you can use to define which files will be migrated. One filter setting is ɹ€Migrate files modified afterɹ€. This setting will only migrate files modified after the selected date.
The first phase of a migration is to perform a scan of the source files to create a manifest of the files that will be migrated. You can use this manifest to identify all the files in Share1 that were modified or created during the last 90 days.
References:
https://docs.microsoft.com/en-us/sharepointmigration/spmt-settings

Community vote distribution
B (100%)

mkoprivnj Highly Voted 1 year, 9 months ago
B for sure. MS SPO migration tool!
upvoted 6 times

charat Most Recent 4 months, 1 week ago
Selected Answer: B
05/22 Exam. B is correct
upvoted 3 times

charat 4 months, 1 week ago
Migration manager if the service mentioned is OneDrive
upvoted 1 times

TechMinerUK 3 months, 2 weeks ago
I haven't done the exam yet however I have completed several SharePoint Migrations and Migration Manager should be a totally acceptable solution since it supports the same filters as SPMT such as Migrate Files Created After and Migrate Files Modified Afte

I would likely imagine SPMT being referenced is due to the material being slightly outdated so if the option is SPMT vs something else then SPMT is still a good an acceptable answer
upvoted 1 times

Wojer 9 months, 4 weeks ago
regarding my previous answer its Migration Manager
upvoted 1 times

Wojer 10 months ago
In my opinion, the answer is wrong because if you want to migrate from share drive you need to use Configuration manager
upvoted 1 times

spg987 1 year, 1 month ago
It is my today's exam

upvoted 3 times

PeterC 1 year, 4 months ago

B - Correct

SPMT supports migration to SharePoint and OneDrive from:
* SharePoint (2010,2013,2016..)
* Network and local file shares

upvoted 4 times

charat 4 months, 1 week ago

So even if the question were to rephrase with OneDrive, it should be SPMT. Thanks!

upvoted 1 times

Your company has two offices. The offices are located in Seattle and New York.
The company uses a third-party email system.
You implement Microsoft 365.
You move all the users in the Seattle office to Exchange Online. You configure Microsoft 365 to successfully receive all the email messages sent to the Seattle office users.
All the users in the New York office continue to use the third-party email system.
The users use the email domains shown in the following table.

Users in	Email domain
Seattle	Contoso.com
New York	Adatum.com

You need to ensure that all the email messages sent to the New York office users are delivered successfully. The solution must ensure that all the email messages for the users in both offices are routed through Microsoft 365.
You create the required DNS records and Send connectors.
What should you do next from Microsoft 365?

A. From the Microsoft 365 admin center, set the default domain. From the Exchange admin center, create a transport rule for all the email messages sent to adatum.com.

B. From the Microsoft 365 admin center, add the adatum.com domain. From the Exchange admin center, configure adatum.com as an internal relay domain.

C. From the Microsoft 365 admin center, add the adatum.com domain. From the Exchange admin center, configure adatum.com as an authoritative domain.

D. From the Microsoft 365 admin center, set the default domain. From the Exchange admin center, configure adatum.com as a remote domain.

Correct Answer: *B*
The first step is to configure Exchange Online to accept emails for the adatum.com domain. To do this, we add the domain in Microsoft 365.
When you add your domain to Microsoft 365, it's called an accepted domain.
The next step is to tell Exchange Online what to do with those emails. You need to configure the adatum.com domain as either an authoritative domain or an internal relay domain.
Authoritative domain means that the mailboxes for that domain are hosted in Office 365. In this question, the mailboxes for the adatum.com domain are hosted on the third-party email system. Therefore, we need to configure the adatum.com domain as an internal relay domain. For an internal relay domain, Exchange
Online will receive the email for the adatum.com domain and then 'relay' (forward) the email on to the third-party email server.
References:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/manage-accepted-domains/manage-accepted-domains

Community vote distribution
B (100%)

F_M Highly Voted 1 year, 4 months ago
The answer provided is correct
upvoted 11 times

donb21 Most Recent 1 month, 3 weeks ago
The answer B is correct
upvoted 1 times

Wesje 7 months, 2 weeks ago
Selected Answer: B
B seems to be good.
upvoted 2 times

JakeH 10 months, 3 weeks ago

In exam today
upvoted 2 times

spg987 1 year, 1 month ago
It was my today's exam
upvoted 4 times

MartiFC 1 year, 2 months ago
Internal Relay is correct
upvoted 2 times

mackypatio 1 year, 4 months ago
answer is internal relay for adatum. done the same few months ago.
upvoted 4 times

dmillion 1 year, 5 months ago
no comment means B is the answer
upvoted 2 times

HOTSPOT -
Your company has a Microsoft 365 subscription that contains the following domains:

Contoso.onmicrosoft.com -

Contoso.com -
You plan to add the following domains to Microsoft 365 and to use them with Exchange Online:
- Sub1.contoso.onmicrosoft.com
- Sub2.contoso.com
- Fabrikam.com

You need to identify the minimum number of DNS records that must be added for Exchange Online to receive inbound email messages for the three domains.
How many DNS records should you add? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

MX records: ▼
0
1
2
3

CNAME records: ▼
0
1
2
3

Correct Answer:

Answer Area

MX records: ▼
0
1
2
3

CNAME records: ▼
0
1
2
3

Box 1: 2 -
You don't need to verify Sub1.contoso.onmicrosoft.com because the onmicrosoft.com domain and DNS is managed by Microsoft. You also don't need to configure an MX record for Sub1.contoso.onmicrosoft.com because that will be done by Microsoft.
For sub2.contoso.com, you don't need to verify the domain because you have already verified its parent domain contoso.com. However, you do need an MX record to direct email for that domain to Exchange Online.
For Fabrikam.com, you will need to verify the domain. You will need an MX record to direct email for that domain to Exchange Online.

Box 2: 0 -

You 'should' create CNAME records for autodiscover to point your email clients to Exchange Online to connect to the mailboxes. However, you don't have to. You could configure the email client manually. Therefore, the minimum number of CNAME records required is zero.

prepre Highly Voted 1 year, 6 months ago

what lmao, I get the technicality but what lmao

upvoted 19 times

monsterjuice Most Recent 1 year, 3 months ago

The question on the exam looks like it does here-https://www.exam4training.com/how-many-dns-records-should-you-add-2/

Here they are missing that Contoso.com has already been added. That's why the answer talks about it already being verified.

upvoted 4 times

venwaik 1 year, 2 months ago

"You plan to add the following domains" which says that contoso.com and fabrikam are not added beforehand. therefore we need t
add 2 MX records for both domains.
If the subscription had the contoso domain included, it doesn't say you already added the mx record. Either way, you need to add 2
records

upvoted 2 times

Wearsy 1 year, 5 months ago

So you've got to guess whether contoso.com already has the mx records added, seeing as though it's already in the tenant...

upvoted 2 times

Wearsy 1 year, 5 months ago

Could be interpreted in both ways but the given answer seems to be asking you to confirm how many MX records you need to have
manually in place for the 3 domains, which the answer is 2, so fair enough...

upvoted 1 times

wonap 1 year, 5 months ago

which one?

upvoted 1 times

prepre 1 year, 5 months ago

you don't need cname records for mail flow. that's needed for outlook autodiscover. So technically it's 0 CNAME Records.

upvoted 8 times

melatocaroca 1 year, 4 months ago

https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?
view=o365-worldwide

upvoted 1 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

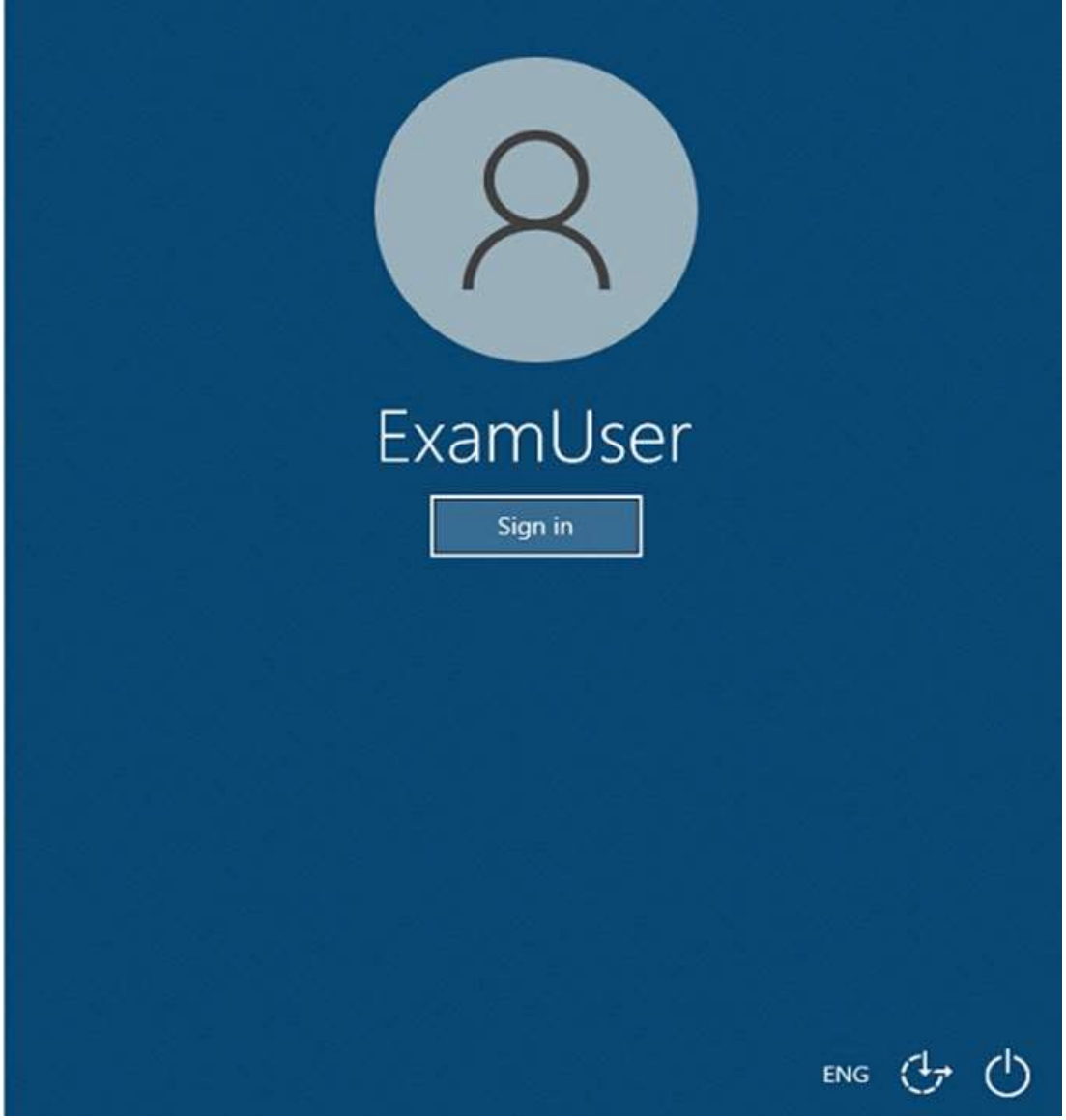
Lab Instance: 111111111 -
You plan to create 1,000 users in your Microsoft 365 subscription.
You need to ensure that all the users can use the @contoso.com suffix in their username.
Another administrator will perform the required information to your DNS zone to complete the operation.

Correct Answer: *See explanation below.*
You need to add the contoso.com domain to Microsoft 365 then set the domain as the default.
1. In the Admin Center, click Setup then click Domains.
2. Click the 'Add Domain' button.
3. Type in the domain name (contoso.com) and click the 'Use this domain' button.
4. The question states that another administrator will perform the required information to your DNS zone. Therefore, you just need to click the 'Verify' button to verify domain ownership.
5. Click Finish.
6. In the domains list, select the contoso.com domain.
7. Select 'Set as default'.
References:
https://docs.microsoft.com/en-us/office365/admin/setup/add-domain?view=o365-worldwide

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to prevent users in your organization from receiving an email notification when they save a document that contains credit card numbers.
To answer the question, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*

You need to edit the Data Loss Prevention Policy to disable the email notifications.

1. Go to https://protection.office.com or navigate to the Security & Compliance admin center.
2. In the left navigation pane, expand Data Loss Protection and select Policy.
3. Select the Data Loss Prevention policy and click the Edit Policy button.
4. Click Policy Settings in the left navigation pane of the policy.
5. Select the policy rule and click the Edit Rule button.
6. Scroll down to the 'User notifications' section.
7. Toggle the slider labelled ɹ€Use Notifications to inform usersɹ.¦€ɹ€ to Off.
8. Click Save to save the changes to the policy rule.
9. Click Save to save the changes to the policy.

Question #53 *Topic 2*

You have a Microsoft 365 subscription.
You add a domain named contoso.com.
When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.
You need to change the email address used to verify the domain.
What should you do?

A. From the domain registrar, modify the contact information of the domain

B. Add a TXT record to the DNS zone of the domain

C. Modify the NS records for the domain

D. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription

Correct Answer: *A*
The email address that is used to verify that you own the domain is the email address listed with the domain registrar for the registered contact for the domain.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide

Community vote distribution
A (100%)

mkoprivnj Highly Voted 1 year, 9 months ago
A for sure!
upvoted 7 times

ALPHA_DELTA 1 year, 7 months ago
For sure!
upvoted 4 times

Moderator Most Recent 1 month, 2 weeks ago
Selected Answer: A
Valid question (30th July 2022)
upvoted 2 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 3 times

VictorSaiz 11 months, 3 weeks ago
Regarding the provided link, there is no mention to the provided answer, is there any other link which explains the correct answer? Tha
& regards
upvoted 1 times

PattiD 1 year, 9 months ago
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
upvoted 4 times

Your company uses email, calendar, contact, and task services in Microsoft Outlook.com.
You purchase a Microsoft 365 subscription and plan to migrate all users from Outlook.com to Microsoft 365.
You need to identify which user data can be migrated to Microsoft 365.
Which type of data should you identify?

A. task

B. email

C. calendar

D. contacts

Correct Answer: *B*
You can use the Internet Message Access Protocol (IMAP) to migrate user email from Gmail, Exchange, Outlook.com, and other email systems that support IMAP migration. When you migrate the user's email by using IMAP migration, only the items in the users' inbox or other mail folders are migrated. Contacts, calendar items, and tasks can't be migrated with IMAP, but they can be by a user.
Reference:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration#migrate-email-from-another-imap-enabled-email-system

mkoprivnj Highly Voted 1 year, 9 months ago
Email only is correct answer!
upvoted 11 times

Storm 6 months, 1 week ago
Thank you so much
upvoted 1 times

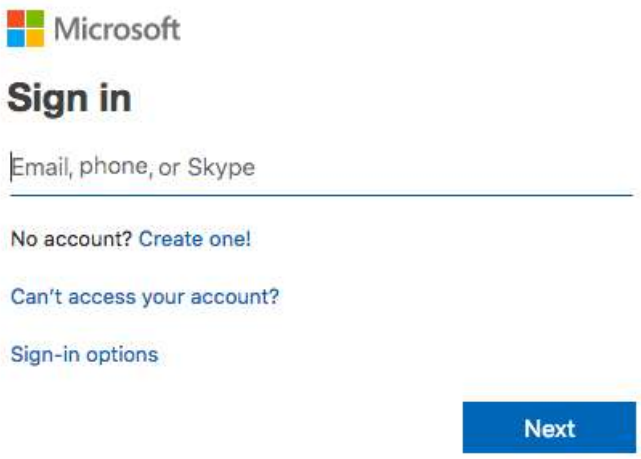
PattiD Most Recent 1 year, 9 months ago
When you migrate the user's email by using IMAP migration, only the items in the users' inbox or other mail folders are migrated. Contacts, calendar items, and tasks can't be migrated with IMAP, but they can be by a user.

IMAP migration also doesn't create mailboxes in Microsoft 365 or Office 365. You'll have to create a mailbox for each user before you migrate their email.
upvoted 2 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to prevent all the users in your organization from sending an out of office reply to external users.
To answer, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*
You need to modify the default remote domain. When you add a remote domain, you specify the domain name and the settings apply to that domain. The default remote domain applies to all other domains. Therefore, we need to disable Out of Office replies for external users in the settings of the default remote domain.
1. Go to the Exchange Admin Center.
2. Click Mail Flow in the left navigation pane.
3. Click on Remote Domains.
4. Select the default remote domain and click the Edit icon (pencil icon).
5. In the 'Out of Office automatic reply types' section, select 'None'.
6. Click Save to save to changes to the default remote domain.

Silverfire 2 weeks, 1 day ago

Setting the value to none will disable out of office replies completely.
I think that, an option 'Allow internal out of office' should be selected here.

upvoted 1 times

rajeshrengasamy 3 weeks, 4 days ago

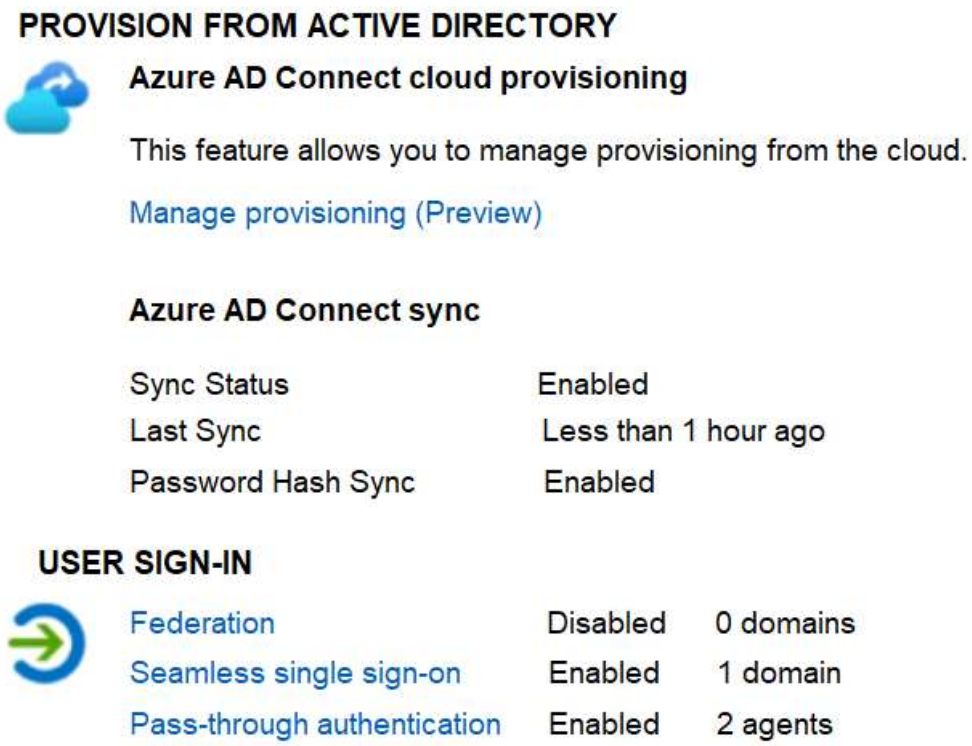
https://www.howto-outlook.com/howto/automaticreply.htm

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure Active Directory (Azure AD) tenant named contoso.com as shown in the exhibit.



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Azure Active Directory admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

Community vote distribution
A (70%) B (30%)

Andy_S Highly Voted 1 year, 5 months ago
I think answer B. Adding adatum.com to custom domain does not configure ADConnect.
upvoted 13 times

tf444 9 months, 1 week ago
ADATUM?

upvoted 1 times

zorro1 1 year, 5 months ago

All users are in the contoso domain. Also the fabrikam users. No need to set up additonal ADConnect.

upvoted 4 times

dngd Highly Voted 1 year, 5 months ago

I go for B. It's not mentioned that the domain is verified.

upvoted 10 times

ckanoz Most Recent 3 weeks, 5 days ago

Selected Answer: A

This question has nothing to do with AD Connect Syncing. The issue in the question is that can not sign in to online applications (Azure with the @fabrikam.

upvoted 1 times

RenegadeOrange 2 months, 1 week ago

Hopefully in the actual exam there will be additional information. I recall a similar question in MS-500 and the issue was that AD Conne configured with Pass-through so another option is local AD is down and no-one can sign into M365. Then you would change AD Conne to use Password Hash instead.

upvoted 1 times

aaron_roman 2 months, 4 weeks ago

Selected Answer: B

the answer is - you need to change the upn to contoso.com

upvoted 1 times

TechMinerUK 3 months, 2 weeks ago

Selected Answer: A

I'm going to go with A as since the user already has the UPN set as fabrikam.com that means Active Directory is configured with it as a UPN suffix for users.

By adding it to AzureAD in my mind that assumes (Which could be the unfolding of my answer) that the domain has succesfully been added and not just added to the portal in "Setup in progress" mode.

Because the domain is added to AzureAD it can then be assigned to users, since User2 already has fabrikam.com as a UPN suffix once delta sync has completed they should receive fabrikam.com as a UPN suffix in AzureAD allowing them to login.

upvoted 6 times

charat 4 months, 1 week ago

Selected Answer: B

Answer is B. Domain was added according to the question, but it wasn't verified.

upvoted 2 times

jjong 1 year ago

this qns came out in exam today

upvoted 3 times

TimurKazan 1 year ago

Besides that, domain is not verified

upvoted 1 times

Ash473 1 year, 1 month ago

In today's exam

upvoted 3 times

venwaik 1 year, 3 months ago

It says that the on-premise domain contains both users. Since Azure AD is configured with the contoso domain, the fabrikam users will sync. if you simply add fabrikam.com to Azure, you should also configure the domain in the on-prem AAD connect app.

The only solution is to change the UPN suffix in the on-prem domain (user2@fabrikam.com to user2@contoso.com) and manually sync wait for an automatic sync cycle.

Therefore, i think, the answer should be B; "no"

upvoted 8 times

melatocaroca 1 year, 3 months ago

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

Solution: From the Azure Active Directory admin center, you add fabrikam.com as a custom domain.

You instruct User2 to sign in as user2@fabrikam.com.

If they add fabrikam.com as a custom domain, configure ad connect verify domain with DNS txt record sync, will be yes, but with the instructions that do not tell nothing apart from fabrikam.com is added IMHO, answer is NO, if you assume add fabrikam.com is add an configure the rest of required steps answer is Yes

upvoted 2 times

melatocaroca 1 year, 3 months ago

Two agents means two domains are connected, so may be YES

upvoted 2 times

venwaik 1 year, 2 months ago

Two agents means two servers with Azure AD Passtrhough authentication module installed for high availability. "Domains" show how much domains are in sync.

upvoted 3 times

adaniel89 1 year, 3 months ago

I thought about this, technically by adding and verifying the new domain, you can then use the domain for signs. There is no need to sy the user from the source domain, just create an Azure AD domain account and add @adatum.com - this should work!

upvoted 2 times

gkp_br 1 year, 4 months ago

B for me. User already sync. After add fabrikam.com domain to Azure AD, we need remove and resync user2 to fix UPN.

upvoted 1 times

gkp_br 1 year, 4 months ago

Sorry. I revew my comment and it is wrong. No need remove and resync user2. So the answer A.

upvoted 2 times

Domza 1 year, 4 months ago

Tick or Treat:

It does not say weather User 2 is part of AD (local) its asking how to access Azure AD resources. By adding Custom Domain, User2 can access Azure AD - online resources. :)
Nothing to do with Azure AD connect :)

upvoted 2 times

PandaTuga 1 year, 3 months ago

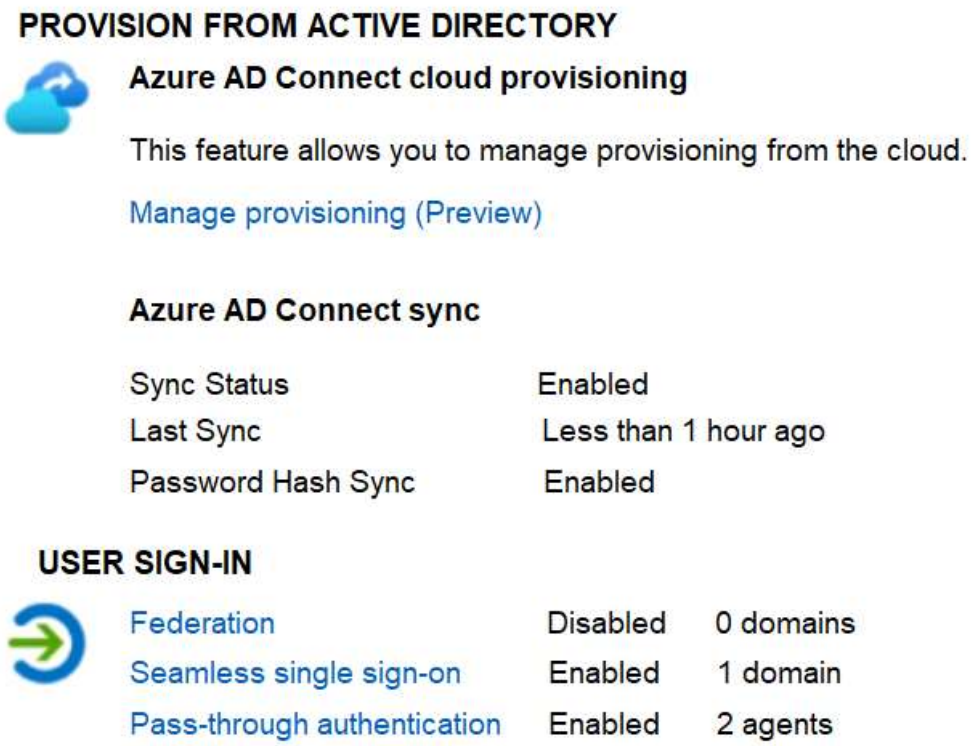
"The domain contains the users shown in the following table"

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure Active Directory (Azure AD) tenant named contoso.com as shown in the exhibit.



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes

B. No

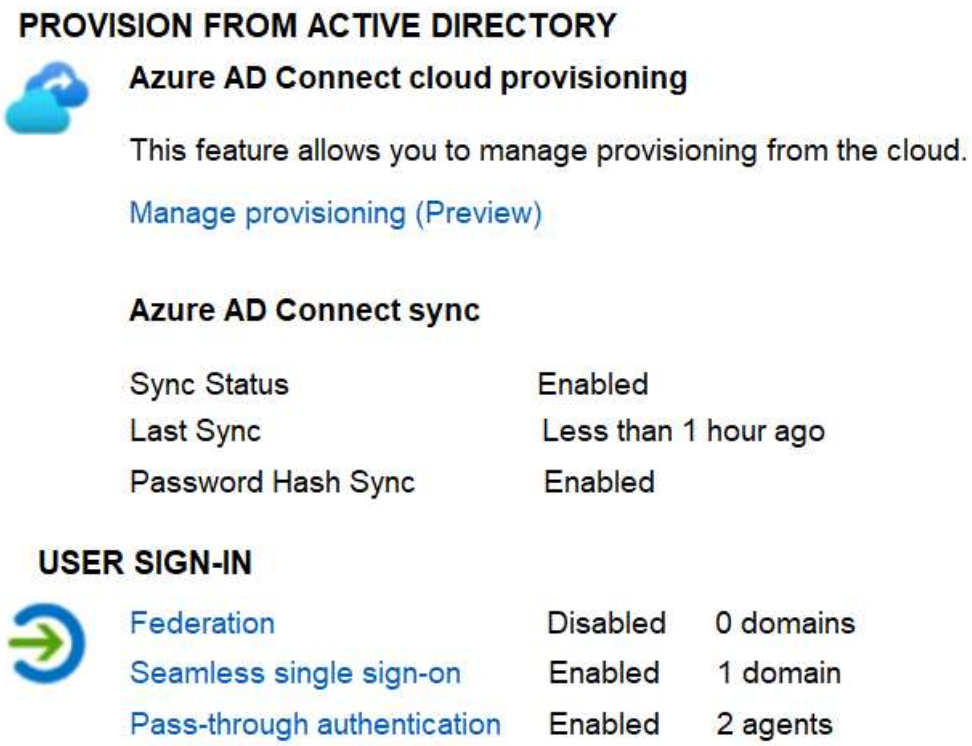
Correct Answer: *B*
This is not a permissions issue.
The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

Ahema 1 year, 1 month ago
Correct answer
upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure Active Directory (Azure AD) tenant named contoso.com as shown in the exhibit.



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

Community vote distribution
A (80%) B (20%)

MartiFC Highly Voted 1 year, 2 months ago
Yes is correct. change UPN
upvoted 6 times

TechMinerUK Most Recent 4 months ago

Selected Answer: A

Changing the UPN to one which is verified and enabled for SSO will allow the user to sign into Microsoft 365 services.
Granted the better option would be to verify fabrikam.com and ensure it is enabled for SSO, that isn't an option here so A is the best available choice

upvoted 2 times

charat 4 months, 1 week ago

Selected Answer: A

The goal is to ensure the user can access Azure AD resources. If that's the case, it would not matter if the user is logging in with a differ UPN suffix. Therefore, A is correct.

upvoted 2 times

gaem 4 months, 2 weeks ago

Selected Answer: B

Correct answer

upvoted 1 times

jjong 1 year ago

this qns came out in exam today

upvoted 3 times

gkp_br 1 year, 4 months ago

Yes for me. User already sync, probably with @contoso.com UPN. So, user can sign in with user2@contoso.com.

upvoted 4 times

jc1993 1 year, 5 months ago

This is correct. Granted you wait for the next AD sync.

upvoted 2 times

forummj 4 months, 1 week ago

You could just push it through with Start-ADSyncSyncCycle -PolicyType Delta Powershell and you don't have to wait.

upvoted 1 times

Josephsmith 1 year, 5 months ago

Not sure this is right. The answer is No

upvoted 3 times

chaoscreater 1 year, 3 months ago

If you're "not sure" then why give an "answer"? Doesn't help anyone. Just don't comment next time.

upvoted 22 times

venwaik 1 year, 2 months ago

You two should swap names :)

upvoted 3 times

Nico95 1 year, 1 month ago

Maybe answer C "not sure" is hidden

upvoted 3 times

TimurKazan 1 year, 1 month ago

Agree. He aint want no smoke

upvoted 1 times

BoxGhost 5 months, 1 week ago

The question hints that contoso.com is already verified since it's been configured as part of AD connect. Therefore changing the UPN contoso.com will allow the user to sign in and solves the issue.

upvoted 1 times

HOTSPOT -

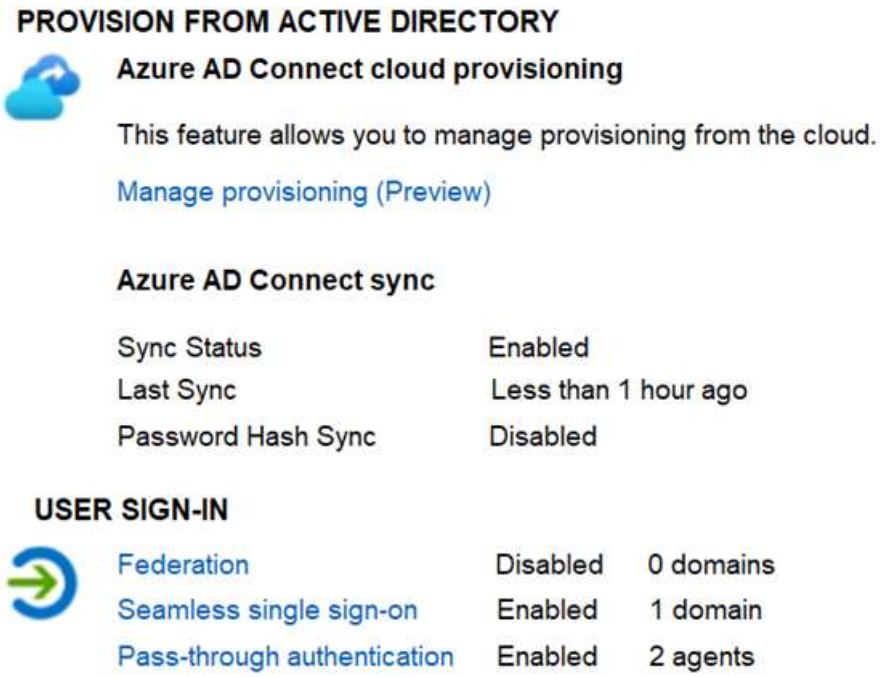
Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

- Contoso.com
- East.contoso.com

The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest syncs to an Azure Active Directory (Azure AD) tenant named contoso.com as shown in the exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

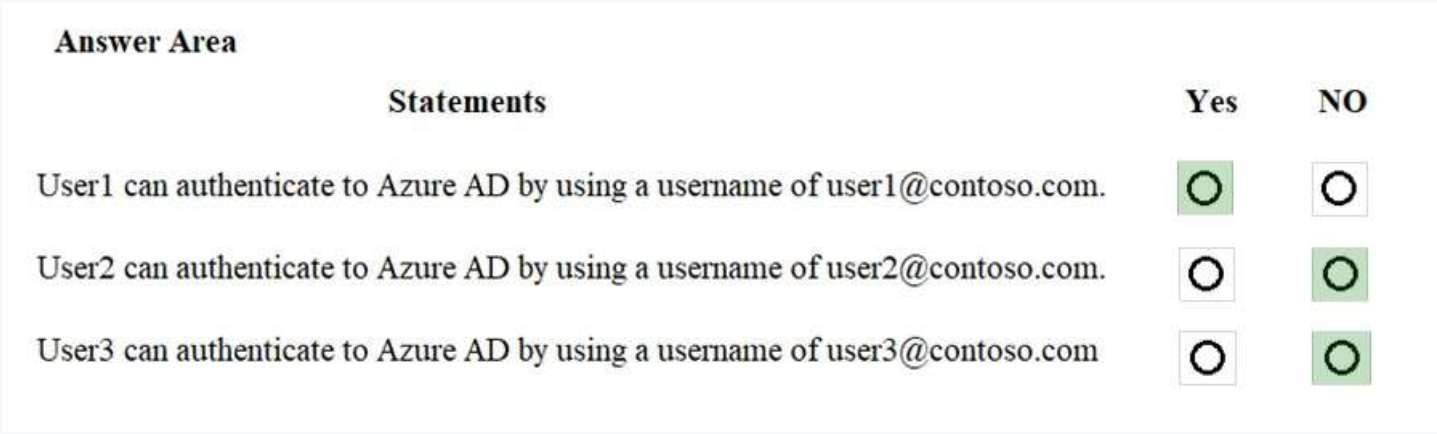
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	NO
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	○	○
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	○	○
User3 can authenticate to Azure AD by using a username of user3@contoso.com	○	○

Correct Answer:



Box 1: Yes -

The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.

Box 2: No -

The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.

Box 3: No -

The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

mkuczynski Highly Voted 1 year, 5 months ago

User1 can authenticate by on-prem AD. YNN

upvoted 9 times

Cheekypoo Most Recent 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

TechMinerUK 3 months, 2 weeks ago

I believe the answer provided is correct as from the question it appears that contoso.com is setup in AzureAD and Microsoft 365 howev because the users still have their east.contoso.com and fabrikam.com set as their UPNs in Active Directory when they synchronise to AzureAD they will likely have a UPN like the bellow:

%username%@contoso.onmicrosoft.com

Because of this they would need to use the above username to sign in succesfully or on Active Directory they would need their UPN suf changing to contoso.com before actioning a delta sync to update their AzureAD profiles with the correct domain for their username

upvoted 2 times

jjong 1 year ago

i agree with the ans provided YNN.
Box 2: No – (need to use east.contoso.com)
Box 3: No – (not configured as domain on on-prem AD)

upvoted 4 times

melatocaroca 1 year, 3 months ago

The default configuration in Azure AD Connect sync assumes:

Each user has only one enabled account, and the forest where this account is located is used to authenticate the user. This assumption for password hash sync, pass-through authentication and federation. UserPrincipalName and sourceAnchor/immutableID come from t forest.
Each user has only one mailbox.
The forest that hosts the mailbox for a user has the best data quality for attributes visible in the Exchange Global Address List (GAL). If there's no mailbox for the user, any forest can be used to contribute these attribute values.
If you have a linked mailbox, there's also an account in a different forest used for sign-in.

So user 1 default user 2 and user 3 default, user 2 and 3 can not login without change their UPN

upvoted 1 times

PandaTuga 1 year, 3 months ago

the answer for this exam is YNN
But you could actually sync the 3 users with sync rule that would set all cloud UPN accounts to @contoso.com and they all will be able t sign-in that way

upvoted 2 times

Gus01 1 year, 5 months ago

All answers should be NO. Password Hash Sync is disabled so user1 cannot authenticate to Azure only Pass Thru is working so has to Authenticate to On Prem AD

upvoted 3 times

Lyl4ch 1 year, 4 months ago

It doesn't specify that he must use the same on-prem password.

upvoted 1 times

Jaxon_84 1 year, 4 months ago

Passthrough authentication is on however, so, that allows for authentication.

upvoted 6 times

J0J0 1 year, 3 months ago

but not on Azure AD. Authentication happens in on-premise.

upvoted 1 times

venwaik 1 year, 2 months ago

if pass-through is on, that means that the on-prem pass-through module is installed and is communicating with Azure. Theref
User1 can succesfully sign in with the on-prem password.
Authentication for User 1 = Yes

upvoted 3 times

Rudelke 2 months, 4 weeks ago

Question asks if you can authenticate TO Azure AD (by any means).
What you are thinking about is "can User one be authenticated BY Azure AD using...."

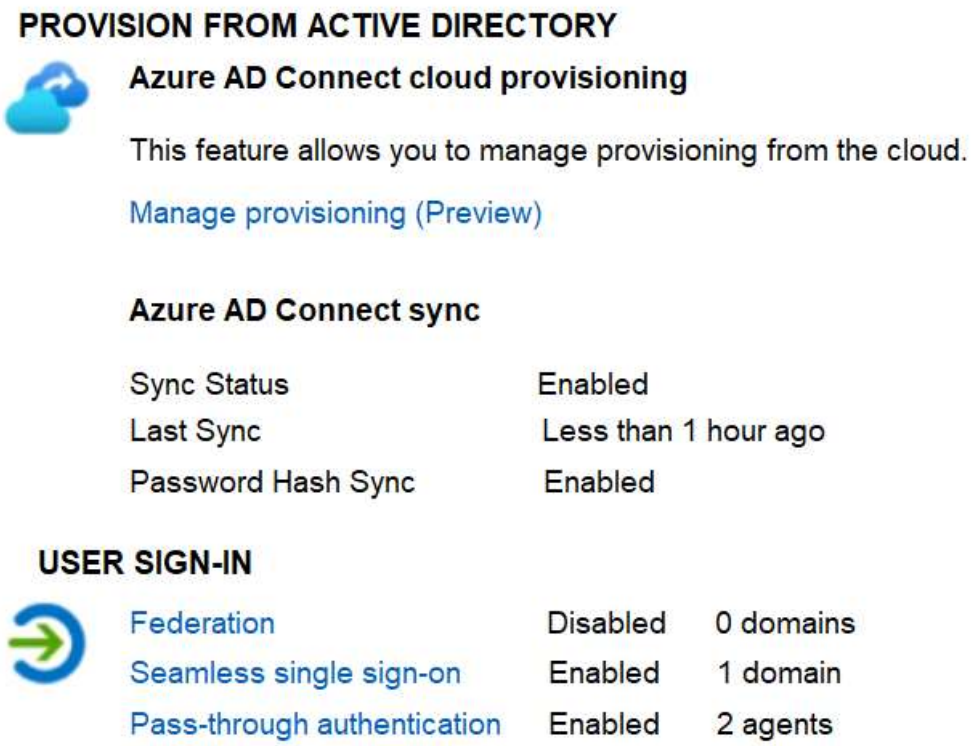
Questions about who is doing the authorisation (AD vs AAD) also happen but it's not this one.

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure Active Directory (Azure AD) tenant named contoso.com as shown in the exhibit.



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Azure Active Directory admin center, you assign User2 the Security reader role. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This is not a permissions issue so you do not need to assign the Security Reader role.
The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of
User2 to user2@contoso.com.

Community vote distribution
B (100%)

Ash473 Highly Voted 1 year, 1 month ago
In today's exqm
upvoted 7 times

TimurKazan 1 year, 1 month ago

we are glad for you

upvoted 8 times

Moderator Most Recent 3 months, 3 weeks ago

Selected Answer: B

Correct answer given.

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a Microsoft

SharePoint Online site named Site1 and the accounts shown in the following table.

Name	Account type
UserA	User
UserB	User
GroupA	Security group

You have an on-premises server named Server1 that contains a folder named Folder1. Folder1 contains the files shown in the following table.

Name	Permission
File1	User1: Full control
File2	User2: Modify
File3	Group1: Full control

The User1, User2, and Group1 accounts have the security identifiers (SIDs) shown in the following table.

Name	SID
User1	S-1-5-21-4534338-1127018997-2609994386-1304
User2	S-1-5-21-4534338-1127018997-2609994386-1228
Group1	S-1-5-21-4534338-1127018997-2609994386-1106

You use the SharePoint Migration Tool to migrate Folder1 to Site1. You preserve the file share permissions and use the following user mapping file.

S-1-5-21-4534338-1127018997-2609994386-1304, UserA@Contoso.com, FALSE

S-1-5-21-4534338-1127018997-2609994386-1228, UserB@Contoso.com, FALSE

S-1-5-21-4534338-1127018997-2609994386-1106, GroupA, TRUE

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point

Hot Area:

Answer Area

Statements	Yes	No
UserA is the owner of File1 on Site1.	○	○
UserB is the owner of File2 on Site1.	○	○
GroupA is the owner of File3 on Site1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
UserA is the owner of File1 on Site1.	○	○
UserB is the owner of File2 on Site1.	○	○
GroupA is the owner of File3 on Site1.	○	○

dngd Highly Voted 1 year, 5 months ago

Correct, You don't specify owner in User mapping file:
Column A: From the source location, enter the log in name of the user. Required.
Column B: On the destination site, enter the principal username. Required.
Column C: If the principal username on the destination site is an Active Directory (AD) group, enter TRUE. If it's not an AD group, enter FALSE. Required.

https://docs.microsoft.com/en-us/sharepointmigration/mm-user-mapping-file

upvoted 18 times

lucidgreen 1 year, 5 months ago

Besides that, it doesn't indicate anywhere that the users were owners in the first place! If I didn't know any better, that would be the first thing I look for.
Dumb, dumb question...

upvoted 16 times

tf444 9 months, 1 week ago

Agreed %100.

upvoted 3 times

NHaikes 2 months, 2 weeks ago

This is also relevant:
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating
No ownership is given, only full-control, which may be interpreted as ownership.

upvoted 2 times

bLINDmONKEY Highly Voted 1 year ago

Sure is a tricky question if you haven't done an SPMT before.
The mapping file is correct and will give the Full Control users and groups owner permissions.
The mapping file maps the onprem users and groups to the AAD users and groups. To do this is maps the SIDs stored in the file/folder properties to the AAD users or groups appropriately.
So User1 is mapped to UserA etc.
If you have DirSync\AD Connect then you don't have to worry about the mapping if you have everything synced nicely.

So the answer is actually YNY - User B is just a member thanks to the modify permissions.

Tell me otherwise.

upvoted 13 times

Durden871 6 months, 2 weeks ago

What if there are more than one member with Full Control?

upvoted 2 times

Archie_Bunker 11 months, 3 weeks ago

Agree with bLINDmONKEY. The TRUE/FALSE in the User Mapping File is for declaring if it's a group or not, and users with Full Control rights in Sharepoint are listed as Owners.

Answer is YNY

upvoted 3 times

jinxie 10 months, 4 weeks ago

I disagree, as far as I can tell it's false for all. The user's current rights will be migrated but I do not see anything of owner there. user1 and group1 will just receive full control on the file. and user 2 will indeed be a member but nowhere does it specify file owner

upvoted 2 times

Storm 6 months, 1 week ago

Why not test before answering?
Full Control translates to owner in sharepoint

upvoted 2 times

forummj Most Recent 4 months, 1 week ago

Based on https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating I'm going to go for an answer of YNY - Specifically, the "Permissions conditions and results" portion of the link above.

My reasoning is that Full Control permissions are only provided to those users in the Owners Group of a document library, and becaus Full Control on-prem AD is translated to Full Control on SP, it stands to reason that User1 will be made an Owner of that file/library.

Likewise, User2 will not due to only having the Modify on-prem permission, which will translate to Edit, Members group in SP.

GroupA will be migrated to a new group that has Full Control permission. Although they won't be in a named group of Owners, they wi still have the same effective permissions.

Hell, I'm probably wrong, but the logic appears sound to me.

upvoted 1 times

joergsi 8 months, 1 week ago

Checking this out:
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating

You find the following about migration of user rights:
There are three types of permissions that will be migrated: Read, Write, and Full control.
- If a file has Write permission for user1, then the file will be set to Contribute for user1 in SPO.
- If a file has Read permission for user1, then the file will be set to Read for user1 in SPO.
- For Full control permission, the file will be migrated as Full control in SPO.

=> Call me a nitpicker, transfer of ownership is not mentioned here at all!

upvoted 3 times

joergsi 8 months, 1 week ago

User Mapping File information:
https://docs.microsoft.com/en-us/sharepointmigration/create-a-user-mapping-file-for-data-content-migration

upvoted 2 times

LillyLiver 8 months, 1 week ago

I haven't ever user the SPMT. So this question was not super easy for me. Since there is a lot of back-and-forth in the discussions on thi question, I setup my tenant to match the conditions of this question to get the actual answer. I also matched my on-prem user accoun and the files to migrate. Same user permissions on the files, same permission preservation on the files in SPMT, and same User Mappi file.

The answers are:
UserA is the owner: Yes
UserB is the owner: No
GroupA is the owner: Yes

It looks like it really comes down to that Full Control perm on the file share. If a user has that level permission, then they will also be an owner in the SPO site after migration.

So I 2/3's don't agree with the given answer to this question.

It's possible I f'ed this practical test up somehow, but the SPMT is pretty straight forward and there isn't a lot of ambiguity in the use. S am confident with my results.

upvoted 8 times

kanag1 8 months, 3 weeks ago

The Given Answer is correct. Please refer the link attached below.
If a file has Write permission for user1, then the file will be set to Contribute for user1 in SPO. If a file has Read permission for user1, th the file will be set to Read for user1 in SPO. For Full control permission, the file will be migrated as Full control in SPO.
##Nothing mentioned about converting a Full control to owner##
Reference: https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating

upvoted 2 times

PDR 9 months, 2 weeks ago

I think these doc pages are key to reference for the answer for this:
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating
https://docs.microsoft.com/en-us/sharepoint/understanding-permission-levels

Problem here is that whilst it states that Full Control permissions will get mapped it doesnt state that user with full control will be migrated and given OWNER .... but the owner role is the only one that has Full Control permissions when using the Permissions setting a Sharepoint site, so logically you would assume that a user given Full Control must be an OWNER.
Need to test to be sure though as something being logical and it actually being the case isnt a given!

upvoted 1 times

PDR 9 months, 2 weeks ago

tested this with a migration:
User1 with Full Control on file1 is given OWNER permission on the file when migrated to Sharepoint Online site
User2 with modify on file1 is given 'Can Edit' permission on the file when migrated to Sharepoint Online site but not Owner.

Whilst not relevant to the question it is worth noting that the migrated users do not get any Sharepoint Site level permissions so do
actually have permission to access the document library and would have to access using a direct link.

upvoted 1 times

TimurKazan 11 months, 1 week ago

YNY just read the links and articles if you are not familiar with SPMT

upvoted 3 times

melatocaroca 1 year, 4 months ago

S-1-5-21-4534338-1127018997-2609994386-1304, UserA@Contoso.com, FALSE
S-1-5-21-4534338-1127018997-2609994386-1228, UserB@Contoso.com, FALSE
S-1-5-21-4534338-1127018997-2609994386-1106, GroupA, TRUE
So, user 1 and 2 FALSE, will not be migrated, trick in group name also, Group1 in mapping csv field typo error GroupA so Will not match
group1 will not have any permission

upvoted 6 times

melatocaroca 1 year, 4 months ago

Also csv does not contain all the required fields
CSV file format for migration needs six columns.
o The first three are source values that detail where your data is currently located.
o The remaining three columns indicate
o the site,
o document library,
o optional subfolder
o where you're migrating your data to.
All six columns must be accounted for in the file, even if you don't need a value for a given field.
https://docs.microsoft.com/en-us/sharepointmigration/mm-user-mapping-file

upvoted 2 times

jinxie 10 months, 4 weeks ago

The TRUE FALSE flag here is to indicate if the entity is an AD group or not. it has nothing to do with the migration. as per MS article c
https://docs.microsoft.com/en-us/sharepointmigration/mm-user-mapping-file

The following example uses Excel to create the CSV file.

Start Excel.

Enter the values for your user-mapping.

Column A: From the source location, enter the log in name of the user. Required.

Column B: On the destination site, enter the principal username. Required.

Column C: If the principal username on the destination site is an Active Directory (AD) group, enter TRUE. If it's not an AD group, ent
FALSE. Required.

Close and save as a comma-delimited (*.csv) file.

upvoted 2 times

You have a DNS zone named contoso.com that contains the following records.

```
@            IN    SOA  dns1.contoso.com. hostmaster.contoso.com. (
                             539            ; serial number
                             900            ; refresh
                             600            ; retry
                             86400          ; expire
                             3600         ) ; default TTL

@            NS         dns1.contoso.com.

@            MX    10   server1.contoso.com.
@            TXT        ( "v=spf1 a include:server1.contoso.com -all" )
Server1      A          193.77.10.15
```

You purchase a Microsoft 365 subscription.

You plan to migrate mailboxes to Microsoft Exchange Online.

You need to configure Sender Policy Framework (SPF) to support Exchange Online.

What should you do?

A. Add an additional TXT record.

B. Modify the TXT record.

C. Modify the expire interval of the SOA record.

D. Modify the default TTL of the SOA record.

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-spf-in-office-365-to-help-prevent-spoofing?view=o365-worldwide#next-steps- after-you-set-up-spf-for-office-365

Community vote distribution

B (100%)

Taophyc Highly Voted 1 year, 4 months ago

Definitely B - Modify TXT Record

upvoted 8 times

spg987 Highly Voted 1 year, 1 month ago

It was in my exam

upvoted 7 times

Cheekypoo Most Recent 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Moderator 2 months ago

Selected Answer: B

Still a valid question (July 30th 2022).

upvoted 1 times

charat 4 months, 1 week ago

Selected Answer: B

On the MS-100 05/22. Answer is B

upvoted 2 times

dumpmaster 8 months, 2 weeks ago

Selected Answer: B

Right.

upvoted 2 times

mackypatio 1 year, 4 months ago

modify txt record in domain register

v=spf1 include:spf.protection.outlook.com ip4:<IP ADDRESS of other authorized smtp source> ~all

upvoted 4 times

jc1993 1 year, 5 months ago

Just to add clarity, the TXT record here is incorrect for two reasons. It's syntax format is incorrect and we will also need to input the supplied SPF provided by the O365 setup page.

upvoted 5 times

DRAG DROP -

You have a Microsoft 365 subscription and a DNS domain. The domain is hosted by a third-party DNS service.

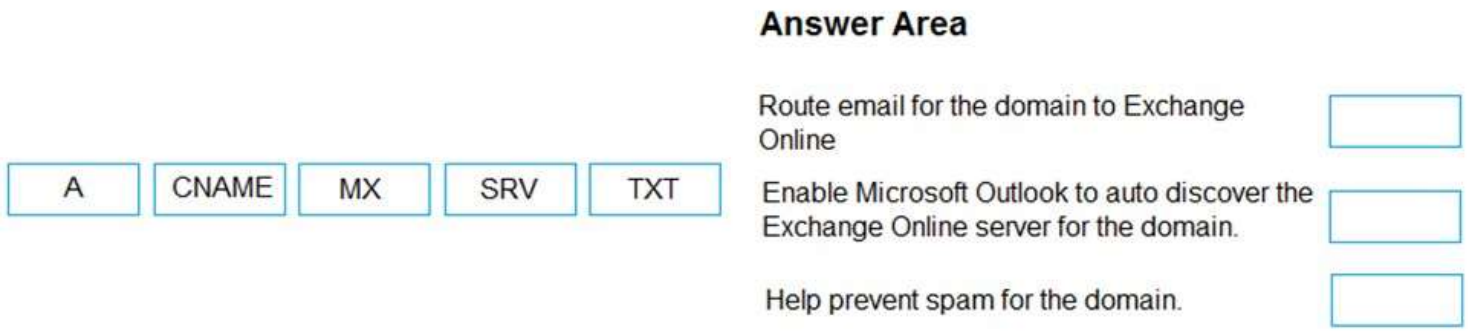
You plan to add the domain to the subscription.

You need to use Microsoft Exchange Online to send and receive emails for the domain.

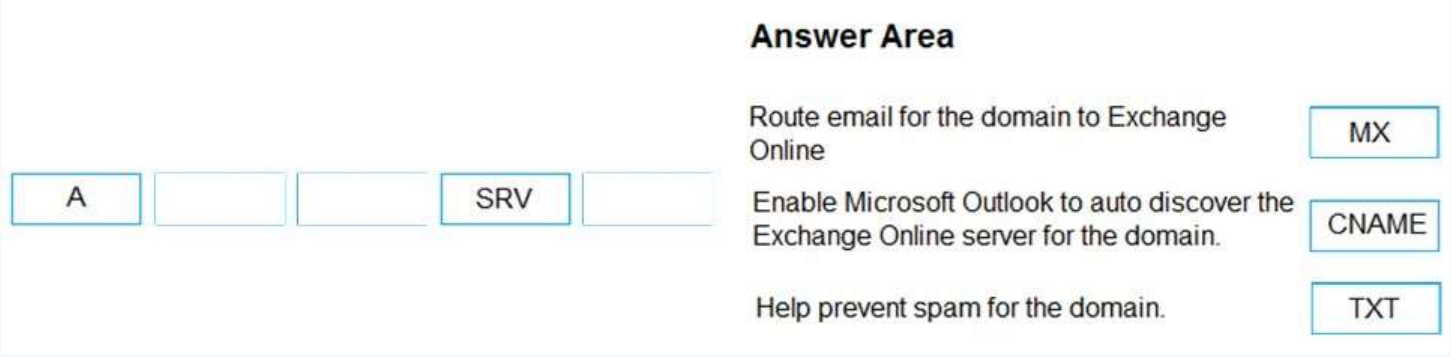
Which type of DNS record should you add to the DNS zone of the domain for each task? To answer, drag the appropriate records to the correct tasks. Each record may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: MX -

When you update your domain's MX record, all new email for anyone who uses your domain will now come to Microsoft 365.

Box 2: CNAME -

Add CNAME records to connect other service. You can add CNAME records for each service that you want to connect.

Box 3: TXT -

Add or edit an SPF TXT record to help prevent email spam

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide

Cheekypoo 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Moderator 3 months, 3 weeks ago

Correct answers given.

upvoted 2 times

dumpmaster 8 months, 2 weeks ago

Correct.

upvoted 1 times

spg987 1 year, 1 month ago

correct.https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide

upvoted 2 times

MartiFC 1 year, 2 months ago

MX > Register to Exchange Servers
CNAME > Register to Autodiscover
TXT > Register for put the IPs autorized senders

upvoted 3 times

HOTSPOT -

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

In the subscription, an administrator adds two custom domains named sub1.contoso.onmicrosoft.com and sub2.contoso.onmicrosoft.com and the objects shown in the following table.

Name	Type	Attribute
Group1	Distribution group	Group email: group1@sub1.contoso.onmicrosoft.com
Group2	Mail-enabled security group	Group email: group2@sub2.contoso.onmicrosoft.com
Group3	Office 365 group	Group email: group3@contoso.onmicrosoft.com
User1	User	Username: user1@sub1.contoso.onmicrosoft.com
Contact2	Contact	Email: contact2@sub2.contoso.onmicrosoft.com

You plan to delete sub1.contoso.onmicrosoft.com and sub2.contoso.onmicrosoft.com.

Which objects must you delete or modify manually before you can delete the domains? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Sub1.contoso.onmicrosoft.com:

- User1 only
- Group1 only
- User1 and Group1 only
- User1, Group1, and Group3
- No resources must be deleted or modified

Sub2.contoso.onmicrosoft.com:

- Contact2 only
- Group2 only
- Contact2 and Group2 only
- Contact2, Group2, and Group3
- No resources must be deleted or modified

Correct Answer:

Answer Area

Sub1.contoso.onmicrosoft.com:

- User1 only
- Group1 only
- User1 and Group1 only
- **User1, Group1, and Group3**
- No resources must be deleted or modified

Sub2.contoso.onmicrosoft.com:

- Contact2 only
- Group2 only
- **Contact2 and Group2 only**
- Contact2, Group2, and Group3
- No resources must be deleted or modified

Anything with an email address in the subdomain needs to be removed or moved to another domain. This includes users, mail-enabled security groups, distribution groups and contacts. Office 365 groups will also need to be removed from the subdomains (they cannot be moved to another domain). However, the only Office 365 group in this question is in the parent domain, not the subdomains.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/remove-a-domain?view=o365-worldwide

TheWallPTA Highly Voted 1 year, 6 months ago

Think answer should be:
Sub1: User1 and Group1 Only
Sub2: Contact2 and Group2 Only
?

upvoted 83 times

extrankie 9 months ago

i think same

upvoted 1 times

Bobalo 1 year, 2 months ago

As usernames revert automatically, but email addresses do not, shouldn't the answer be:
Sub1: Group1 only
Sub2: Contact2 and Group2 only

upvoted 2 times

LillyLiver 8 months, 1 week ago

Totally agree. You can't delete a domain with any resources still assigned to that domain. Even if using PS and using a -Force the operation will fail.

So, yes;
Sub1: User1 and Group1
Sub2: Contact2 and Group2

upvoted 4 times

lucidgreen Highly Voted 1 year, 5 months ago

Why Group 3? It doesn't belong to either of the subdomains. If it mattered, it would have to be in both answers!
Nope!
1: User 1 and Group 1
2: Contact 2 and Group 2

upvoted 44 times

JEricThomas610 Most Recent 1 month, 1 week ago

Thank you all for confirming what I was thinking. Makes no sense as Group 3 has nothing to do with what they are asking for.

upvoted 3 times

Rudelke 3 months ago

Soooooooo here is the deal. If you use admin panel you can remove domain that still has users assigned (provided you can fall back to something). So technically you don't HAVE TO change any user/group/contact manually.

If you use PS, than yes, it will error out and you need to change objects manually (switch -force doesn't force anything. It responds "yes confirmation dialog).

Assuming M$ want's you to find what will be afected the answeer provided seems correct.

upvoted 1 times

chriscert 3 months, 3 weeks ago

The question has no sense beacuse is not possible to delete a subdomain of onmicrosoft.com after creation. You can add at most 5 onmicrosoft.com subdomains, but you cannot remove them later even if no objects are linked to them - test it!

upvoted 2 times

manis73 3 months, 2 weeks ago

I Just deleted one and it worked :)

upvoted 2 times

chriscert 3 months, 1 week ago

I don't know what you have actually tested, because I CANNOT delete my sub.mytestdomain.onmicrosoft.com after creation, as official MS doc states:

You can't remove your onmicrosoft domain. Microsoft 365 needs to keep it around because it's used behind the scenes for your subscription. But you don't have to use the domain yourself after you've added a custom domain. If you choose to create a new onmicrosoft.com domain, it cannot be removed. You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.

https://docs.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide

upvoted 1 times

Durden871 7 months, 1 week ago

I genuinely believe some of these questions are wrong on purpose because they don't want people getting 100% on these tests.

There is absolutely no way the parent domain matters, at all.

I thought contacts might, but tell me where in this MS document does it mention changing/deleting contacts?
https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/remove-a-domain?view=o365-worldwide

upvoted 3 times

Mahesh_A 7 months, 1 week ago

Sub1: User1 & Group1
Sub2: Contact2 & Group2
Even though contact can exist without domain, we need to think from working scenario point of view. If Contact2 is not deleted/modifi then mail sent to contact2 will result in delivery failure

upvoted 2 times

Durden871 6 months, 2 weeks ago

But the question is explicitly asking, "Which objects must you delete or modify manually before you can delete the domains?"
It isn't asking about anything other than what is absolutely required to remove the sub domains. Since your answer indicates that a contact can survive without a domain, the answer would suggest that we don't NEED to delete the contact.

upvoted 2 times

Durden871 6 months, 2 weeks ago

Meant to say we don't NEED to delete or modify the contact.

upvoted 1 times

PDR 9 months, 2 weeks ago

Another one where we have to guess a bit what they want and is a bit ambigous (too common unfortunately)
I would probably go for :
Sub1: User 1 and Group1 only
Sub2: Group2 only

Even though I agree that user1 would automatically revert anyway, I am working on the assumption that they are looking for you to choose the objects that will be impacted.
A contact can have any domain and it doesnt in fact even check to see if it is a valid domain when you create them (try it by adding a contact with a made up domain, sub domain, sub domain of your tenants onmicrosoft.com - all work without error)

upvoted 6 times

davem90 10 months, 1 week ago

Correct answer is:
Sub1: User1 and Group1 Only
Sub2: Group2 Only
https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/remove-a-domain?view=o365-worldwide

upvoted 19 times

FumerLaMoquette 10 months, 1 week ago

Contacts do not need to be deleted as their external to your tenant. I agree with davem90

upvoted 5 times

TechMinerUK 3 months, 2 weeks ago

I also agree with davem90 and FumerLaMoquette as contacts can be for external users, as such if Group2 has it's UPN suffix changed then there should be no errors raised when the domain is removed from 365.

I have had tenants before where I have removed the domain despite having a contact present with the domain name (Used for testing) and there were no issues.

upvoted 1 times

fofo1960 12 months ago

Based on the following link
https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/remove-a-domain?view=o365-worldwide
The answer should be:
A: - User1 - Group1
B: Group2
In the article there is nothing related to contact

upvoted 8 times

nicolasganzaroli 1 year ago

Just tested in my tenant
Sub1: User1 and Group1 Only
Sub2: Group2 Only

https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/remove-a-domain?view=o365-worldwide

upvoted 15 times

Kas1990 5 months, 3 weeks ago

Correct - you don't need a verified domain to add exchange contacts (as they'll mostly be external domains)

upvoted 1 times

TimurKazan 1 year ago

I think nothing is neccesarry to be deleted before deleting domain. Also, I think that would be too easy question - you can actually chec for each entity which domain it belongs to and solve question that way. That's why I would go with NO resources MUST be deleted or modified

upvoted 1 times

AlexLiourtas 10 months, 1 week ago

it says "delete or modify"

upvoted 1 times

lengySK 1 year, 1 month ago

I think the answers are:
Sub1: Group1 only
Sub2: Contact2 and Group2 only

upvoted 1 times

saikelu 1 year, 3 months ago

I believe contact is independent on domain.

upvoted 5 times

birzorirko 1 year, 3 months ago

Group3 is an error.

upvoted 7 times

Tryggr 1 year, 3 months ago

Why do we need to change any of them? You can, but it doesn't appear to be a requirement. The note at the bottom of the linked articl states "when you remove a domain, user accounts will revert back to the ".onmicrosoft.com" address as the Primary SMTP/UserprincipalName." It also states in the article that when you remove the domain, if it's reference by lots of groups, lists, users then it can take hours to complete.
https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/remove-a-domain?view=o365-worldwide

upvoted 4 times

PandaTuga 1 year, 3 months ago

The MS statement is correct for usernames. I tried on a tenant and successfully removed the domain and all usernames were revert to the default tenant name.
But if you have them associated with an SMTP address you need to manually remove alias and primary addresses from them first. A groups are totally dependent of the email address. So you need to delete or change them to another SMTP.
Contacts can have email based the tenant domains, but these are independent if you delete them or change

upvoted 1 times

PandaTuga 1 year, 3 months ago

My answer would be 1:Group 1, 2: Group 2

upvoted 1 times

J0J0 1 year, 3 months ago

That might be MS statement, but even their support engineers best practices is to remove all dependencies to the domain manu (UPN/SMTP Address). We have performed a domain migration from different tenant (like tenant-to-tenant migration). We only migrate one of the domains of the other tenant. And part of that process is to update UPN and email addresses.

As the question states, "Which objects must you delete or modify manually..." I'll go with:
1: User 1 and Group 1
2: Group 2 (contact is independent)

upvoted 2 times

michszym 1 year, 2 months ago

The question is not about "best practicies" but what you must delete or modify manually before you can delete the domains?" As I wrote before, I tested it - I was able to delete subdomain without modifying anythind - usernames and primary email add changed to initial onmicrosoft.com domain (the same with User, Contact (mail user), Distribution List and Mail-enabled securit group). Aliases in that subdomain from all these objects just dissappeared - no need to modify or remove them manually.
So in my opinion answer should be "No resources must be deleted or modified"

upvoted 4 times

michszym 1 year, 2 months ago

OK, I see it - it's related to the place from you are working - I was able to delete subdomain without of modifying anything from M365 Admin Center (all magic was done by Microsoft). When I try to do the same from Azure Portal I have to modify Users and Groups. The question does not say from which portal you have to do it... If we assume that from Azure Portal so need to modify Box1: User1 and Group1, Box2: Group2 (Contact2 if it is Mail user)

upvoted 2 times

michszym 1 year, 2 months ago

Agree, I've tested it in my tenant - I've added subdomain, created all these objects and remove subdomain - all usernames revert to initial onmicrosoft.com domain (even contact - I've created mail user and assign address in onmicrosoft.com subdomain)
The question is: "Which objects must you delete or modify manually before you can delete the domains?" - both answers are: "no resources must be deleted or modified"

upvoted 8 times

TimNov 1 year, 4 months ago

1: User 1 and Group 1
2: Contact 2 and Group 2

Not sure why Group3 is relevant as it's the parent domain.

upvoted 4 times

Question #65 *Topic 2*

You have an on-premises Microsoft Exchange Server organization that contains 100 mailboxes.
You have a hybrid Microsoft 365 tenant.
You run the Hybrid Configuration wizard and migrate the mailboxes to the tenant.
You need to ensure that Microsoft 365 spam filtering is applied to incoming email.
What should you do?

A. Run the Hybrid Configuration wizard again.

B. Update the Sender Policy Framework (SPF) TXT record to point to the on-premises Exchange IP address.

C. Run the Azure Active Directory Connect wizard again.

D. Update the MX record to point to Exchange Online.

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/manage-mailboxes-using-microsoft-365-or-office-365

Community vote distribution

PeterC Highly Voted 1 year, 4 months ago
Correct - MX Records
1.) Add Custom Domain
2.) Move Mailboxes
3.) Update DNS Records (MX, SPF) to point to EXO

https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/manage-mail-flow-for-multiple-locations#manage-mail-flow-wher
some-mailboxes-are-in-microsoft-365-or-office-365-and-some-mailboxes-are-on-your-organizations-email-servers
upvoted 6 times

Cheekypoo Most Recent 2 months ago
Was in my exam today 05/08/22.
upvoted 1 times

TechMinerUK 3 months, 2 weeks ago
Selected Answer: D
D is the correct answer as in order to use Microsoft Defender for Office 365 you must route all mail via Microsoft Exchange Online meaning the MX records must be updated to point to Exchange Online.

This means D is the only sensible answer
upvoted 2 times

FelixG 8 months, 1 week ago
Selected Answer: D
Answer is D
upvoted 1 times

blackbic 1 year ago
The Microsoft learning harps on using them for spam. They give examples to point the MX record to them, and then have a connector
send the mail to onsite exchange. That's why D was chosen for the answer.
upvoted 3 times

zacmzee 1 year ago
Correct answer in my opinion is updating MX record. EOP provides built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect your network from spam transferred through email. This action alone can help meet the requirement specified in the question.
upvoted 2 times

stromnessian 1 year, 2 months ago
Ref: https://docs.microsoft.com/en-us/exchange/transport-routing

If you change your MX record to point to the Exchange Online Protection service in Microsoft 365 or Office 365: This is the recommend configuration for hybrid deployments. All messages sent to any recipient in either organization will be routed through the Exchange Online organization first. A message addressed to a recipient that's located in your on-premises organization will be routed first throug your Exchange Online organization and then delivered to the recipient in your on-premises organization. This route is recommended if you have more recipients in your Exchange Online organization than in your on-premises organization. This configuration option is required for Exchange Online Protection to provide scanning and blocking for spam.

upvoted 1 times

Flojo2 1 year, 4 months ago

The answer is not create an MX record. In the question, that is already done as you are migrating the mailboxes already. The question a specifically about preventing Spam. This is done with a SPF TXT record. https://docs.microsoft.com/en-us/microsoft-365/admin/get-help with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide

upvoted 1 times

Flojo2 1 year, 4 months ago

None of these answers prevent the spam. Since the only answer that talks about SPF TXT record is pointing to on premise Exchange server. Uggh, another really bad question with no good answer.

upvoted 3 times

J0J0 1 year, 3 months ago

Agreed. No correct answer here.

upvoted 1 times

saikelu 1 year, 3 months ago

If Mx record is pointed to EOP then the on-premise mailflow can take protection from EOP. That's what asked in the question. So correct.

upvoted 2 times

jc1993 1 year, 5 months ago

In order for EOP to be applied, email must be routed through M365 Exchange. Of the available options, only updating the MX record would do this. Even though the question does not allude to the current MX configuration but is assumed due the existing config being Hybrid.

upvoted 3 times

Question #66 *Topic 2*

You have an on-premises Microsoft Exchange Server organization that contains 500 mailboxes and a third-party email archive solution.
You have a Microsoft 365 tenant that contains a user named User1.
You plan to use the User1 account to perform a PST import of the archive mailboxes to the tenant.
Which two roles does User1 require to perform the import? The solution must use the principle of least privilege. Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Mail Recipients

B. Exchange admin

C. Records Management

D. Mailbox Import Export

E. eDiscovery Manager

Correct Answer: *AD*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/importing-pst-files-to-office-365?view=o365-worldwide

Community vote distribution
AD (100%)

Sr15 Highly Voted 1 year, 3 months ago
"Consider creating a new role group in Exchange Online that's specifically intended for importing PST files to Office 365. For the minim level of privileges required to import PST files, assign the Mailbox Import Export and Mail Recipients roles to the new role group, and th add members."
upvoted 10 times

melatocaroca 1 year, 3 months ago
You right, but they do not give use that option

You can add the Mailbox Import Export role to the Organization Management role group.
Or you can create a new role group, assign the Mailbox Import Export role, and then add yourself or other users as a member.

Additionally, to create import jobs in the Security & Compliance Center, one of the following must be true:

You have to be assigned the Mail Recipients role in Exchange Online.

By default, this role is assigned to the Organization Management and Recipient Management roles groups.

Or

You have to be a global administrator in your organization.

Reference
https://docs.microsoft.com/en-us/microsoft-365/compliance/faqimporting-pst-files-to-office-365?view=o365-worldwide
upvoted 2 times

charat Most Recent 4 months, 1 week ago
Selected Answer: AD
This question was in exam on 05/22/22
upvoted 2 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 2 times

Ash473 1 year, 1 month ago
In labs today
upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a Microsoft Office 365 tenant.
You suspect that several Office 365 features were recently updated.
You need to view a list of the features that were recently updated in the tenant.
Solution: You review the Windows release health in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Reference:
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-release-health-now-available-in-the-admin-center/ba-p/2235908

Community vote distribution
B (100%)

Kosta Highly Voted 1 year, 1 month ago
We have seen this question many times. The answer is B: No. We can see the updates in the Message Center.
upvoted 22 times

LouahZA Highly Voted 1 year, 1 month ago
B, should be Message Center
upvoted 13 times

sliix Most Recent 7 months, 4 weeks ago
Selected Answer: B
Pretty direct answer actually.
upvoted 1 times

VictorPCS 8 months, 1 week ago
Selected Answer: B
Should be called Message Center
upvoted 1 times

Blankenp 8 months, 1 week ago
Selected Answer: B
Windows Release Health shows known issues for supported versions, not update features.
upvoted 1 times

LillyLiver 8 months, 1 week ago
Selected Answer: B
Yeah, the Message Center is where you'll see this info. B for sure.
upvoted 1 times

davem90 9 months, 1 week ago
Selected Answer: B
B, Message Center
upvoted 1 times

PDR 9 months, 2 weeks ago
Selected Answer: B
definitely B
upvoted 1 times

opek 9 months, 2 weeks ago

Selected Answer: B

Message Center

upvoted 1 times

AlexLiourtas 10 months, 1 week ago

Selected Answer: B

b for obviously reasons

upvoted 3 times

Jcbrow27 10 months, 2 weeks ago

i think would be B, because it is not windows is office 365.

upvoted 1 times

L33D 10 months, 2 weeks ago

Selected Answer: B

Message Center

https://docs.microsoft.com/en-us/microsoft-365/admin/manage/message-center?view=o365-worldwide

Message center is the primary way we communicate the timing of individual changes in Microsoft 365. See Stay on top of Microsoft 365

upvoted 4 times

Deevibes 10 months, 3 weeks ago

The Windows release health experience on the admin centre also offers insights into known issues, workarounds, and resolutions relat to Windows updates. so the Answer is B

upvoted 1 times

Minniebeast 11 months ago

It does seem like you can see the version of all your Microsoft products and the update history
https://docs.microsoft.com/en-us/windows/deployment/update/check-release-health

It is stated in this link and there are screen shots so A: Yes

upvoted 1 times

extrankie 11 months, 1 week ago

it says Windows release Health not Service heal, so A is correct

upvoted 1 times

Jcbrow27 10 months, 2 weeks ago

But release health is for Windows not for Office 365.

upvoted 2 times

xofowi5140 11 months, 2 weeks ago

Windows release health
Find information about known issues for currently supported versions of the Windows operating system.

upvoted 1 times

fofo1960 12 months ago

WTF, it should be Message Center..
This is wrong Answer is B

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a Microsoft Office 365 tenant.
You suspect that several Office 365 features were recently updated.
You need to view a list of the features that were recently updated in the tenant.
Solution: You use the Service health option in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide

Community vote distribution
B (100%)

Davidchercm 9 months ago
Selected Answer: B
message centre
upvoted 1 times

xofowi5140 11 months, 2 weeks ago
Service health
View the health status of all services that are available with your current subscriptions.
upvoted 1 times

Rlcky 1 year ago
Correct its B, Message Center
upvoted 2 times

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains the resources shown in the following table.

Name	Type
User1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group

User1 is assigned a Microsoft Office 365 Enterprise E5 license.

You need to create a mail flow rule that will add a recipient to the To field of email messages sent to a specific address.

Which resources can you use in the mail flow rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If the messages are sent to:

- User1 only
- User1 and Group3 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3

Add the following recipients to the To field:

- User1 only
- User1 and Group3 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3

Correct Answer:

Answer Area

If the messages are sent to:

- User1 only
- User1 and Group3 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3

Add the following recipients to the To field:

- User1 only
- User1 and Group3 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3

Reference:

https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/common-message-approval-scenarios

pozzetttt 1 week, 4 days ago

1. User 1
2. User 1

https://admin.exchange.microsoft.com/ --> Mail Flow --> Rules --> + --> Create a new rule --> Apply this rule if "The recipient is.." --> Do t

following "Add these recipients to the To box"
Only user 1 can be added.
upvoted 1 times

PmgCosta 5 months ago
Yes i can confirm, is not possible to add DL, O365Groups, MailEnabledSecurityGroups.

When you try to save you get an error, only User1 can be added added to TO Filed
upvoted 1 times

PmgCosta 5 months ago
The same for the first question if you select a DL or MailEnabledSecurityGroup you get

error
SentTo predicate does not allow distribution groups.
upvoted 1 times

VictorSaiz 5 months, 1 week ago
I have tested this, when creating a new mail flow rule you can add all the resources except the Microsoft 365 Group to “Apply this rules The recipient is”, and, regarding the second question, the same happens, you can add all the resources except the Microsoft 365 Group “Do the following...Redirect the message to”. So the answer is C&C.
upvoted 2 times

sandi412 5 months, 1 week ago
I tested and in both casses only user mailbox could be used.
upvoted 2 times

briandavisrtr 5 months, 1 week ago
I agree with sandi412. I tested and got the same results. You have to click save to get the error. You can select groups when creat the rule but when you hit save you get the error.
1st part = https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/conditions-and-exceptions#recipients
2nd part = https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions
upvoted 2 times

miszczswiata 1 month ago
Just to be sure, did you test security mail-enabled group and O365 group as well? It says

Adds one or more recipients to the To field of the message. The original recipients can see the additional addresses.
Note: In Exchange Online, you can't add a distribution group as a recipient.
upvoted 1 times

renrenren 2 weeks, 2 days ago
Tested. Only user mailbox could be used in both.
upvoted 1 times

DRAG DROP -

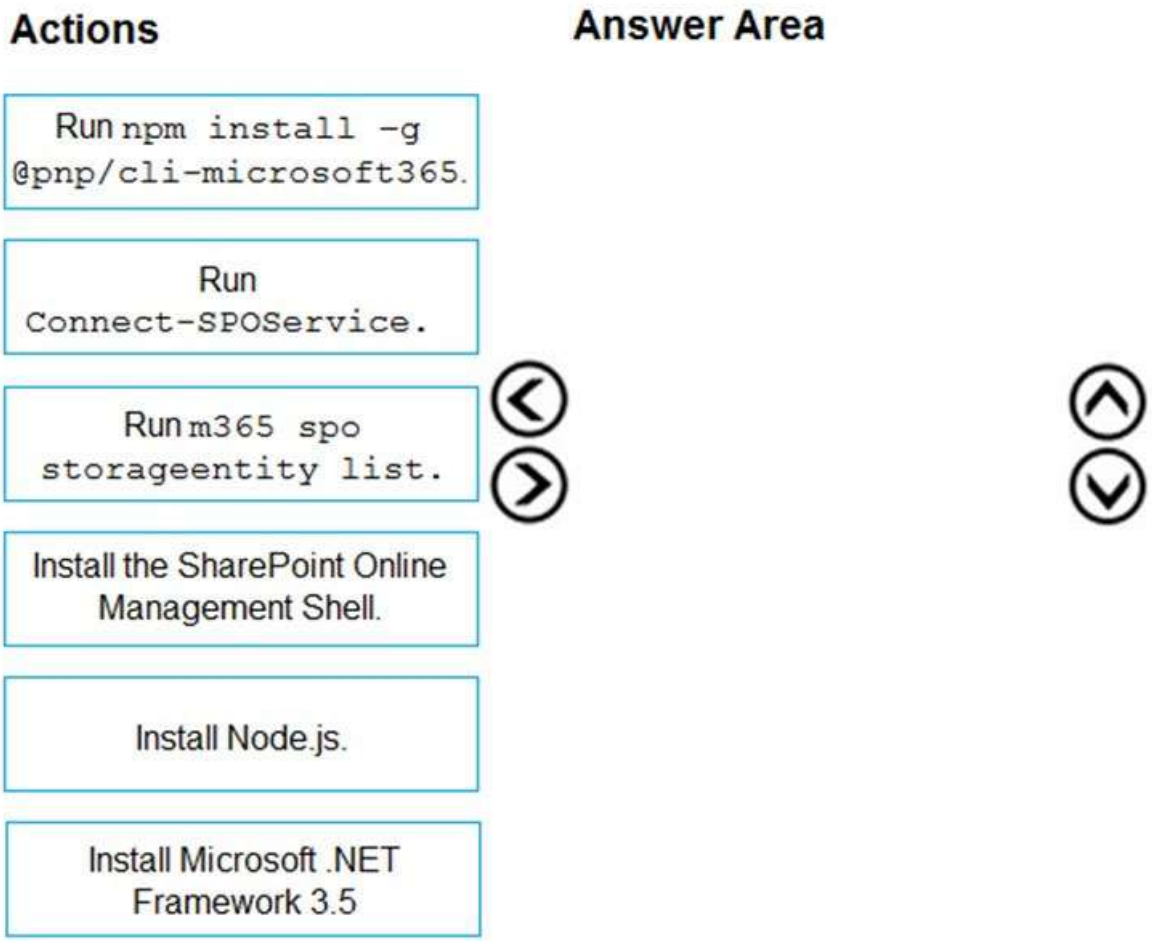
You have a Microsoft 365 E5 tenant.

You have a computer named Computer1 that runs Windows 10.

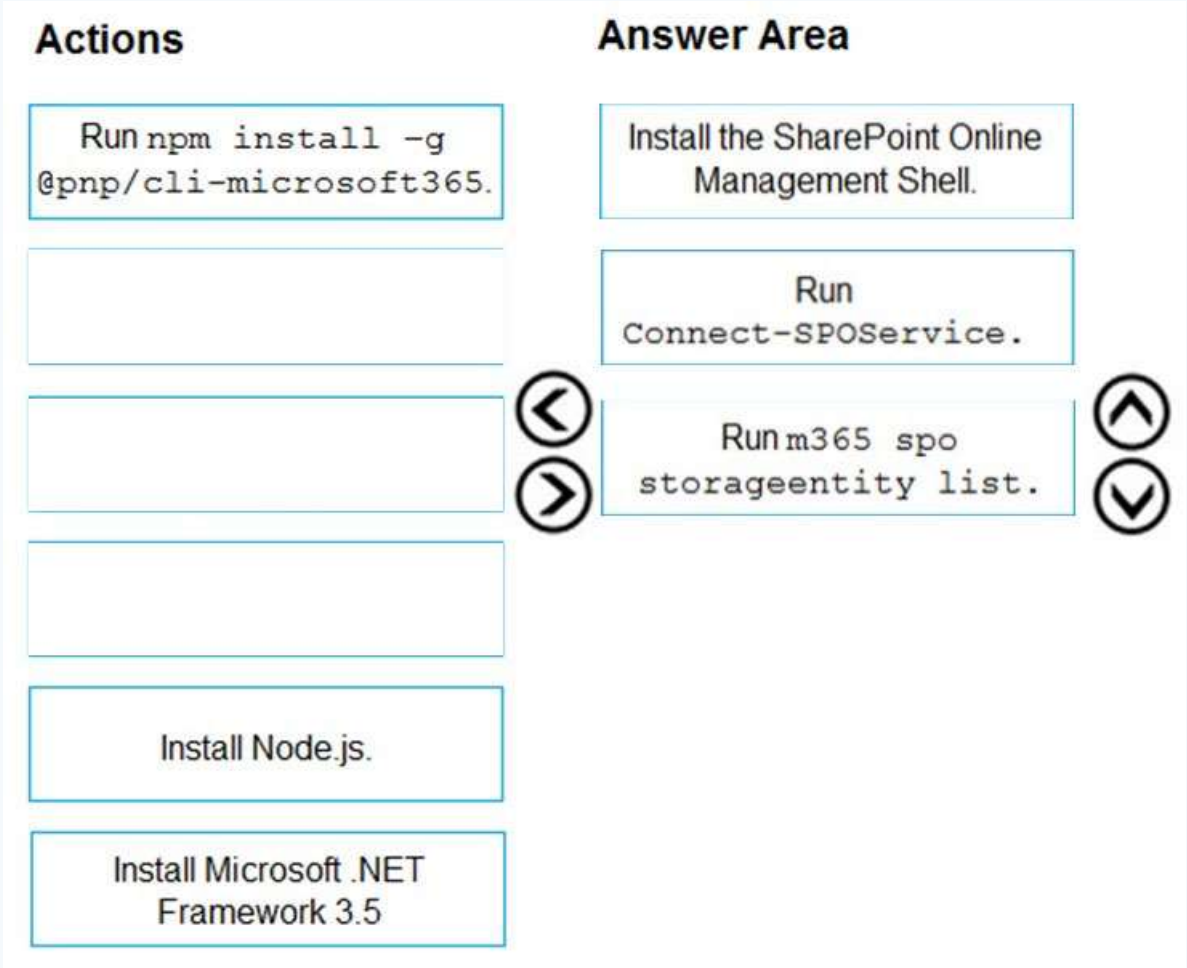
You need to list the properties of a Microsoft SharePoint Online tenant by using the CLI for Microsoft 365 on Computer1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/sharepoint/dev/spfx/tenant-properties?tabs=o365cli https://docs.microsoft.com/en-us/powershell/sharepoint/sharepoint-online/connect-sharepoint-online?view=sharepoint-ps&redirectedfrom=MSDN

Miqqo 5 months, 1 week ago

https://devblogs.microsoft.com/microsoft365dev/getting-started-office365-cli-powershell/
https://pnp.github.io/cli-microsoft365/user-guide/installing-cli/

You don't use the SPO module to input CLI for M365 commands based on these sources. The product name is specifically mentioned in the question so I believe the CLI for M365 is what is being tested here. My assumption is that this is the new cross-platform way and yo should therefore know it. You need Node.js, the install command and then based on the options available the command to do what the question asks.

Is this really in the scope of this exam? Who knows.

upvoted 1 times

MEG 5 months, 1 week ago

1. Install Node.js
2. Run npm install -q @pnp/cli-microsoft365
3. Run m365 spo storageentity list

Referenz...
for 1. > https://pnp.github.io/cli-microsoft365/user-guide/installing-cli/#prerequisites
for 2. > https://pnp.github.io/cli-microsoft365/user-guide/installing-cli/#install-the-cli-for-microsoft-365_1
for 3. > https://pnp.github.io/cli-microsoft365/cmd/spo/storageentity/storageentity-list/#spo-storageentity-list

But to run the command you have to login first with "m365 login". Reference login > https://pnp.github.io/cli-microsoft365/user-guide/connecting-office-365/#log-in-to-microsoft-365

upvoted 3 times

Balvosko 5 months, 1 week ago

Wrong.
-install node.js => it is prerequisite to run CLI
"To use the CLI for Microsoft 365 you need Node.js. The CLI has been tested with Node.js versions 6 and higher, but we recommend yo use the Node.js"
-> then install CLI itself
-> run the command m365 spo storageentity list

Question #71 *Topic 2*

Your company has an on-premises Microsoft SharePoint Server environment and a Microsoft 365 subscription.
When users search for content from Microsoft 365, you plan to include content from the on-premises SharePoint Server environment in the results.
You need to add crawled metadata from the on-premises SharePoint Server content to the Microsoft Office 365 search index.
What should you do first?

A. Run the SharePoint Migration Tool.

B. Create a site collection that uses the Basic Search Center template.

C. Create a site collection that uses the Enterprise Search Center template.

D. Run the SharePoint Hybrid Configuration Wizard.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/sharepoint/hybrid/plan-hybrid-federated-search

Mercious 2 days, 8 hours ago
A has nothing to do with content search on SharePoint
upvoted 1 times

PmgCosta 5 months, 1 week ago
Prerequisites for outbound hybrid search

Before you can configure SharePoint Server to display hybrid federated search results, you have to complete all the steps in the Config hybrid federated search from SharePoint Server to SharePoint in Microsoft 365 - roadmap. You must also do the following:

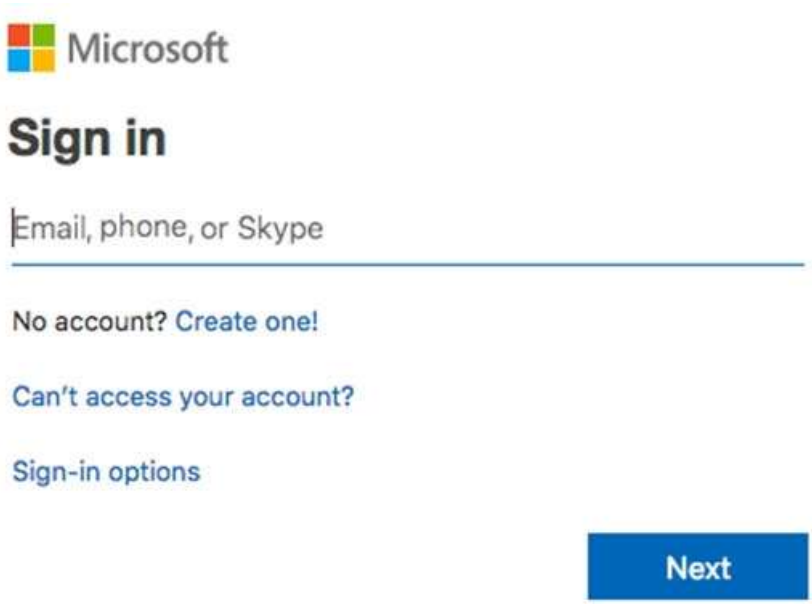
Perform at least one crawl in the SharePoint Server deployment, so that there is content in the SharePoint Server search index. (The SharePoint in Microsoft 365 content must also be crawled, but you don't have to attend to that because SharePoint in Microsoft 365 cra its content automatically.) For more info, see Manage crawling in SharePoint Server.

Create an enterprise Search Center in the SharePoint Server deployment by using the Enterprise Search Center template to create a ne site collection. For more info, see Create a Search Center site in SharePoint Server.
upvoted 1 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@abc.com
Microsoft 365 Password: XXXXXXXX
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 1111111111 -



You need to modify Lynne Robbins to meet the following requirements:
- Lynne Robbins must be able to view the service dashboard and the Microsoft Office 365 Message center.
- Lynne Robbins must be able to create Microsoft support requests.
- The solution must use the principle of least privilege.

To answer, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*
1. In the admin center, go to Role assignments. Choose the Azure AD tab to view the admin roles available for your organization.
2. Select the Service Support Administrator role.
3. Select Assigned admins > Add.
4. Type Lynne Robbins' display name or username, and then select the her from the list of suggestions.

5. Select Save, and then Lynne Robbins will be added to the list of assigned admins.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/assign-admin-roles?view=o365-worldwide https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#service-support-administrator

Balvosko 5 months, 1 week ago

Correct
Service Support admin =>
Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:
- Open and manage service requests
- View and share message center posts
- Monitor service health

https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 tenant that contains the users shown in the following table.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com
User3	User3@contoso.com

Microsoft Exchange Online has the mail flow rules shown in the following table.

Name	Priority
Rule1	0
Rule2	1
Rule3	2

Rule1 has the following settings:

- Apply this rule if: The sender is 'user1@contoso.com'
- Do the following: Redirect the message to 'user2@contoso.com'
- Choose a mode for this rule: Enforce
- Stop processing more rules: Disabled

Rule2 has the following settings:

- Apply this rule if: The recipient is 'user2@contoso.com'
- Do the following: Append the disclaimer 'Disclaimer1 message'; and fall back to action ignore if the disclaimer can't be inserted
- Choose a mode for this rule: Enforce
- Stop processing more rules: Enabled

Rule3 has the following settings:

- Apply this rule if: The recipient is 'user2@contoso.com'
- Do the following: Append the disclaimer 'Disclaimer2 message'; and fall back to action ignore if the disclaimer can't be inserted
- Choose a mode for this rule: Enforce
- Stop processing more rules: Disabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Hot Area:

Answer Area

Statements	Yes	No
If User1 sends an email to User3, User3 receives the email.	○	○
If User1 sends an email, a disclaimer is added to the email.	○	○
If an email is sent to User2, two disclaimers are added to the email.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If User1 sends an email to User3, User3 receives the email.	○	○
If User1 sends an email, a disclaimer is added to the email.	○	○
If an email is sent to User2, two disclaimers are added to the email.	○	○

Reference:

https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

miszczswiata Highly Voted 1 month ago

Should bo No, No, No
There is nothing about adding disclaimer for messages sent by User1 (unless the recipient is User2)
Only 1 disclaimer can be added as the middle rule says stop processing more rules

upvoted 6 times

HenryVo 4 weeks ago

Confirm. I tested.

upvoted 1 times

renrenren Highly Voted 2 weeks, 2 days ago

Tested. User1 sends an email to anyone, User2 will receive and contains a disclaimer.
Answer: NYN

upvoted 5 times

SkullRage Most Recent 1 day, 9 hours ago

I agree with xyz213

upvoted 1 times

relaxswe 2 weeks, 4 days ago

If sender is user1 then messages will be redirected to user2 so user3 will never get the message. More rules will be processed so a disclaimer will be added with rule2 to the message that was originally sent to user3.
Answer should be NO on Q1 (User3 never gets the email)

As all emails sent from user1 are redirected to user2 and rule2 adds a disclaimer and stops processing more rules answer should be YE to Question2 (A disclaimer is added to message)

As rule2 is processed before rule3 and rule2 states that no further rules should be processed we should not be able to get two disclaimers.
Answer to Question 3 should be no.

So, answers should be "no, yes, no"

upvoted 5 times

xyz213 2 weeks, 4 days ago

Shouldn't it be N/Y/N?
1:
Mail gets redirected to user2 (No Mail for User3)

2:
User1 sends an email (no matter who the recipient is) it gets redirectet to User2.
So Rule 2 applies and Disclaimer1 gets added and further rule processing is stopped.

3:
Only 1 disclaimer can be added as rule2 says stop processing more rules

upvoted 4 times

ckanoz 3 weeks, 3 days ago

Should be No, No, No

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 tenant that uses Microsoft Exchange Online.

You have two partner companies that have domains named adatum.com and litwareinc.com.

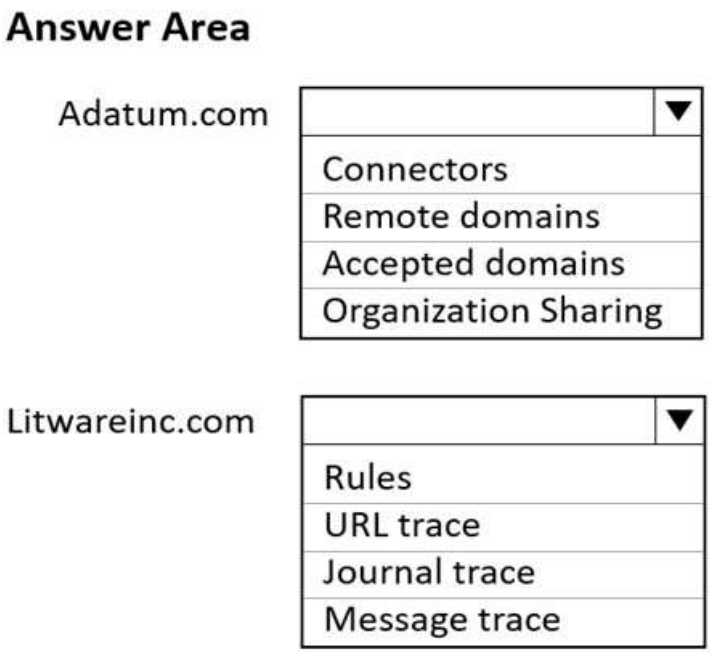
You need to meet the following requirements:

- Connections to the email server of adatum.com must use TLS and require that the remote server has a digital certificate.
- Email messages sent to litwareinc.com that contain the word `confidential` must be encrypted.

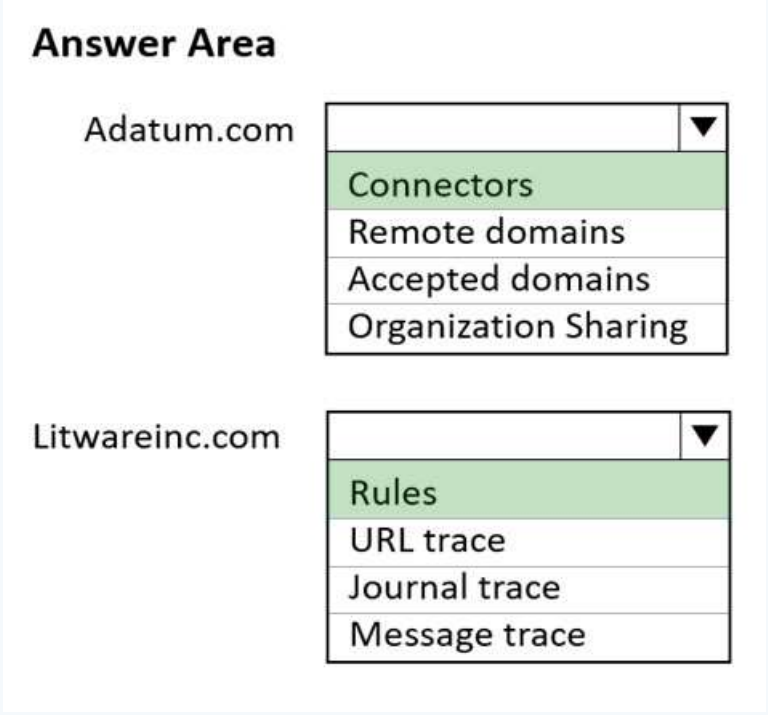
What should you use for each domain? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



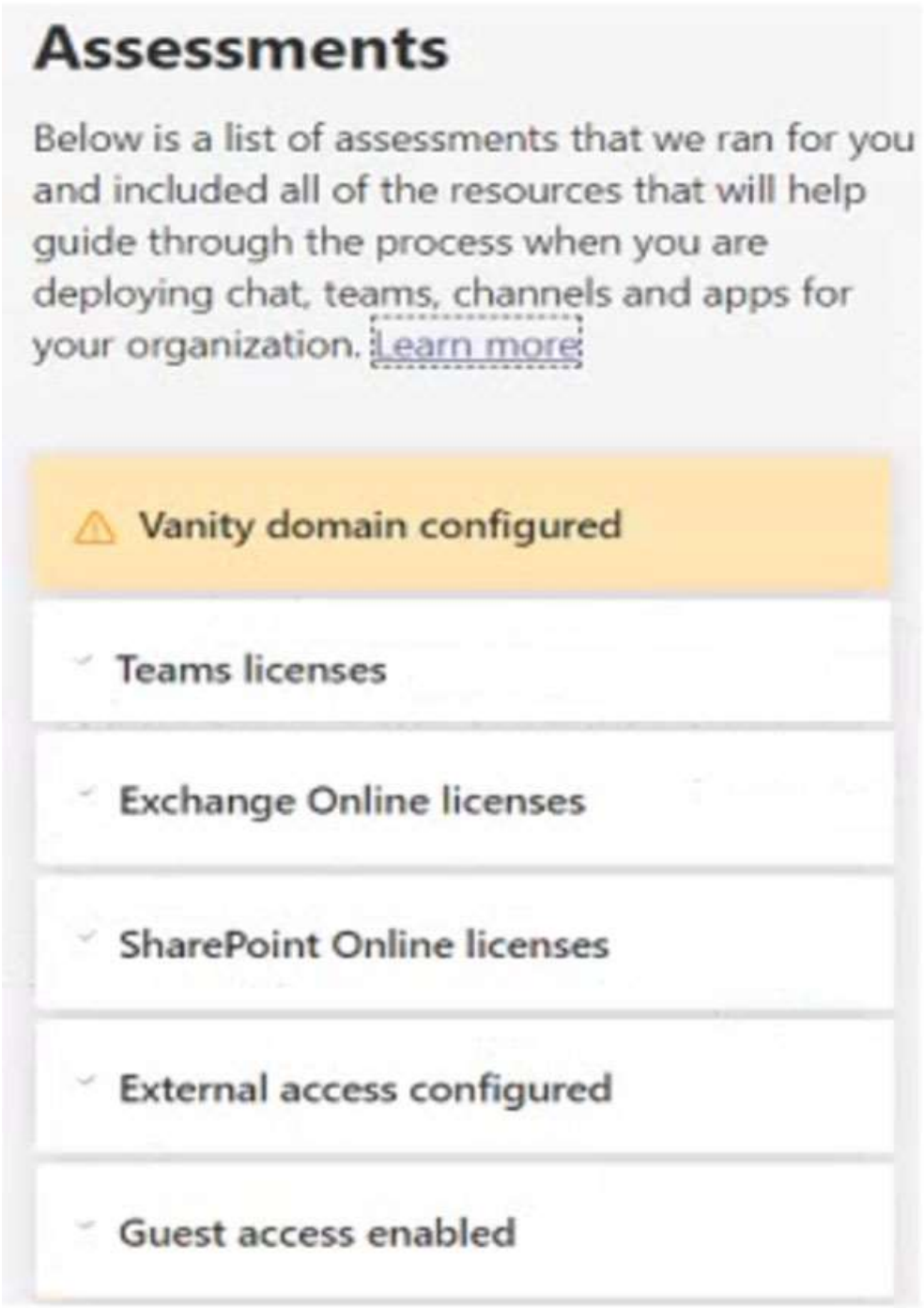
Correct Answer:



Reference:

https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner https://thevaliantway.com/2019/01/encrypting-email-office-365-azure-information-protection/

You have a Microsoft 365 subscription that contains a domain named contoso.onmicrosoft.com.
Advisor for Teams assessments for the chat teams, channels, and apps workloads are shown in the following exhibit.



You need to resolve the assessment warning.
What should you do first?

A. Add and verify a new custom domain.

B. Assign a user the Domain Name Administrator role.

C. Add a TXT record to the contoso.onrmcrosoft.com domain.

D. From the Microsoft 365 admin center, update the Organization information profile.

Correct Answer: *A*
Assessment test includes Vanity domain configured: It tells you whether there's a non-@onmicrosoft.com domain configured for your tenant (for example,
@contoso.onmicrosoft.com). You can use the @onmicrosoft.com domain, of course, or you can configure a vanity domain - your choice.
Reference:
https://docs.microsoft.com/en-us/microsoftteams/use-advisor-teams-roll-out

Topic 3 - Question Set 3

Question #1 *Topic 3*

You have a Microsoft 365 subscription.
You plan to enable Microsoft Azure Information Protection.
You need to ensure that only the members of a group named PilotUsers can protect content.
What should you do?

A. Run the Add-AadrmRoleBaseAdministrator cmdlet.

B. Create an Azure Information Protection policy.

C. Configure the protection activation status for Azure Information Protection.

D. Run the Set-AadrmOnboardingControlPolicy cmdlet.

Correct Answer: *D*
If you don't want all users to be able to protect documents and emails immediately by using Azure Rights Management, you can configure user onboarding controls by using the
Set-AadrmOnboardingControlPolicy cmdlet.
Note: Set-AadrmOnboardingControlPolicy from the AADRM module is now deprecated. After July 15, 2020, this cmdlet name will be supported only as an alias to its replacement in the AIPService module. Set-AipServiceOnboardingControlPolicy Sets the user on-boarding control policy for Azure Information Protection.
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/activate-service

ctfalci Highly Voted 2 years, 2 months ago
Answer: D
Explanation
If you don't want all users to be able to protect documents and emails immediately by using Azure Rights Management, you can config user onboarding controls by using the Set-
AadrmOnboardingControlPolicy
References:
https://docs.microsoft.com/en-us/azure/information-protection/activate-service
upvoted 16 times

AlexanderSaad Highly Voted 2 years, 6 months ago
The answer is correct, just more information on the cmdlet:
This cmdlet from the AADRM module is now deprecated. After July 15, 2020, this cmdlet name will be supported only as an alias to its replacement in the AIPService module.
https://docs.microsoft.com/fr-fr/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps
upvoted 8 times

charat Most Recent 4 months, 2 weeks ago
Updated module is Set-AipServiceOnboardingControlPolicy
:https://docs.microsoft.com/en-us/powershell/module/aipservice/set-aipserviceonboardingcontrolpolicy?view=azureipps
upvoted 1 times

emilianogalati 1 year ago
Further Update.
July, 5th 2021

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/azure-aip-portal-label-amp-policy-management-admin-experience/ba-p/2182678
upvoted 2 times

emilianogalati 1 year ago
UPDATED ON July, 5th 2021:
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/azure-aip-portal-label-amp-policy-management-admin-experience/ba-p/2182678
upvoted 1 times

venwaik 1 year, 3 months ago
New answer would be: Set-AipServiceOnboardingControlPolicy as the AADRM module is deprecated. Answer is correct in though.

upvoted 7 times

airairo 1 year, 4 months ago

This is in ms 101

upvoted 4 times

bog23 1 year, 6 months ago

D. should be Set-AipServiceOnboardingControlPolicy.
The AADRM cmd is deprecated from July 2020

upvoted 4 times

Bempa 1 year, 8 months ago

This cmdlet from the AADRM module is now deprecated. After July 15, 2020, this cmdlet name will be supported only as an alias to its replacement in the AIPService module.

https://docs.microsoft.com/en-us/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps

upvoted 2 times

mkoprivnj 1 year, 9 months ago

D for sure!

upvoted 3 times

sam76 2 years, 3 months ago

I guess the answer should be B. Sice the Question relates to Azure Information Protection.

upvoted 2 times

kmjunk 2 years, 3 months ago

I thought that as well.

upvoted 1 times

DiscGolfer 2 years, 2 months ago

The Set-AadrmOnboardingControlPolicy cmdlet sets the policy that controls user on-boarding for Azure Rights Management. This cmdlet supports a gradual deployment by controlling which users in your organization can protect content by using Azure Rights Management.

You must use PowerShell to set this configuration; you cannot do this configuration by using a management portal.

https://docs.microsoft.com/en-us/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps

upvoted 1 times

JOCER 2 years, 7 months ago

I agree WoneAix

upvoted 1 times

WoneSix 2 years, 7 months ago

This is the type of answer I like to see - it not only gives a reference, it says what must be done to answer the question.

upvoted 5 times

ExamStudy68 2 years, 8 months ago

The reference in answer points to Set-AipServiceOnboardingControlPolicy

The link for Set-AadrmOnboardingControlPolicy shown in answer is https://docs.microsoft.com/en-us/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps

Now confused as to when to use which...

upvoted 4 times

Hamster5000 2 years, 8 months ago

Set-AipServiceOnboardingControlPolicy is replacing Set-AadrmOnboardingControlPolicy . The latter will now be just an alias and stil work but new exams may have the new one as the answer.

upvoted 11 times

SMHH 2 years, 7 months ago

Yup
https://docs.microsoft.com/en-us/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps#description

upvoted 1 times

h3nk13 2 years, 1 month ago

This cmdlet from the AADRM module is now deprecated.

upvoted 3 times

Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

- Deleted a folder from the second-stage Recycle Bin if Microsoft SharePoint
- Opened a mailbox of which the user was not the owner

Reset a user password -

▪

What should you use?

A. Microsoft Azure Active Directory (Azure AD) audit logs

B. Microsoft Azure Active Directory (Azure AD) sign-ins

C. Security & Compliance content search

D. Security & Compliance audit log search

Correct Answer: *A*

You can view the required information in the audit logs. The Azure AD audit logs provide records of system activities for compliance. To access the audit report, select Audit logs in the Activity section of Azure Active Directory.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

Tryggr Highly Voted 1 year, 3 months ago

D is the correct answer.
"Because you can search for the following types of user and admin activity in Microsoft 365:
User activity in SharePoint Online and OneDrive for Business
Admin activity in Exchange Online (Exchange admin audit logging)"
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

upvoted 19 times

Agbantu Highly Voted 1 year, 3 months ago

Definitely D, Audit log search from the SCC (now compliance.microsoft.com)

upvoted 10 times

Contactfornitish Most Recent 2 months, 1 week ago

Selected Answer: D

A, are you joking? Deletion of files isn't privileged that way

upvoted 2 times

Contactfornitish 2 months, 2 weeks ago

Selected Answer: D

Been doing since a while

upvoted 2 times

Stiobhan 4 months ago

1000% answer is D. Just ran exact audit on my tenant and all choices are there 😄

upvoted 2 times

jru24 5 months, 2 weeks ago

yes, I tested it. D is correct

upvoted 1 times

Wojer 9 months, 1 week ago

just test it and its D

upvoted 2 times

PDR 9 months, 2 weeks ago

also D

upvoted 1 times

tcmaggio 9 months, 2 weeks ago

Selected Answer: D

D for me.

upvoted 3 times

kaveri123 9 months, 3 weeks ago

Should be letter D. I made some test in my LAB and compare the two. Azure Audit logs only see who reset the password. Audits Logs > Filter the activity

Security & Compliance > Audit has all the necessary options that mentioned on this questions (Passwords, Deleted Folder, Opened a mailbox)

upvoted 4 times

tcmaggio 10 months, 1 week ago

Selected Answer: D

I also vote D.

upvoted 5 times

Mavula 10 months, 2 weeks ago

So why don't they update this answer to be D?

upvoted 2 times

L33D 10 months, 3 weeks ago

Selected Answer: D

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

upvoted 5 times

PandaTuga 1 year, 3 months ago

D
"Need to find if a user viewed a specific document or purged an item from their mailbox? If so, you can use the Microsoft 365 complian center to search the unified audit log to view user and administrator activity in your organization. Why a unified audit log? Because you can search for the following types of user and admin activity in Microsoft 365:..."
>> Deleted file from second-stage recycle bin: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#file-and-page-activities
>> User signed in to mailbox: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#exchange-mailbox-activities
>> Reset a user password: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#user-administration-activities

upvoted 4 times

Carlo5 1 year, 4 months ago

I think D is right.

upvoted 3 times

Tiit 1 year, 4 months ago

Searching the audit log is now available in the Microsoft 365 compliance center
D:

upvoted 6 times

Question #3 *Topic 3*

You have a Microsoft 365 subscription. You have a user named User1.
You need to ensure that User1 can place a hold on all mailbox content.
What permission should you assign to User1?

A. the User management administrator role from the Microsoft 365 admin center

B. the eDiscovery Manager role from the Security & Compliance admin center

C. the Information Protection administrator role from the Azure Active Directory admin center

D. the Compliance Management role from the Exchange admin center

Correct Answer: *B*
To create a query-based In-Place Hold, a user requires both the Mailbox Search and Legal Hold roles to be assigned directly or via membership in a role group that has both roles assigned. To create an In-Place Hold without using a query, which places all mailbox items on hold, you must have the Legal Hold role assigned. The Discovery Management role group is assigned both roles.
Reference:
https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
To create a query-based In-Place Hold, a user requires both the Mailbox Search and Legal Hold roles to be assigned directly or via membership in a role group that has both roles assigned. To create an In-Place Hold without using a query, which places all mailbox ite on hold, you must have the Legal Hold role assigned.
The Discovery Management role group is assigned both roles.
Reference:
https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-andcompliance-permissions
upvoted 15 times

Jokke71 Highly Voted 2 years, 7 months ago
I think this is a better reference for the answer than the current provided link: https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide#rbac-roles-related-to-ediscovery
upvoted 7 times

gxsh Most Recent 1 year ago
Correct!
upvoted 1 times

Ash473 1 year, 1 month ago
In today's exam
upvoted 2 times

Jake1 1 year, 10 months ago
Answer is correct. eDiscovery Manager & Administrator, as well as Compliance Administrator and Organization Management role allow you to create query-based holds.https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o36 worldwide#rbac-roles-related-to-ediscovery
upvoted 4 times

HOTSPOT -

You have a new Microsoft 365 subscription.

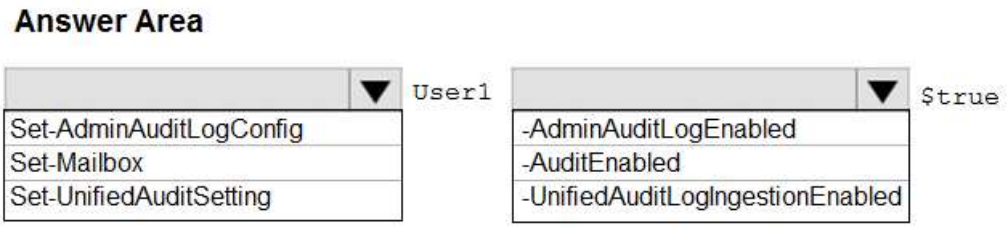
A user named User1 has a mailbox in Microsoft Exchange Online.

You need to log any changes to the mailbox folder permissions of User1.

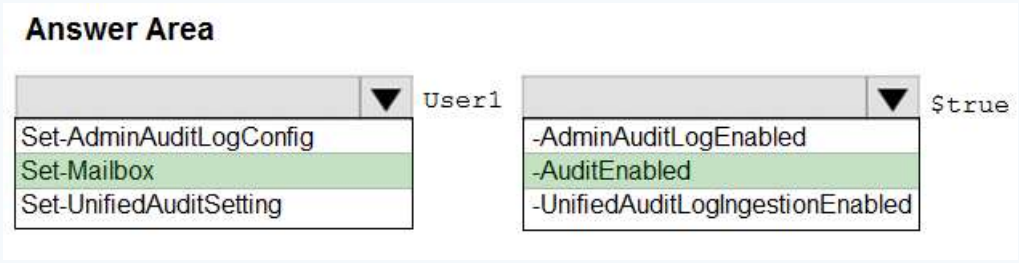
Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



To enable auditing for a single mailbox use this PowerShell command: Set-Mailbox username -AuditEnabled $true

Reference:

https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps-ps

Sr15 Highly Voted 1 year, 3 months ago

To enable auditing for a single mailbox use this PowerShell command: Set-Mailbox username -AuditEnabled $true
Reference:
https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps-ps

upvoted 11 times

Moderator Most Recent 3 months, 3 weeks ago

Correct, pretty straight forward.

upvoted 1 times

You have a Microsoft E5 subscription.
You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange administrator role for five hours at a time.
What should you implement?

A. a conditional access policy

B. a communication compliance policy

C. Azure AD Identity Protection

D. groups that have dynamic membership

E. Azure AD Privileged Identity Management (PIM)

Correct Answer: *E*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

Question #6 *Topic 3*

Your network contains a single Active Directory domain and two Microsoft Azure Active Directory (Azure AD) tenants.
You plan to implement directory synchronization for both Azure AD tenants. Each tenant will contain some of the Active Directory users.
You need to recommend a solution for the planned directory synchronization.
What should you include in the recommendation?

A. Deploy two servers that run Azure AD Connect, and then filter the users for each tenant by using attribute-based filtering.

B. Deploy one server that runs Azure AD Connect, and then specify two sync groups.

C. Deploy one server that runs Azure AD Connect, and then filter the users for each tenant by using attribute-based filtering.

D. Deploy one server that runs Azure AD Connect, and then filter the users for each tenant by using domain-based filtering.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-azure-ad-tenants

ctfalci Highly Voted 2 years, 2 months ago
Answer: A
Explanation
There's a 1:1 relationship between an Azure AD Connect sync server and an Azure AD tenant. For each Azure AD tenant, you need one Azure AD Connect sync server installation.
Therefore, we need to deploy two servers that run Azure AD Connect for the two Azure AD tenants.
Each user account can only be synchronized to one Azure AD tenant. Therefore, we need a way of splitting the users between the two Azure AD tenants. Azure AD Connect offers three ways to filter
which users get synchronized to an Azure AD tenant. You can use domain-based filtering if you have multiple domains in a forest, attribute-based filtering or OU-based filtering.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multipleazure-ad-tenan
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configurefiltering
upvoted 21 times

STFN2019 Highly Voted 2 years, 2 months ago
A is correct. "There's a 1:1 relationship between an Azure AD Connect sync server and an Azure AD tenant. For each Azure AD tenant, y need one Azure AD Connect sync server installation. The Azure AD tenant instances are isolated by design. That is, users in one tenant can't see users in the other tenant."
upvoted 6 times

Tibo49100 Most Recent 5 months, 3 weeks ago
Selected Answer: A
You will need to deploy an AADConnect server for every Azure AD tenant you want to synchronize to - one AADConnect server cannot synchronize to more than one Azure AD tenant : https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-azure-ad-tenants
upvoted 2 times

spg987 1 year, 1 month ago
In exam today
upvoted 2 times

Prates_BR 1 year, 5 months ago
Correct. A for sure!
upvoted 2 times

FableFa 2 years, 3 months ago
One AD Connect per destination tenant (excepted Staging server) - Answer A correct
upvoted 4 times

kazaki 2 years, 3 months ago
Having multiple Azure AD Connect sync servers connected to the same Azure AD tenant is not supported, except for a staging serve
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-azure-ad-tenants
So A is definite wrong answer
upvoted 5 times

DavidSapery 2 years, 3 months ago

But the question says that there are 2 tenants.

upvoted 25 times

lucidgreen 1 year, 6 months ago

It would appear that using 1 AD Connect for multiple tenants is unsupported.
A is the only viable option, but in case there are other answers, remember that they must be configured for filtering so that each
a mutually exclusive set of objects to process.

upvoted 5 times

HOTSPOT -

You have a Microsoft 365 tenant that contains a Microsoft Power Platform development environment named Dev1, a Power Platform production environment named Prod1, and two users named User1 and User2.

You need to assign roles to the users to meet the following requirements:

- User1 must have full access permissions to Dev1 and Prod1.
- User2 must be able to acquire and assign Microsoft Power BI licenses.

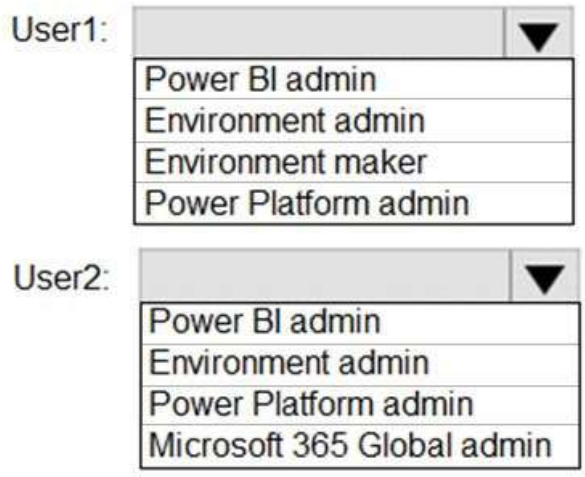
The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

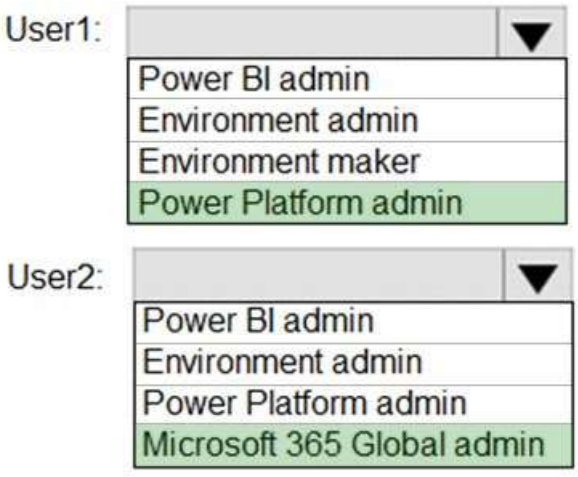
Hot Area:

Answer Area



Correct Answer:

Answer Area



Reference:

https://docs.microsoft.com/en-us/power-bi/admin/service-admin-licensing-organization https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign up for Microsoft Store for Business.

The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator
User5	*None*	*None*

Microsoft Store for Business has the following Shopping behavior settings:

- Allow users to shop is set to On.
- Make everyone a Basic Purchaser is set to Off.

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

A. A. user1, User2, User3, User4, and User5

B. User1 only

C. User1 and User2 only

D. User3 and User4 only

E. User1, User2, User3, and User4 only

Correct Answer: *C*

Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

Reference:

https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

scottims Highly Voted 1 year, 12 months ago

The answer should be A

https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

"The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. Whe admins add apps to the private store, all employees in the organization can view and download the apps."

upvoted 24 times

ctfalci Highly Voted 2 years, 2 months ago

Answer: C
Explanation
Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.
References:
https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

upvoted 16 times

PrinceVarghese 2 years ago

Answer: C
If "Allow users to shop" is off, both Purchasers and Basic Purchasers can't purchase products and services from Microsoft Store. So t answer should be "C". Lets hope this is ON and hence the Purchasers and Basic Purchasers can purchase products and services fron Microsoft Store.

upvoted 6 times

PrinceVarghese 1 year, 11 months ago

In my questionnaire it was "purchase". Looks "install" is a foolishness..

upvoted 3 times

Benatha Most Recent 2 months, 1 week ago

I will go for C.
Underline Install "from Microsoft" for business private store.
English is playing us here...

upvoted 1 times

Jkayx94 9 months ago

I would guess the answer is determined by a couple things. There's no mention of any actual applications being placed in the Private Store? So in order to install apps a Purchaser would be required to Acquire the applications into the Private Store and install.
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

However, without this being the case, it doesn't mention the default behaviour of the Private Store availability? Is this set to Everyone b default? Or None by Default.
https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#private-store-availability

My guess would be C.

upvoted 1 times

tcmaggio 9 months, 2 weeks ago

Selected Answer: A

For me and after reading some comments here, its A for install. Add or Purchase, I would really go with C but if this question shows for tomorrow, I will take my chances with A...

upvoted 4 times

us3r 9 months, 3 weeks ago

2 different versions of this question

1) You need to identify which users can INSTALL apps from the private store.

Answer: All users (A)

2) You need to identify which users can ADD/ PURCHASE apps from the private store.

Answer: Purchaser only (B)

(BASIC purchaser exists only in Microsoft Store for Education)

upvoted 4 times

davem90 10 months, 1 week ago

Selected Answer: A

Answer is definitely A (Private store -> all users)
Please note that Basic purchaser role is only available in Microsoft Store for Education
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

upvoted 3 times

FreddyLao 10 months ago

A is correct:
capture from your reference link:
Curate private store for all employees – A private store can include content you've purchased from Microsoft Store for Business, and your line-of-business apps that you've submitted to Microsoft Store for Business. Apps in your private store are available to all of yo employees. They can browse the private store and install apps when needed.

upvoted 1 times

TimurKazan 11 months, 1 week ago

with these settings only Purchaser role assigned users can buy from Microsoft Store for Business

upvoted 1 times

xofowi5140 11 months, 2 weeks ago

Its is B
Source: https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

upvoted 1 times

allesglar 11 months, 4 weeks ago

I believe that the wording "install" means purchase and therefore the answer is correct. View and download does not mean neither ins nor purchase ;)
Answer is C

upvoted 1 times

PDR 9 months, 2 weeks ago

no - install does not mean purchase.
Install - means install the app on a device , which an end user can do without needing admin permissions, if the app is enabled for them in the store
Purchase - this is how apps are obtained and published into a private store. Even free apps need to be 'purchased' and can the be se available to users, group or everyone.

upvoted 2 times

lengySK 1 year, 1 month ago

if Private store...all users

upvoted 1 times

Tiit 1 year, 4 months ago

Question is, : which users can install apps from the Microsoft for Business "private store".
The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps.

From privatstore can install/Acquire only purchasers (or admins)
C

upvoted 2 times

lucidgreen 1 year, 7 months ago

If an app is available in the corporate or private store, anyone who can see the app can install it, since apps are user-space.
Only those with purchasing roles can purchase when allowing everyone to purchase is off.

upvoted 2 times

lucidgreen 1 year, 7 months ago

The answer should be A.
Look for other questions that might change the wording from "install" to "purchase".

upvoted 5 times

Logitech 1 year, 8 months ago

of course you dont need the purchaser roles to install apps from S4B , awnser is A, just tested it. users 1 und 2 can purchase apps.

upvoted 3 times

mkoprivnj 1 year, 9 months ago

C for sure!

upvoted 1 times

VTHAR 1 year, 11 months ago

This question was asked in MS-101 exam recently. But the exact wording in the question is as such "You need to identify which users ca add apps to the Microsoft for Business private store."

upvoted 8 times

soubhagya96 1 year, 5 months ago

What is the answer?

upvoted 1 times

BradNicho 1 year, 4 months ago

Think this could be a trick question as according to Microsoft basic purchaser is only available in store education:

Note
Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education. For more information, see Microsoft Store for Education permissions.

upvoted 1 times

melatocaroca 1 year, 3 months ago

https://docs.microsoft.com/en-us/microsoft-store/settings-reference-microsoft-store-for-business

upvoted 1 times

Adam0273 2 years ago

is the question who can INSTALL or PURCHASE apps?

upvoted 4 times

gigiscula 2 years ago

i think that the question is incorrect. Unless install equals Purchase for microsoft store for business....

upvoted 1 times

Requi3m 1 year, 2 months ago

I'm not sure if this is a typo in the question. It makes no sense to purchase an app from a private store. So either the part about t private store is also wrong, or the answer is.

upvoted 1 times

You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
In the tenant, you create a user named User1.
You need to ensure that User1 can publish retention labels from the Security & Compliance admin center. The solution must use the principle of least privilege.
To which role group should you add User1?

A. Security Administrator

B. Records Management

C. Compliance Administrator

D. eDiscovery Manager

Correct Answer: *C*
Members of your compliance team who will create retention labels need permissions to the Security & Compliance Center. By default, your tenant admin has access to this location and can give compliance officers and other people access to the Security & Compliance Center, without giving them all of the permissions of a tenant admin. To do this, we recommend that you go to the Permissions page of the Security & Compliance Center, edit the Compliance Administrator role group, and add members to that role group.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/labels#permissions

examxe Highly Voted 2 years, 10 months ago
The answer is correct and the ref should be
https://docs.microsoft.com/en-gb/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles
Records Management Role Group has the role Retention Management and is less priviliged than compliance admin so the correct answ
upvoted 35 times

ctfalci Highly Voted 2 years, 2 months ago
Answer: C
Explanation
Members of your compliance team who will create retention labels need permissions to the Security & Compliance Center. By default, your tenant admin has access to this location and can give
compliance officers and other people access to the Security & Compliance Center, without giving them all of the permissions of a tenan admin. To do this, we recommend that you go to the Permissions page of the Security & Compliance Center, edit the Compliance Administrator role group, and add members to that role group.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/labels#permissions
upvoted 18 times

donathon 2 years ago
I went into the SCC and confirmed that Records Management only have the RecordManagement role and does not have the permissions to modify labels.
upvoted 1 times

Requi3m 1 year, 2 months ago
The question only asks what role is neede to PUBLISH retention labels, not create or modify them. Members of Records Management can configure retention labels, so surely publishing them should be possible.
upvoted 1 times

mmraouf Most Recent 1 week, 1 day ago
The Answer is correct: C

https://learn.microsoft.com/en-us/microsoft-365/compliance/get-started-with-data-lifecycle-management?view=o365-worldwide#permissions-for-retention-policies-and-retention-labels
upvoted 1 times

Debadatta 2 weeks, 6 days ago
Selected Answer: B
Records Management Members can configure all aspects of records management, including retention labels and disposition reviews.
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?

view=o365-worldwide
upvoted 1 times

ovd 3 weeks, 2 days ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-data-lifecycle-management?view=o365-worldwide
- Compliance Administrator admin role group (Ok)
- new role group and add the Retention Management role to this group (not Ok)
upvoted 1 times

Cebsiej_28 1 month, 1 week ago
least privilege is Records Management, so the answer is B.
upvoted 1 times

Sweethaven 2 months, 2 weeks ago
Do your research, Answer is C!
There is no specific 'records manager' role in Microsoft 365. The closest in terms of functionality is the Compliance admin role that includes several several sub-roles including 'RecordManagement', 'Disposition Management' and 'Retention Management'.

Answer C, you cannot assign a records management role to a user so there :)
upvoted 1 times

RenegadeOrange 2 months ago
Uhm, did you read the article below? The answer is B = Records Management.
Records Management: Members can configure all aspects of records management, including retention labels and disposition reviews

I just went into the Microsoft Purview portal and added a user as a member of the Records Management role.

So There :)
upvoted 1 times

RazielLycas 7 months, 2 weeks ago
Selected Answer: B
Records Management is the ones with less privilege "Members can configure all aspects of records management, including retention labels and disposition reviews." ref: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide
upvoted 4 times

mfaisal786 8 months ago
Records Management role is good enough to publish retention labels
upvoted 1 times

VictorPCS 8 months, 1 week ago
Selected Answer: B
Least privilege so should be B
upvoted 2 times

davem90 10 months, 1 week ago
I tested this and a user assigned to Records Management role has the necessary permissions to create and publish retention labels. So answer is B, following the least privilege principle.
upvoted 3 times

tejb 1 year ago
o grant permissions for this limited administration, we recommend that you add users to the Compliance Administrator admin role gro

Alternatively to using this default role, you can create a new role group and add the Retention Management role to this group. For a re only role, use View-Only Retention Management.

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-retention?view=o365-worldwide#permissions-required-to-create-and-manage-retention-policies-and-retention-labels
upvoted 1 times

Rlcky 1 year ago
The solution must use the principle of least privilege, B is the answer.
upvoted 3 times

Vizsgazo1 1 year ago
records management: Additionally, retention labels support records management for email and documents across Microsoft 365 apps and services. You can use a retention label to mark items as a record.
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#permissions
upvoted 1 times

TheRealLionKing 1 year, 1 month ago

It's B ,
Records Management : Members can configure all aspects of records management, including retention labels and disposition reviews.

source: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-cente
view=o365-worldwide

upvoted 5 times

Kepurikee 1 year, 2 months ago

Gotta be Records Management - Members can configure all aspects of records management, including retention labels and dispositior
reviews.

upvoted 2 times

venwaik 1 year, 2 months ago

This should be Records Management as this role is the least priviliged role.
Compare the roles in this link. Both have Retention management rights, but Records management has fewer priviliges.

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 subscription.

You are configuring permissions for Security & Compliance.

You need to ensure that the users can perform the tasks shown in the following table.

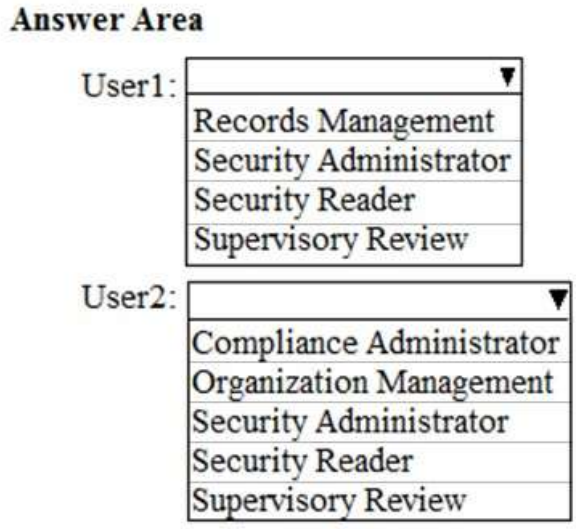
Name	Task
User1	Download all Security & Compliance reports.
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.

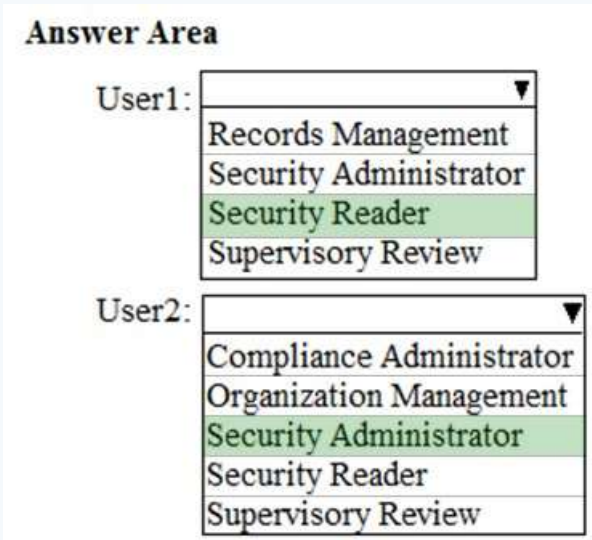
To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Security Reader: Members can manage security alerts (view only), and also view reports and settings of security features.

Security Administrator, Compliance Administrator and Organization Management can manage alerts. However, Security Administrator has the least privilege.

Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles

Rstilekar Highly Voted 1 year, 8 months ago

User1 : This doc appears to say a Security Reader can download the reports. https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o365-worldwide In general, global administrators, security administrators, and secur readers can access and download reports in the Security & Compliance Center. Least privilege is for Security Reader.

User2: Security Administrator, Compliance Administrator and Organization Management can manage alerts. However, Security Administrator has the least privilege.

upvoted 35 times

test123123 Highly Voted 2 years, 8 months ago
Both are Security Administrator.
upvoted 14 times

minajahan 2 years, 7 months ago
I agree. Since both (Security Administrator and Compliance Administrator) can do the things mentioned in the question.

And keeping in mind the principle of least privilege, the list of "Assigned roles" for SA is limited as compared to CA.
upvoted 3 times

melatocaroca 1 year, 3 months ago
With my best respects your position about need to be revieved
upvoted 4 times

machinegf 6 months, 2 weeks ago
right, Global admin can also do that LOL.
upvoted 1 times

davem90 Most Recent 10 months, 1 week ago
Answer is correct! Security Reader & Security Administrator
upvoted 3 times

Rlcky 1 year ago
Security Reader and Security Administrator. For Users 1 its Security Reader.
To use the reports, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:

Organization Management
Security Administrator
Security Reader
Global Reader
upvoted 2 times

lengySK 1 year, 1 month ago
Both are Security Administrator.
upvoted 1 times

TimurKazan 1 year, 1 month ago
Following the principle of least privilege I would go with records management and security administrator.
upvoted 1 times

TimurKazan 11 months ago
perhaps, security READER has less rights than records MANAGEMENT...
upvoted 4 times

Davidchercm 1 year, 1 month ago
security reader can download report :https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o3
worldwide#:~:text=In%20general%2C%20global%20administrators%2C%20security,to%20Reports%20%3E%20Reports%20for%20down
d.
upvoted 2 times

Kepurikee 1 year, 2 months ago
1. Security reader - In general, global administrators, security administrators, and security readers can access reports in the Security & Compliance Center

2. Security Administrator
upvoted 3 times

melatocaroca 1 year, 3 months ago
Global Reader Members have read-only access to reports, alerts, and can see all the configuration and settings. The primary difference between Global Reader and Security Reader is that a Global Reader can access configuration and settings. Security Reader Sensitivity Label Reader
Security Administrator Organization Management Members can control permissions for accessing features in the Security & Compliance Center, and manage settings for device management, data loss prevention, reports, and preservation. Users who are not global administrators must be Exchange administrators to see and act on devices that are managed by Basic Mobility and Security for Microsoft 365 (formerly known as Mobile Device Management or MDM). Global admins are automatically added as members of this role group.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles
upvoted 1 times

Mario007 1 year, 4 months ago

Security Reader can download the reports.
"Make sure that you have the necessary permissions assigned in the Security & Compliance Center. In general, global administrators, security administrators, and security readers can access reports in the Security & Compliance Center."
https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o365-worldwide

upvoted 4 times

RNG60FR 1 year, 8 months ago

i think it's an MS-101 exam question

upvoted 4 times

Takloy 1 year, 8 months ago

true, can't recallthis in the exam which i failed.lol

upvoted 2 times

mkoprivnj 1 year, 9 months ago

3 & 3 for sure. Security Reader & Security Administrator!

upvoted 4 times

Prianishnikov 1 year, 10 months ago

what is the correct answer?

upvoted 3 times

scottims 1 year, 12 months ago

Pulled from descriptions in the Security -> Permissions of lab tenant

Records management
Description
Members of this management role group have permissions to manage and dispose record content.

Compliance Administrator
Description
Manage settings for device management, data loss prevention, reports, and preservation.
Edit
Assigned roles
View-Only Retention Management
Manage Alerts

upvoted 2 times

Annna 2 years ago

for user1, can it be record management ? (for Record Management :Members can manage and dispose record content.)

upvoted 1 times

ctfalci 2 years, 2 months ago

Security Reader: Members can manage security alerts (view only), and also view reports and settings of security features.
Security Administrator, Compliance Administrator and Organization Management can manage alerts.
However, Security Administrator has the least privilege.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance

upvoted 8 times

Myko 2 years, 2 months ago

This doc appears to say a Security Reader can download the reports.
https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o365-worldwide

upvoted 6 times

kev001 1 year, 10 months ago

I just assigned the security reader role to a test user and successfully 'exported' a report.

upvoted 2 times

kev001 1 year, 10 months ago

Download existing reports
Important

Make sure that you have the necessary permissions assigned in the Security & Compliance Center. In general, global administrat
security administrators, and security readers can access reports in the Security & Compliance Center.

In the Security & Compliance Center, go to Reports > Reports for download.

Select one or more items in the list.

Click Download report, and then click Close.

https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o365-worldwide#:~:text=Make%20sure%20that%20you%20have,to%20Reports%20%3E%20Reports%20for%20download.

upvoted 2 times

Question #11 *Topic 3*

Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.
What should you do from the Security & Compliance admin center?

A. Create a data loss prevention (DLP) policy that has a Content contains condition.

B. Create a data loss prevention (DLP) policy that has a Content is shared condition.

C. Modify the default safe links policy.

D. Create a new safe links policy.

Correct Answer: *D*
ATP Safe Links, a feature of Office 365 Advanced Threat Protection (ATP), can help protect your organization from malicious links used in phishing and other attacks. If you have the necessary permissions for the Office 365 Security & Compliance Center, you can set up ATP Safe Links policies to help ensure that when people click web addresses (URLs), your organization is protected. Your ATP Safe Links policies can be configured to scan URLs in email and URLs in Office documents.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients

ctfalci Highly Voted 2 years, 2 months ago
Answer: D
Explanation
ATP Safe Links, a feature of Office 365 Advanced Threat Protection (ATP), can help protect your organization from malicious links used i
phishing and other attacks. If you have the necessary permissions for the Office 365 Security & Compliance Center, you can set up ATP
Safe Links policies to help ensure that when people click web addresses (URLs), your organization is protected. Your ATP Safe Links poli
can be configured to scan URLs in email and URLs in Office documents.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-linkspolicies#
policies-that-apply
upvoted 17 times

melatocaroca 1 year, 3 months ago
research department users so do not modify default, create a new one
upvoted 2 times

trexar Most Recent 7 months ago
Selected Answer: D
The complete path is https://security.microsoft.com/ -->
policies -->Policies & rules
Threat policies
Safe links
upvoted 2 times

Mike3033 1 year, 2 months ago
From https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-links-policies?view=o365-worldwide#policies-that-apply-to-specific-email-recipients
There's no built-in or default Safe Links policy. To get Safe Links scanning of URLs, you need to create one or more Safe Links policies.
upvoted 1 times

mkoprivnj 1 year, 9 months ago
D for sure!
upvoted 4 times

Jake1 1 year, 10 months ago
Answer D is correct. My concern was can this policy be applied to certain user groups and or is it global only but yes you can apply it to
certain groups only.https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o3
worldwide
upvoted 2 times

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the roles shown in the following table.

Name	Permission	Assigner user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	○	○
User2 can sign in to Windows Defender Security Center.	○	○
User3 can view Device1 in Windows Defender Security Center.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	○	○
User2 can sign in to Windows Defender Security Center.	○	○
User3 can view Device1 in Windows Defender Security Center.	○	○

Box 1:

Yes. User1 is in Group1 which is assigned to Role1. Device1 is in the device group named ATP1 which Group1 has access to. Role1 gives Group1 (and User1)

View Data Permission. This is enough to view Device1 in Windows Security Center.

Box 2:

Yes. User2 is in Group2 which is assigned to Role2. Role2 gives Group2 (and User2) View Data Permission. This is enough to sign in to Windows Security

Center.

Box 3:

Yes. User3 is in Group3 which is assigned the Windows ATP Administrator role. Someone with a Microsoft Defender ATP Global administrator

role has unrestricted access to all machines, regardless of their machine group association and the Azure AD user groups assignments.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/user-roles https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/rbac

Couch Highly Voted 2 years, 9 months ago
What is the point of the "View Data" permission by itself? If you can't login to the portal with just that permission (as the answer indicat
then what data can you actually view with that permission?
upvoted 17 times

jabbrwcky 2 years, 9 months ago
My thoughts exactly.
upvoted 2 times

itmp 2 years, 4 months ago
Tested and I can confirm: Creating a "ViewData only" role allows user access to ATP portal. (after about 3min)

So Y/Y/Y
upvoted 16 times

ctfalci Highly Voted 2 years, 2 months ago
Y - Y - Y
Box 1:
Yes. User1 is in Group1 which is assigned to Role1. Device1 is in the device group named ATP1 which Group1 has access to. Role1 gives
Group1 (and User1) View Data Permission. This is enough to view Device1 in Windows Security Center.
Box 2:
Yes. User2 is in Group2 which is assigned to Role2. Role2 gives Group2 (and User2) View Data Permission.
This is enough to sign in to Windows Security Center.
Box 3:
Yes. User3 is in Group3 which is assigned the Windows ATP Administrator role. Someone with a Microsoft Defender ATP Global
administrator role has unrestricted access to all machines, regardless of their machine group association and the Azure AD user group
assignments.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/userroles
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/rbac
upvoted 14 times

donathon 2 years ago
Agree too
upvoted 3 times

donb21 Most Recent 1 month, 3 weeks ago
Answer is Y Y Y
upvoted 1 times

melatocaroca 1 year, 3 months ago
Y,Y,Y,

Read-only access
Users with read-only access can log in, view all alerts, and related information
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/basic-permissions?view=o365-worldwide
upvoted 1 times

lucidgreen 1 year, 7 months ago
Question 1: Yes. View Data Access and Alert investigation access. Assigned this device by Group 1.
Question 2: Yes. View Data Access gives user the ability to log in to Windows Defender Security Center.
Question 3: Yes. User 3 is an Administrator.
upvoted 1 times

RNG60FR 1 year, 8 months ago
MS-101 Exam Question ?
upvoted 6 times

imEmi 1 year, 7 months ago
It is.
upvoted 2 times

Rstilekar 1 year, 8 months ago

Tested and I can confirm: Creating a "ViewData only" and "Alerts investigting role" roles allows user access to ATP portal for user2. Question asks if USer2 can sign in to protection.office.com viz. Security portal. So answer is Yes.

Overall So Y/Y/Y

upvoted 2 times

mkoprivnj 1 year, 9 months ago

Y, Y, Y for sure! ctfalci

upvoted 4 times

Carlos1787 1 year, 11 months ago

YNY is correct. the key is the device must be a part of a device group. See the Important at the end of the section https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/user-roles#create-roles-and-assign-the-role-to-an-azure-active-directory-group

upvoted 3 times

lucidgreen 1 year, 7 months ago

The second question doesn't ask if the user can view a device. It only asks if the user can log in. And the user can.

upvoted 1 times

STFN2019 2 years, 2 months ago

y n y no yes?

upvoted 1 times

Raj2020 2 years, 3 months ago

Tested in my Lab: View Data permission role is not allowed to login to Security center (MS Defender ATP)

upvoted 1 times

TonySuccess 2 years, 3 months ago

Thanks for confirming, i went YNY

upvoted 3 times

fgdsgfdsa 2 years, 1 month ago

Confirmed. Portal access is controlled separately https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/rbac https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/basic-permissio

upvoted 1 times

asdkjhbfc 2 years, 4 months ago

"view data" permission grants access to the portal
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/user-roles

upvoted 2 times

FcoGlezRoy 2 years, 4 months ago

Correct me if wrong, I think the answer is correct you can use event viewer or so to subscribe to remote events without login into the Windows Security Center:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/report-monitor-windows-defender-antivirus

upvoted 1 times

rogerthis1 2 years, 6 months ago

How is the a MS-100 question, surely it must be MS-101?

upvoted 12 times

AlexanderSaad 2 years, 6 months ago

Yes
Yes
Yes

upvoted 3 times

Goofer 2 years, 7 months ago

Y - Y - Y

upvoted 7 times

Zaada 2 years, 7 months ago

I feel like this is a wrong answer. How can you view the data if you don't have a permission to login at first place?

upvoted 3 times

zordss 2 years, 5 months ago

exactly!

upvoted 2 times

ExamStudy101 1 year, 2 months ago

Maybe someone else can clarify but where exactly does it say you would not have sign in access for User2?

upvoted 1 times

Question #13 *Topic 3*

A user receives the following message when attempting to sign in to https://myapps.microsoft.com:
"Your sign-in was blocked. We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin."
Which configuration prevents the users from signing in?

A. Security & Compliance supervision policies

B. Security & Compliance data loss prevention (DLP) policies

C. Microsoft Azure Active Directory (Azure AD) conditional access policies

D. Microsoft Azure Active Directory (Azure AD) Identity Protection policies

Correct Answer: *C*
The user is being blocked due to a 'risky sign-in'. This can be caused by the user logging in from a device that hasn't been used to sign in before or from an unknown location.
Integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to perform password changes or multi-factor authentication to reduce their risk level or be blocked from access until an administrator takes manual action.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

DJHASH786 Highly Voted 2 years, 9 months ago
I believe conditional access is the correct answer

Requiring multi-factor authentication for users with administrative roles
Requiring multi-factor authentication for Azure management tasks
Blocking sign-ins for users attempting to use legacy authentication protocols
Requiring trusted locations for Azure Multi-Factor Authentication registration
Blocking or granting access from specific locations
Blocking risky sign-in behaviors
Requiring organization-managed devices for specific applications
upvoted 28 times

STFN2019 2 years, 2 months ago
Yes I'd stick with conditional access as well
upvoted 2 times

Man1ak 1 year, 5 months ago
However in this case this error is clearly an MCAS error. Therefore it's D.
upvoted 1 times

melatocaroca 1 year, 3 months ago
C is the right answer

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access
upvoted 3 times

d3an Highly Voted 2 years, 8 months ago
The answer is D, Azure Identity Protection, which allows for the configuration of a Sign-in Risk Policy. If Conditional Access was blocking the sign-in, you would not receive that error message.
upvoted 25 times

Logico 1 year, 11 months ago
Agreed. If you Google the error message, you'll see that it's in relation to Azure Identity Protection, rather than Conditional Access.
upvoted 9 times

Cebsiej_28 Most Recent 1 month, 2 weeks ago
Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determin access.

upvoted 1 times

RenegadeOrange 2 months ago

Can be either Identity Protection set to Block Access or using the Risk Policies in Conditional Access. Hopefully in the exam the question will have more information about which feature was configured or let you choose multiple options.

upvoted 2 times

Contactfornitish 2 months, 2 weeks ago

Selected Answer: C

It would be conditional access only. Identity protection does provide the signal but doesn't block itself. In absence of no conditional acc policy, it can be used for reporting purposes only as well. Ca only blocks

upvoted 2 times

aaron_roman 2 months, 4 weeks ago

Selected Answer: D

Identity protection policies is based in Conditional Access for configuration - however they form a different service. I hope MS is consist to its engineering
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

upvoted 1 times

DenisRossi 3 months, 2 weeks ago

Selected Answer: D

D isthe answer.
Conditional Access policy notifies the user with "Your sign-in was successful but does not meet the criteria to access this resource..."

upvoted 2 times

TechMinerUK 3 months, 3 weeks ago

Selected Answer: D

I believe this is AzureAD Identity Protection related since it is not referencing any conditional access policy which would be preventing access e.g. preventing access from certain IP addresses or countries

upvoted 1 times

Stiobhan 4 months ago

It's defo C, take time to actually read the link - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
I have these policies in my tenant, with location conditions in place.

upvoted 1 times

m43s 4 months ago

Selected Answer: C

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

upvoted 1 times

charat 4 months, 1 week ago

Selected Answer: C

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies
The above article was updated in 08/2021
"Administrators can also choose to create a custom Conditional Access policy including sign-in risk as an assignment condition. More information about risk as a condition in a Conditional Access policy can be found in the article, Conditional Access: Conditions"

Therefore, the answer is C. This feature is an Azure Identity Protection feature but it is enabled through conditional access.

upvoted 2 times

charat 4 months, 1 week ago

Conditions on conditional access
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#sign-in-risk

upvoted 2 times

Sh1rub10 4 months, 2 weeks ago

Selected Answer: D

As per d3an comment

upvoted 1 times

Jubei612 7 months, 1 week ago

So the answer given is incorrect? Why after over 2 years this is not "fixed?

upvoted 1 times

Mea988 7 months, 3 weeks ago

Selected Answer: D

This specific message appears only for Identity Protection. Conditional Access has a slightly different one

upvoted 2 times

NiTian 8 months ago

It's conditional access guys. Identity Protection is just tech jargon for the same thing. But the official documentation calls the setting Conditional access

upvoted 1 times

Blankenp 8 months, 1 week ago

Selected Answer: C

C is the right answer. Conditional access policies can block access from untrusted locations or stop risky sign-in behaviors such as signi in from a new device.

upvoted 1 times

AlexLiourtas 8 months, 2 weeks ago

Selected Answer: D

tested, D

upvoted 2 times

HOTSPOT -

You have several devices enrolled in Microsoft Intune.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	*None*

The device type restrictions in Intune are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You add User3 as a device enrollment manager in Intune.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Intune.	○	○
User2 can enroll Android devices in Intune.	○	○
User3 can enroll iOS devices in Intune.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Intune.	○	○
User2 can enroll Android devices in Intune.	○	○
User3 can enroll iOS devices in Intune.	○	○

Box 1:

No. User1 is in Group1. The two device type policies that apply to Group1 are Policy3 and the Default (All Users) policy. However, Policy3 has a higher priority than the default policy so Policy3 is the only effective policy. Policy3 allows the enrolment of Android and iOS devices only, not Windows.

Box 2:

No. User2 is in Group1 and Group2. The device type policies that apply to Group1 and Group2 are Policy2, Policy3 and the Default (All Users) policy. However,

Policy2 has a higher priority than Policy 3 and the default policy so Policy2 is the only effective policy. Policy2 allows the enrolment of Windows devices only, not

Android.

Box 3:

Yes. User3 is a device enrollment manager. Device restrictions to not apply to a device enrollment manager.

Reference:

https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set

Jokke71 Highly Voted 2 years, 7 months ago

According to me the correct answer is No, No, Yes. User 1 cannot enroll the Windows device because Policy 3 is applied to him via Grou
. User 2 cannot enroll the Android device because policy 2 is applied to him via Group 2. Policy 3 is also assigned to him via Group 1 but
has a lower priority than Policy 2 and is therefore overruled. User 3 can enroll any type of device because he is assigned as Device
Enrollment Manager and Device restriction do not apply to them as stated here: https://docs.microsoft.com/en-
us/intune/enrollment/enrollment-restrictions-set#create-a-device-limit-restriction

upvoted 38 times

ctfalci Highly Voted 2 years, 2 months ago

Box 1:
No. User1 is in Group1. The two device type policies that apply to Group1 are Policy3 and the Default (All Users) policy. However, Policy
has a higher priority than the default policy so Policy3 is the only effective policy. Policy3 allows the enrolment of Android and iOS devic
only, not Windows.
Box 2:
No. User2 is in Group1 and Group2. The device type policies that apply to Group1 and Group2 are Policy2, Policy3 and the Default (All
Users) policy. However, Policy2 has a higher priority than Policy 3 and the default policy so Policy2 is the only effective policy. Policy2 all
the enrollment of Windows devices only, not Android.
Box 3:
Yes. User3 is a device enrollment manager. Device restrictions to not apply to a device enrollment manager.
Reference:
https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set

upvoted 21 times

donb21 Most Recent 1 month, 3 weeks ago

I go with N N Y as user3 assign with device enroll manager

upvoted 1 times

RenegadeOrange 2 months ago

No, No, No.
The Device Enrollment Manager can't enroll iOS.
It also can only enroll a personal Android with work profile, not corporate owned or fully managed.
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll

upvoted 1 times

DenisRossi 3 months, 2 weeks ago

no, no, NO.
"DEM isn't compatible with Apple Automated Device Enrollment (ADE)."
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#apple-automated-device-enrollment

upvoted 2 times

DenisRossi 3 months, 2 weeks ago

no, no, NO.
"DEM isn't compatible with Apple Automated Device Enrollment (ADE)."
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#apple-automated-device-enrollment

upvoted 2 times

Durden871 7 months, 1 week ago

Is this really MS-100?

upvoted 3 times

TimurKazan 1 year, 1 month ago

Should No, NO. No. Device restrictions do not applu to device enrollment manager only in Windows 10, hence he can not enroll IOS

upvoted 6 times

Iamrandom 9 months ago

From the reference link posted by ctfalci:

Device limit restrictions don't apply for the following Windows enrollment types:

Co-managed enrollments
GPO enrollments
Azure Active Directory joined enrollments
Bulk Azure Active Directory joined enrollments
Autopilot enrollments
Device Enrollment Manager enrollments

Device limit restrictions are not enforced for these enrollment types because they're considered shared device scenarios. You can se
hard limits for these enrollment types in Azure Active Directory.

** It says "WIndows" enrollment", so for iOS, restriction should be applied

upvoted 3 times

LillyLiver 8 months, 1 week ago

According to this article there aren't any restrictions to a DEM account:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll

upvoted 1 times

stromnessian 1 year, 3 months ago

No No No
Part 3: This seems to be misunderstood by many people: DEM accounts are subject to device type restrictions just like other users. If yo
don't believe me , test it for yourself.

upvoted 3 times

bsldwp_2020 1 year, 4 months ago

Priority is used when a user exists in multiple groups that are assigned restrictions. Users are subject only to the highest priority restriction assigned to a group that they are in. For example, Joe is in group A assigned to priority 5 restrictions and also in group B assigned to priority 2 restrictions. Joe is subject only to the priority 2 restrictions.

Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priori

upvoted 1 times

lucidgreen 1 year, 7 months ago

If the solution is restricted by Priority, the answer is:
User 1, Group 1: Policy 3 only.
User 2, Group 1,2: Policy 2 only.
User 3, No group, DEM: All devices.

Question 1: No.
Question 2: No.
Question 3: Yes.

upvoted 5 times

lucidgreen 1 year, 7 months ago

Otherwise, it is Yes, Yes, Yes.

upvoted 2 times

Andy555 1 year, 8 months ago

- Conditions: Include All device state, exclude Device marked as compliant
⇨ Access controls is set to Block access.
Means that all compliant devices will be excluded from the policy.
The policy is set to "Block".
Thus... N/Y/Y

upvoted 1 times

mkoprivnj 1 year, 9 months ago

N, N, Y for sure. cfalci

upvoted 5 times

madsa 1 year, 10 months ago

This is the right link "https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll#:~:text=If%20you're%20enrolling%20Android,DEM%20accounts%20isn't%20supported." In this case the restrictions do not apply a DEM account, but number of devices that can be enrolled does apply to a DEM account.

upvoted 1 times

shark1 2 years, 3 months ago

No
No - higher priority wins
Yes - DEM roles guys!

upvoted 6 times

zmart 2 years, 4 months ago

User2 -> No
Reference search for the name "multiple groups"
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

upvoted 2 times

itmp 2 years, 4 months ago

NO/NO/YES

User 1 - meets policy3 with higher priority than "default" so no windows for him.
User 2 - meets policy2 at priority 2 so he can't get to policy 3 for android.
User 3 - is DEM so he can enroll.

upvoted 12 times

HOTSPOT -

You have the Microsoft Azure Active Directory (Azure AD) users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

The device compliance policies in Intune are configured as shown in the following table.

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

You create a conditional access policy that has the following settings:

⇨ The Assignments settings are configured as follows:

- Users and groups: Group1
- Cloud apps: Exchange Online
- Conditions: Include All device state, exclude Device marked as compliant

⇨ Access controls is set to Block access.

For each of the following statements, select yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

Box 1:

Yes. User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is marked as compliant.

BitLocker is disabled for Device1. Device1 is in Group3 which is assigned device Policy1. The BitLocker policy in Policy1 is 'not configured' so BitLocker is not required.

Therefore, Device1 is compliant so User1 can access Exchange online from Device1.

Box 2:

No. User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is

marked as compliant.
BitLocker is disabled for Device2. Device2 is in Group4 which is assigned device Policy2. The BitLocker policy in Policy2 is 'Required so BitLocker is required.
Therefore, Device2 is not compliant so User1 cannot access Exchange online from Device2.
Box3:
Yes. User2 is in Group2. The Conditional Access Policy applies to Group1. The Conditional Access Policy does not apply to Group2. So even though Device2 is non-compliant, User2 can access Exchange Online using Device2 because there is no Conditional Access Policy preventing him/her from doing so.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions

Hamster5000 Highly Voted 2 years, 8 months ago
Correct should be Yes, No, Yes:
1) User 1 on Device 1 - part of affected Group1, but the device IS compliant so its excluded from being blocked
2) User 1 on Device 2 - part of affected Group1 AND device NOT compliant, so its blocked
3) User 2 can use any device and access Exchange Online as he is NOT a member of affected Group1
upvoted 50 times

test123123 2 years, 8 months ago
Yes, No, No
Device 2 is not compliant, as btilocker is not running.
upvoted 1 times

WoneSix 2 years, 7 months ago
test123123 (and earlier, zzuk and vikaswins), the question doesn't say anything about blocking all non-compliant devices. User2 i affectede by the policy in question, nor is device2 as long as a non-affected user is using it.
upvoted 6 times

Moji1 2 years, 8 months ago
You are right. The scope of the conditional access policy is Group 1, so User 2 is not in the scope
upvoted 3 times

ctfalci Highly Voted 2 years, 2 months ago
Y - N - Y
Box 1:
Yes. User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device marked as compliant. BitLocker is disabled for Device1. Device1 is in Group3 which is assigned device Policy1. The BitLocker policy in Policy1 is 'not configured' so BitLocker is not required. Therefore, Device1 is compliant so User1 can access Exchange online from Devic
Box 2:
No. User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device marked as compliant. BitLocker is disabled for Device2. Device2 is in Group4 which is assigned device Policy2. The itLocker policy in Policy2 is 'Required so BitLocker is required.
Therefore, Device2 is not compliant so User1 cannot access Exchange online from Device2.
Box3:
Yes. User2 is in Group2. The Conditional Access Policy applies to Group1. The Conditional Access Policy does not apply to Group2. So ev though Device2 is non-compliant, User2 can access
Exchange Online using Device2 because there is no Conditional Access Policy preventing him/her from doing so.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions
upvoted 20 times

sehlohomoletsane Most Recent 8 months, 3 weeks ago
can someone please explain what the answer is?
upvoted 1 times

lucidgreen 1 year, 7 months ago
Device 1: Compliant
Device 2: Not Compliant

The policy is applied to Users, not Devices.

Group 1 can only access Exchange Online if the device compliant.
Group 2 is not affected, no policy assigned.

Question 1: Yes.
Question 2: No.
Question 3: Yes.

upvoted 7 times

Andy555 1 year, 8 months ago

- Conditions: Include All device state, exclude Device marked as compliant
➪ Access controls is set to Block access.
Means that all NOT compliant devices will be excluded from the policy.
The policy is set to "Block".
Thus... N/Y/Y

upvoted 2 times

[Removed] 1 year, 8 months ago

YNY - User 2 is not part of CA.

upvoted 2 times

mkoprivnj 1 year, 9 months ago

Y - N - Y

upvoted 3 times

Pabanda 2 years, 3 months ago

Third answer is wrong:
User2 is in Group2. The Conditional Access Policy applies to Group1. The Conditional Access Policy does not apply to Group2. So even though Device2 is non-compliant, User2 can access Exchange Online using Device2 because there is no Conditional Access Policy preventing him/her from doing so.

upvoted 3 times

HvD 2 years, 2 months ago

I think you're right.

upvoted 1 times

Jhill777 2 years, 4 months ago

Because every Azure admin is going to create these types of scenarios to confuse themselves.

upvoted 10 times

ChrisKon 2 years, 4 months ago

What is the correct answer?

upvoted 1 times

STFN2019 2 years, 2 months ago

Yes no yes

upvoted 4 times

itmp 2 years, 5 months ago

This is a about a Conditional access policy that applies to Group1 ONLY!

User1 can access Exchange from device1 (device1 IS compliant)
User1 can't access Exchange from device2 (device2 is NOT compliant)
User2 CAN access Exchange from ANY device (the 'BLOCK policy' ONY applies to User1)

There is NO "block all non-compliant devices" policy in the statements.

upvoted 7 times

Dylan 3 years ago

Hmm - Agree with Mendel here, the device state is part of the decision but if the user hasn't got the policy applied then I would expect not to be considered - maybe I need to recreate in a lab

upvoted 1 times

Mendel 3 years ago

Why can't user 2 access exchange online? User 2 is not affected by any conditional access. If I understand this correctly the block policy only affects group 1.

upvoted 14 times

vikaswins 3 years ago

It is because user 2 is trying to access from device 2 which is affected by policy.

upvoted 1 times

zzuk01 2 years, 9 months ago

Device 2 is a member of Group 4 and therefore not in scope for the Conditional Access Policy (that is assigned to Group 1 only)

upvoted 13 times

lusis987 2 years, 7 months ago

Device 2 (bitlocker turned off)- Policy 2 (requires bitlocker). Thats why

upvoted 1 times

mafevaso 2 years, 3 months ago

But the blocking policy is assigned to group1 and user2 is not member of group1, therefore it does not matter if he is accessing from a non compliance device as the policy does not apply to him.

upvoted 4 times

lucidgreen 1 year, 6 months ago

Device 1: Compliant
Device 2: Not Compliant

The policy is applied to Users, not Devices.

Group 1 can only access Exchange Online if the device compliant.
Group 2 is not affected, no policy assigned.

Question 1: Yes.
Question 2: No.
Question 3: Yes.

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain.
You deploy a Microsoft Azure Active Directory (Azure AD) tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The question states that ɹ€all the user account synchronizations completed successfullyɹ€. Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

Sisko Highly Voted 2 years, 8 months ago
This answer is right. You can make a new rule and include the missing OU. It's not the best way to do it (better to just re-run the AAD Config and select the missing OU), but it is a valid solution. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration
upvoted 17 times

WoneSix 2 years, 7 months ago
Agreed, Sisko - not ideal, but it will work if the new rule is configured correctly.
upvoted 3 times

Marz Highly Voted 2 years, 8 months ago
It is mentioned that 10 users an OU are not synced. So id guess that we need to change the sync sertings to include this OU
upvoted 7 times

Davood Most Recent 1 year, 6 months ago
Answer is no. You need to modify the Filter
upvoted 3 times

txrocker13 1 year, 9 months ago
If there is a new rule to be made, wouldn't it be an "in from AD" rule and not an "out to AAD" rule? If you don't get the users into the metaverse from AD then you can't export them to AAD with an out to AAD rule.
upvoted 2 times

mkoprivnj 1 year, 9 months ago
Answer is NO.
upvoted 3 times

paddyh 1 year, 9 months ago
with only 10 failing then the rule itself is ok otherwise all would fail , is this not more to do with adding filtering rule to determine what wrong with the failed accounts
upvoted 1 times

LuckyCricket 1 year, 10 months ago
Experts agree - The answer is NO
The question states "all the user accounts sync completed successfully" - therefore AAD Connect is working and config'd correctly. Hen the issue is likely that they are being excluded from the sync cycle by a filtering rule. Although I don't see the option listed here, the tes

does include a question that ends with:
Solution: From Azure AD Connect, you modify the filtering settings. This answer should you encounter it would be the correct one and should select Y.

upvoted 6 times

donathon 1 year, 11 months ago

The editor is just used for transformation and mapping of attributes. It does not solve the underlying problem which is the OU are excluded.

upvoted 1 times

TonySuccess 2 years, 3 months ago

Who in their right mind would go and start running scripts, rather than just check that the OU is seleted in AD Sync.

upvoted 4 times

Hakimi 2 years, 5 months ago

I think this answer is wrong, the Snyc was successful so it make no sense to create new one rather than check the filter on the current Sync and include those Users (OU) in Sync.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

upvoted 4 times

ExamStudy68 2 years, 8 months ago

I think this might be wrong - if someone comes up with a link to read on this please post. I think you would check the UPN?

upvoted 1 times

WoneSix 2 years, 7 months ago

If the users' UPNs are wrong and the OU is synched, there will be errors in the synch. There were none. WHat they SHOULD do is re the wizard and add the OU to the list of synched OUs, but the answer does give another (more problemmatic) way of solving the iss

upvoted 3 times

Dylan 2 years, 9 months ago

I guess it would have reported issues if there was an AD related issues, makes sense now! Ignore please...

upvoted 2 times

Dylan 2 years, 9 months ago

Why would this fix the 10 problematic accounts?

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain.
You deploy a Microsoft Azure Active Directory (Azure AD) tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: You run idfix.exe and export the 10 user accounts.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The question states that ɹ€all the user account synchronizations completed successfullyɹ€. If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.
It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

donathon Highly Voted 1 year, 11 months ago
IDFIX.exe just fix the issues with the attributes of the users which would show up in the sync errors. In this case there was no such erro
and further more it does not fix the issue where the OU are not included in the sync.
upvoted 10 times

forummj Most Recent 2 weeks, 1 day ago
I would suggest that this is yes.

https://learn.microsoft.com/en-us/troubleshoot/azure/active-directory/objects-dont-sync-ad-sync-tool

Under the heading "Symptoms"
"You don't receive an error message, and directory synchronization seems to be completed. However, some objects or attributes aren't
updated as expected." - Which sounds like what has been described in the question: i.e. "organizational unit (OU) are NOT synchronized
Azure AD" and "all the user account synchronizations completed successfully."
upvoted 1 times

forummj 2 weeks, 1 day ago
Scratch that. I've reread the question. Ignore the above comment.
upvoted 1 times

Ash473 1 year, 1 month ago
In exam today
upvoted 3 times

MartiFC 1 year, 2 months ago
Not for sure!
upvoted 2 times

mkoprivnj 1 year, 9 months ago
No for sure!
upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain.
You deploy a Microsoft Azure Active Directory (Azure AD) tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: From Azure AD Connect, you modify the Azure AD credentials.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The question states that ɹ€all the user account synchronizations completed successfullyɹ€. Therefore, the Azure AD credentials are configured correctly in Azure AD
Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

titan_91 Highly Voted 1 year, 11 months ago
No, because there are no directory sync errors. Also, if the Azure AD Connect credentials were wrong, all syncs would fail, not just 10 accounts.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-azureadaccount
upvoted 6 times

Ash473 Most Recent 1 year, 1 month ago
In exam today as multiple choice
upvoted 1 times

MartiFC 1 year, 2 months ago
No, because there are not any errors to sync.
upvoted 1 times

mkoprivnj 1 year, 9 months ago
Answer is NO.
upvoted 1 times

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Billing administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self-service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:
- Email address only
- Phone number only
- Security questions only
- Phone number and email address

User2:
- Email address only
- Phone number only
- Security questions only
- Phone number and email address

User3:
- Email address only
- Phone number only
- Security questions only
- Phone number and email address

Correct Answer:

Answer Area



Microsoft enforces a strong default two-gate password reset policy for any Azure administrator role. This policy may be different from the one you have defined for your users and cannot be changed. You should always test password reset functionality as a user without any Azure administrator roles assigned.

With a two-gate policy, administrators don't have the ability to use security questions.

The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number.

User3 is not assigned to an Administrative role so the configured method of Security questions only applies to User3.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-password-policy-differences

Moderator 2 months ago

Still a valid question (July 30th 2022).

upvoted 3 times

BennyS 7 months, 2 weeks ago

By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced. This policy may be different from the one you have defined for your users, and this policy can't be changed. You should alwa test password reset functionality as a user without any Azure administrator roles assigned.

With a two-gate policy, administrators don't have the ability to use security questions.
Source: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

upvoted 3 times

melatocaroca 1 year, 3 months ago

The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number., According with MS phrase , you one will be required, one more, email

upvoted 4 times

chaoscreater 1 year, 3 months ago

Unrelated to answer. SSPR policies for admins are separate to policies for normal users. By default, admins require 2 authentication methods.

upvoted 6 times

RAJULROS 1 year, 4 months ago

HOTSPOT -

You have a Microsoft 365 subscription.

You need to provide an administrator named Admin1 with the ability to place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations.

The solution must use the principle of least privilege.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Admin center to use:

- Azure Active Directory
- Exchange
- Microsoft 365 admin center
- Microsoft 365 compliance center

Role to assign:

- eDiscovery Manager
- Information Protection Administrator
- User management administrator

Correct Answer:

Answer Area

Admin center to use:

- Azure Active Directory
- Exchange
- Microsoft 365 admin center
- **Microsoft 365 compliance center**

Role to assign:

- **eDiscovery Manager**
- Information Protection Administrator
- User management administrator

Core eDiscovery in Microsoft 365 provides a basic eDiscovery tool that organizations can use to search and export content in Microsoft 365 and Office 365. You can also use Core eDiscovery to place an eDiscovery hold on content locations, such as Exchange mailboxes, SharePoint sites, OneDrive accounts, and
Microsoft Teams.
To access Core eDiscovery or be added as a member of a Core eDiscovery case, a user must be assigned the appropriate permissions. Specifically, a user must be added as a member of the eDiscovery Manager role group in the Microsoft 365 compliance center. Members of this role group can create and manage Core eDiscovery cases. They can add and remove members, place an eDiscovery hold on users, create and edit searches, and export content from a Core eDiscovery case.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide

JackeD 1 month ago
correct answer. this is the updated version of the question after security and compliance was split. The old answer was Security and compliance, no m365 compliance center. I would assume any questions referencing security and compliance is outdated.
upvoted 2 times

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Exchange administrator
User2	User administrator
User3	Global administrator
User4	*None*

You add another user named User5 to the User administrator role.
You need to identify which two management tasks User5 can perform.
Which two tasks should you identify? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Delete User2 and User4 only.

B. Reset the password of User2 and User4 only.

C. Delete User1, User2, and User4 only.

D. Delete any user in Azure AD.

E. Reset the password of any user in Azure AD.

F. Reset the password of User4 only.

Correct Answer: *AB*
Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).
Only on users who are non-admins or in any of the following limited admin roles:
⇨ Directory Readers
⇨ Guest Inviter
⇨ Helpdesk Administrator
⇨ Message Center Reader
⇨ Reports Reader
⇨ User Administrator
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain.
You deploy a Microsoft Azure Active Directory (Azure AD) tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: From Azure AD Connect, you modify the filtering settings.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
The question states that ɹ€all the user account synchronizations completed successfullyɹ€. Therefore, we know that Azure AD Connect is working and configured correctly. The only thing that would prevent the 10 user accounts from being synchronized is that they are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

JakeH 10 months, 3 weeks ago
In exam today
upvoted 2 times

junior6995 1 year ago
Filtering is where you select the OU's to be synchronized with AAD.
upvoted 3 times

MartiFC 1 year, 2 months ago
If the sync is succesfully, then will see the filtering settings
upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has 3,000 users. All the users are assigned Microsoft 365 E3 licenses.
Some users are assigned licenses for all Microsoft 365 services. Other users are assigned licenses for only certain Microsoft 365 services.
You need to determine whether a user named User1 is licensed for Exchange Online only.
Solution: You run the Get-MsolUser cmdlet.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The Get-MsolUser cmdlet will tell you if a user is licensed for Microsoft 365 but it does not tell you which licenses are assigned.
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0

saumade Highly Voted 2 years, 10 months ago
I think the correct answer should be A
for example: get-msoluser -UserPrincipalName abcd@example.com | select -ExpandProperty licenses | ft AccountSkuId
Lists all the licenses of a user
upvoted 30 times

itmp 2 years, 4 months ago
@saumade, your command gives you the output below.
Can you tell if the user has EXO ? ...

Provided answer is correct.

mycompany:FLOW_FREE
mycompany:AAD_PREMIUM_P2
mycompany:EMS
mycompany:TEAMS_COMMERCIAL_TRIAL
mycompany:ENTERPRISEPREMIUM_NOPSTNCONF
upvoted 2 times

Logitech 1 year, 8 months ago
yes you can if you have exonline then this will return: EXCHANGE_S_ENTERPRISE or EXCHANGE_S_STANDARD
upvoted 3 times

BGM_YKA 1 year, 4 months ago
example...
(Get-MsolUser -UserPrincipalName Name@Domain.com).licenses.servicestatus | Where {$_.ServicePlan.serviceName -like "EXCHANGE*"}

has output...
ServicePlan ProvisioningStatus
---------- ----------
EXCHANGE_S_ENTERPRISE Success
EXCHANGE_ANALYTICS Success
upvoted 1 times

ranc1d 2 years, 6 months ago
Its not about the license, its about the service "Exchange Online".
Nevertheless A should be correct
To view services for a user account: (Get-MsolUser -UserPrincipalName belindan@litwareinc.com).Licenses.ServiceStatus
upvoted 17 times

andrejkamensky 2 years, 2 months ago
the whole command:
$userUPN="<user account UPN>"

```
$AllLicenses=(Get-MsolUser -UserPrincipalName $userUPN).Licenses
$licArray = @()
for($i = 0; $i -lt $AllLicenses.Count; $i++)
{
$licArray += "License: " + $AllLicenses[$i].AccountSkuId
$licArray += $AllLicenses[$i].ServiceStatus
$licArray += ""
}
$licArray
```

upvoted 3 times

CMal Highly Voted 1 year, 10 months ago

The answer is correct. In the sentence, it states "All the users are assigned Microsoft 365 E3 licenses.". With an E3, Exchange Online is a service/workload, not a license. The only way the Exchange Online license would appear would be if you purchased an Exchange Online Plan 1 or Plan 2 license separate from the E3.

upvoted 25 times

originalwitness 1 year, 10 months ago

This makes much more sense than the other explanations. Tricky wording!

upvoted 4 times

Maroslaw 1 year, 3 months ago

Correct, tested on my E3

upvoted 2 times

Cebsiej_28 Most Recent 1 month, 2 weeks ago

B is correct because Get-MsolUser cmd will only tell you if the user is licensed or not.

upvoted 1 times

Stiobhan 4 months, 1 week ago

Answer is correct. It's suggesting you are only running Get-MsolUser with no additional arguments. This commannd on its own retrieves all users in the company. It displays up to the default value of 500 results. It's about 1/4 way down on this link - https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0

upvoted 3 times

KSvh53 6 months, 2 weeks ago

Selected Answer: A

I have a test environment set up and have verified this. The correct answer is A. You can run this exact command after connecting to msonline and get all the licenses they belong to (you just have to know how to read them):
(Get-MsolUser -UserPrincipalName user@domain.com).licenses
The output gave me the accountSKU ID for all the licenses. You might have to do additional work to know what those licenses are if you not familiar with them but it's not too hard to guess which one is. It lets you see any licenses that are assigned, the same ones you can in Microsoft 365 Admin Center under that user.

upvoted 1 times

mikaiwhodakno 3 months, 2 weeks ago

Except Exchange Online is a service that cannot be listed via "Get-MsolUser", not a license, therefore B is correct.

upvoted 1 times

trexar 7 months ago

Selected Answer: A

Output of the command:
Licenses. A list of the user's licenses.

https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0

upvoted 1 times

mikaiwhodakno 3 months, 2 weeks ago

Except Exchange Online is a service that cannot be listed via "Get-MsolUser", not a license, therefore B is correct.

upvoted 2 times

jkklim 9 months, 1 week ago

tested - answer is A

upvoted 1 times

tf444 9 months, 1 week ago

Get-MsolUser -All | where {$_.isLicensed -eq $true}.

upvoted 1 times

EaaGleee 9 months, 1 week ago

Selected Answer: A

get-msoluser -UserPrincipalName abcd@example.com | select -ExpandProperty licenses | ft AccountSkuId

upvoted 1 times

Madball 1 year, 1 month ago

I think you all may be misunderstanding the question, the question states "you run the get-msoluser cmdlet". If you run this on its own you do not get what license each user has, however you can get the license details using this cmdlet but it require further additional cmdlets. So I would say the answer is NO on this one.

upvoted 3 times

Fcnet 1 year, 2 months ago

Answer is A get-msoluser gives details
PS C:\> (get-msoluser -userprincipalname admin@truc.onmicrosoft.com).licenses.servicestatus

ServicePlan ProvisioningStatus
---------- ----------
RMS_S_BASIC PendingProvisioning
POWER_VIRTUAL_AGENTS_O365_P1 Success
CDS_O365_P1 Success
PROJECT_O365_P1 Success
DYN365_CDS_O365_P1 Success
KAIZALA_O365_P2 Success
MICROSOFT_SEARCH PendingProvisioning
WHITEBOARD_PLAN1 Success
MYANALYTICS_P2 Success

and
Get-AzureADSubscribedSku
gives
SkuPartNumber

STANDARDPACK
no details

upvoted 1 times

melatocaroca 1 year, 3 months ago

https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-account-license-and-service-details-with-microsoft-365-powershell?view=o365-worldwide

upvoted 2 times

kanag1 8 months, 3 weeks ago

This command provides details of all assigned services. Cool !! melatocaroca Thanks for the reference
(Get-MsolUser -UserPrincipalName belindan@litwareinc.com).Licenses.ServiceStatus

upvoted 1 times

melatocaroca 1 year, 3 months ago

$userUPN="<user account UPN, such as belindan@contoso.com>"
$licensePlanList = Get-AzureADSubscribedSku
$userList = Get-AzureADUser -ObjectID $userUPN | Select -ExpandProperty AssignedLicenses | Select SkuID
$userList | ForEach { $sku=$_.SkuId ; $licensePlanList | ForEach { If ($sku -eq $_.ObjectId.substring($_.ObjectId.length - 36, 36)) { Write Host $_.SkuPartNumber } } }

Reference
https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-account-license-and-service-details-with-microsoft-365-powershell?view=o365-worldwide

upvoted 1 times

mackypatio 1 year, 4 months ago

answer is no. and microsoft should make a way to do this. i raised a case about this a couple of times and MS support says everytime there is no way.

upvoted 1 times

mackypatio 1 year, 4 months ago

i meant powershell way, currently there is no way.

upvoted 1 times

mackypatio 1 year, 4 months ago

i stand corrected, (get-msoluser -userprincipalname user1@domain.com).licenses.servicestatus

upvoted 2 times

Razuli 1 year, 5 months ago

Get-MsolUser only tells you if they are licensed or not e.g. True or Fales, doesnt tell you what they are licensed for. I have just tested thi
on my tenant

upvoted 1 times

bog23 1 year, 6 months ago

The answer is Yes, Ori Sictify

upvoted 1 times

Logitech 1 year, 8 months ago

Really stupid questions. get-MsolUser Cmdlet can get you the license and service info. But not if you run only get-msoluser without paramters and selecting the right properties. Hate this shit.... I go with NO, because of MS. In Reality: YES this is the right cmdlet.

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has 3,000 users. All the users are assigned Microsoft 365 E3 licenses.
Some users are assigned licenses for all Microsoft 365 services. Other users are assigned licenses for only certain Microsoft 365 services.
You need to determine whether a user named User1 is licensed for Exchange Online only.
Solution: You run the Get-MsolAccountSku cmdlet.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The Get-MsolAccountSku cmdlet returns all the SKUs that the company owns. It does not tell you which licenses are assigned to users.
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolaccountsku?view=azureadps-1.0

fofo1960 12 months ago
No, Running this cmdlet will return all the available licenses in the tenant
AccountSkuId ActiveUnits WarningUnits ConsumedUnits
---------- ---------- ---------- ----------
Myorg:VISIOCLIENT 10 0 9
Myorg:STREAM 1000000 0 23
Myorg:DYN365_FINANCE 20 0 0
Myorg:DYN365_TEAM_MEMBERS 366 0 1
Myorg:WINDOWS_STORE 25 0 0
Myorg:FLOW_FREE 10000 0 36
upvoted 2 times

mkoprivnj 1 year, 9 months ago
No for sure!
upvoted 1 times

melatocaroca 1 year, 3 months ago
https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-licenses-and-services-with-microsoft-365-powershell?view=o365-worldwide
upvoted 1 times

CMal 1 year, 10 months ago
The answer is correct. In the sentence, it states "All the users are assigned Microsoft 365 E3 licenses.". With an E3, Exchange Online is a service/workload, not a license. The only way the Exchange Online license would appear would be if you purchased an Exchange Online Plan 1 or Plan 2 license separate from the E3.
upvoted 2 times

scottims 1 year, 11 months ago
B
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolaccountsku?view=azureadps-1.0
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has 3,000 users. All the users are assigned Microsoft 365 E3 licenses.
Some users are assigned licenses for all Microsoft 365 services. Other users are assigned licenses for only certain Microsoft 365 services.
You need to determine whether a user named User1 is licensed for Exchange Online only.
Solution: You launch the Azure portal, and then review the Licenses blade.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
In the Licenses blade, click All Products then select the E3 License. This will display a list of all users assigned an E3 license. Select User1. You'll see how many services are assigned in the Enabled Services column. Click on the number in the Enabled Services column for User1 and you'll be taken to the licenses page for that user. Click on the number in the Enabled Services column for User1 again and a page will open which shows you exactly which services are enabled or disabled.
Alternatively, you can go into the user account properties directly then select Licenses. This will display the licenses blade for that user. You can then click on the number in the Enabled Services column for the user and a page will open which shows you exactly which services are enabled or disabled.

Faheem2020 Highly Voted 1 year, 9 months ago
I take back the earlier comment. You can do it from license blade.
upvoted 8 times

Faheem2020 Highly Voted 1 year, 10 months ago
Answer is B
You need to open the Users Blade, select the user and select license to see the enabled services.
The license blade does not give you information about the enabled services for induvial users, only the license and list of services withi the license that can be enabled for the users
upvoted 6 times

J0J0 1 year, 3 months ago
you're wrong. Definitely correct, but not the shortest path to check.
upvoted 5 times

Takloy 1 year, 8 months ago
Faheem is right but I still find it tricky. But if we want to be in details, then yes, Faheem2020 is absolutely correct.
upvoted 1 times

m43s Most Recent 3 months, 1 week ago
Selected Answer: A
correct is A
upvoted 1 times

Cebsiej_28 5 months, 1 week ago
I think this solution is not complete for the goal we want to achieve, because on license blade you will get the available services/license only.
upvoted 1 times

ARYMBS 5 months, 1 week ago
Selected Answer: B
From Licenses blade REVIEW ITLSEF you cannot (you have to click and go deeper) which explicitly question is asking about. Therefore I for B.
Either way this depends on how you understand a question.
upvoted 1 times

trexar 7 months ago

Selected Answer: A

The Get-MsolAccountSku cmdlet returns all the SKUs that the company owns.
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolaccountsku?view=azureadps-1.0

upvoted 1 times

fofo1960 12 months ago

Yes, you can.
Azure AD --> License --> All product --> Click on the Plan E3/E5 --> Click on any user --> Again Click on the Assigned Product, and you wil
see all the assigned Services.
Long way, but doable.

upvoted 2 times

josemariamr 1 year, 4 months ago

A (yes) is valid but not the faster way to do it.
An easier way should be go to User, click user1, view its licenses and then activated services for the E3 license: click on the E3 license ar
you can see a page with "on/off" for each service.
You can also take the long way as the proposed solution: go first to Licenses blade, click "All products", click E3 licenses, you will see the
of users, then click the user, etc.

upvoted 4 times

Razuli 1 year, 5 months ago

Testing this on my tenant now, it does not show me individual services within a license so im confused with this one

upvoted 1 times

Goseu 1 year, 5 months ago

YES is correct answer , confirmed it as we speak .
Go to Azure AD , Licenses , all products , MS 365 E3 , click on user and see enabled services

upvoted 2 times

PD1885 1 year, 8 months ago

If you click through from the licences blade into the E3 license you're then presented with the users that have it assigned, if you then cl
a user you can then drill through and see exactly what plans are specified in the E3 license. YES is the correct answer.

upvoted 2 times

mkoprivnj 1 year, 9 months ago

Yes for sure!

upvoted 1 times

mkoprivnj 1 year, 9 months ago

NO is correct. Reference to Faheem2020's answer!

upvoted 1 times

cdsa 1 year, 8 months ago

Yes, Selecting the license will show the users assigned.

upvoted 2 times

MerryWeasel 1 year, 8 months ago

You are assuming that they have separate individual Exchange Plan 1 or 2 purchased. Question states that all the users are
assigned Microsoft 365 E3 licenses.
Under licenses blade you cannot see individual licenses under Office E3 package, you can only see individual licenses assigned
for E3 package under Users blade->licenses->Office 365 E3 like Faheem2020 said.

upvoted 2 times

JeepScratch 1 year, 8 months ago

He was wrong please, YES is correct. Please do your homework.

upvoted 2 times

jnecode 2 years ago

Licenses blade then click the EO license and all users that have the license will show up. Correct Answer.

upvoted 1 times

AlexanderSaad 2 years, 6 months ago

From azure ad - licenses - you cannot see if the user is licenses for a single service only.

upvoted 1 times

AlexanderSaad 2 years, 5 months ago

You need to open the user account in azure ad, then go to licenses, expand the license to see the assigned services.

upvoted 10 times

kuuser 2 years, 1 month ago

So is the answer correct or not? Is the "licenses blade" the same as the "user account -> licenses -> expand"?
upvoted 1 times

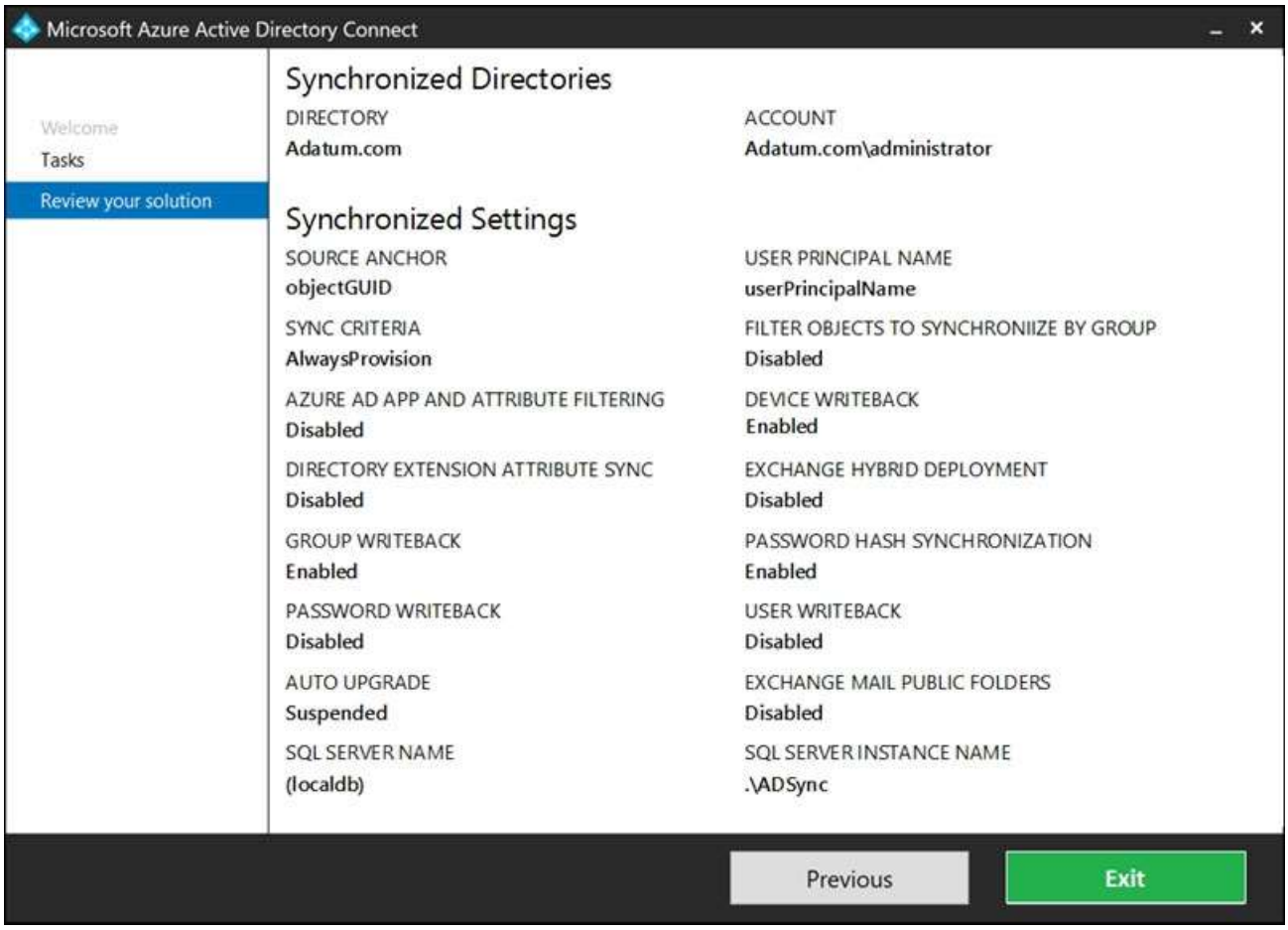
donathon 1 year, 11 months ago
Yes you can click on the license like E5 then it will show the specific service that are enabled.
upvoted 2 times

Jayatheerthan 1 year, 11 months ago
Azure AD Licenses there is is an option Manage your purchased licenses, select the product then search the user in that.
upvoted 1 times

steven1 2 years, 8 months ago
You need Enterprise Mobility + Security E5 for this feature, so I'm not sure A is the right answer.
upvoted 4 times

HOTSPOT -

You have an Active Directory domain named Adatum.com that is synchronized to Azure Active Directory as shown in the exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you create a security group in Azure AD, the group will **[answer choice]**.

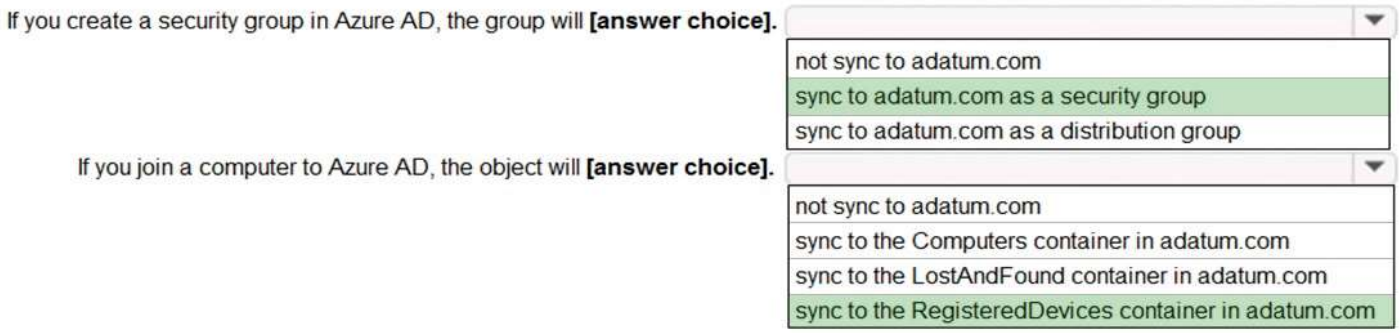
- not sync to adatum.com
- sync to adatum.com as a security group
- sync to adatum.com as a distribution group

If you join a computer to Azure AD, the object will **[answer choice]**.

- not sync to adatum.com
- sync to the Computers container in adatum.com
- sync to the LostAndFound container in adatum.com
- sync to the RegisteredDevices container in adatum.com

Correct Answer:

Answer Area



Group Writeback is enabled in the Azure AD Connect configuration so groups created in Azure Active Directory will be synchronized to the on-premise Active

Directory. A security group created in Azure Active Directory will be synchronized to the on-premise Active Directory as a security group.

Device Writeback is enabled in the Azure AD Connect configuration so computers joined to the Azure Active Directory will be synchronized to the on-premise

Active Directory. They will sync to the RegisteredDevices container in the on-premise Active Directory.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

acamfox224 Highly Voted 1 year, 6 months ago

I am confused... I thought you could only sync O365 groups back to on-prem AD
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback

upvoted 16 times

eknnob 1 year, 6 months ago

you are correct Security group will not sync

upvoted 16 times

LillyLiver 8 months, 1 week ago

At first I was thinking "what are you talking about?" So I tried it out in my tenant. I don't have Exchange on-prem, so I can't enable group writeback. Another condition (from the link you supplied) is that Exchange Hybrid has to be setup. In this question it isn't setu So the group won't be written back.

As I understand it anyway.

upvoted 1 times

RenegadeOrange 2 months ago

Looks like security groups can be writen back to on-prem now.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback-v2

upvoted 4 times

Eltooth Highly Voted 1 year, 6 months ago

Also group write back has specific requirements before only M365 groups can sync back...including Exchange Hybrid. Image shows tha Exchange Hybrid is disabled. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback#pre-requisites

Answer for security group should be “Not synced back to adatum.com.com”

upvoted 9 times

amitsharma170490 Most Recent 3 weeks, 2 days ago

Now you can writeback Azure AD security Groups to On-premise AD: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/h to-connect-group-writeback-v2

upvoted 1 times

rajeshrengasamy 3 weeks, 3 days ago

Answer is correct : Microsoft 365 groups can be written back as Distribution groups, Security groups, or Mail-Enabled Security groups. Azure AD Security groups can be written back as Security groups. (So Azure AD security Group is sync'd as Security Group

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback-v2

upvoted 1 times

Contactfornitish 2 months, 2 weeks ago

1. Only O365 groups sync, not security groups
2. Device writeback enabled so device would sync

upvoted 1 times

charat 4 months, 1 week ago

Security group won't sync to on-prem AD but the device. However, the device will sync to the RegisteredDevices OU as stated on the answer because device writeback is enabled.
Reference article: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

upvoted 1 times

charat 4 months, 1 week ago

Important passage regarding group writeback:
Groups writeback enables customers to leverage cloud groups for their hybrid needs. If you use the Microsoft 365 Groups feature, t
you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange pres
in your on-premises Active Directory.

upvoted 1 times

BoxGhost 5 months, 1 week ago

As others have said, only 365 groups will get written back not security groups.

The second answer is correct, device writeback will sync AAD devices to the RegisteredDevices OU:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback#verify-devices-are-synchronized-to-active-directory

upvoted 1 times

RazielLycas 7 months, 2 weeks ago

Group writeback is for M365 groups only, device writeback send them into the Registered Devices ref:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

upvoted 1 times

tf444 9 months, 1 week ago

After searching and searching more here what I found
No write-back for the security group, for Office 365 group write back you need an Exchange server on the premises.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback
https://docs.microsoft.com/en-us/answers/questions/91022/use-aadconnect-to-create-on-prem-security-groups-a-1.html

upvoted 2 times

fofo1960 12 months ago

I tested on my lab, the Security groups are not written back to my AD, I don't have any device to join it to Azure AD, so additional comm
are welcome

upvoted 1 times

fofo1960 12 months ago

But the Microsoft 365 Group are written back, so Security group wont be Synced down to AD

upvoted 1 times

Davidchercm 1 year, 1 month ago

is the answer for the device showing correct ?

upvoted 2 times

junior6995 1 year ago

For the security group, definitely not syncing, for the computers, I'd go for not syncing as well.

upvoted 2 times

Greyexam 1 year, 3 months ago

All online articles i read seem to indicate that only 365 Groups are compatible with write back.
Yet all questions in these exam files seem to indicate that other groups beyond just the 365 type are able to write back ??
Dammit MS which is it?

upvoted 2 times

RAJULROS 1 year, 4 months ago

MS-100 Exam question on 28May21

upvoted 2 times

PlumpyTumbler 1 year, 4 months ago

MS-101 question anyway.

upvoted 1 times

Goseu 1 year, 5 months ago

Groups writeback enables customers to leverage cloud groups for their hybrid needs. If you use the Microsoft 365 Groups feature, ther you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange present your on-premises Active Directory.

upvoted 1 times

Eltooth 1 year, 6 months ago

AAD security group write back is NOT possible yet. https://feedback.azure.com/forums/34192--general-feedback/suggestions/4080999 in-azure-ad-connect-enable-group-writeback-for-a

upvoted 3 times

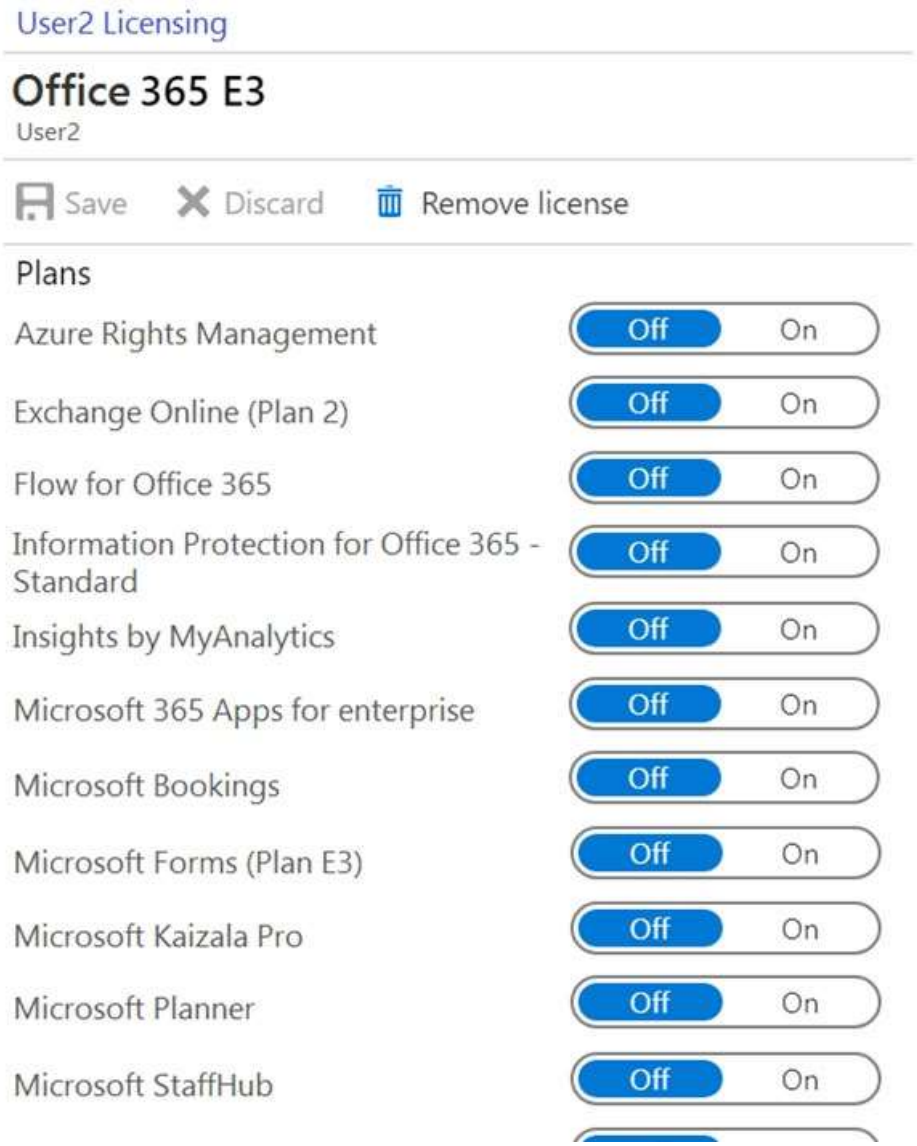
HOTSPOT -

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that includes the users shown in the following table.

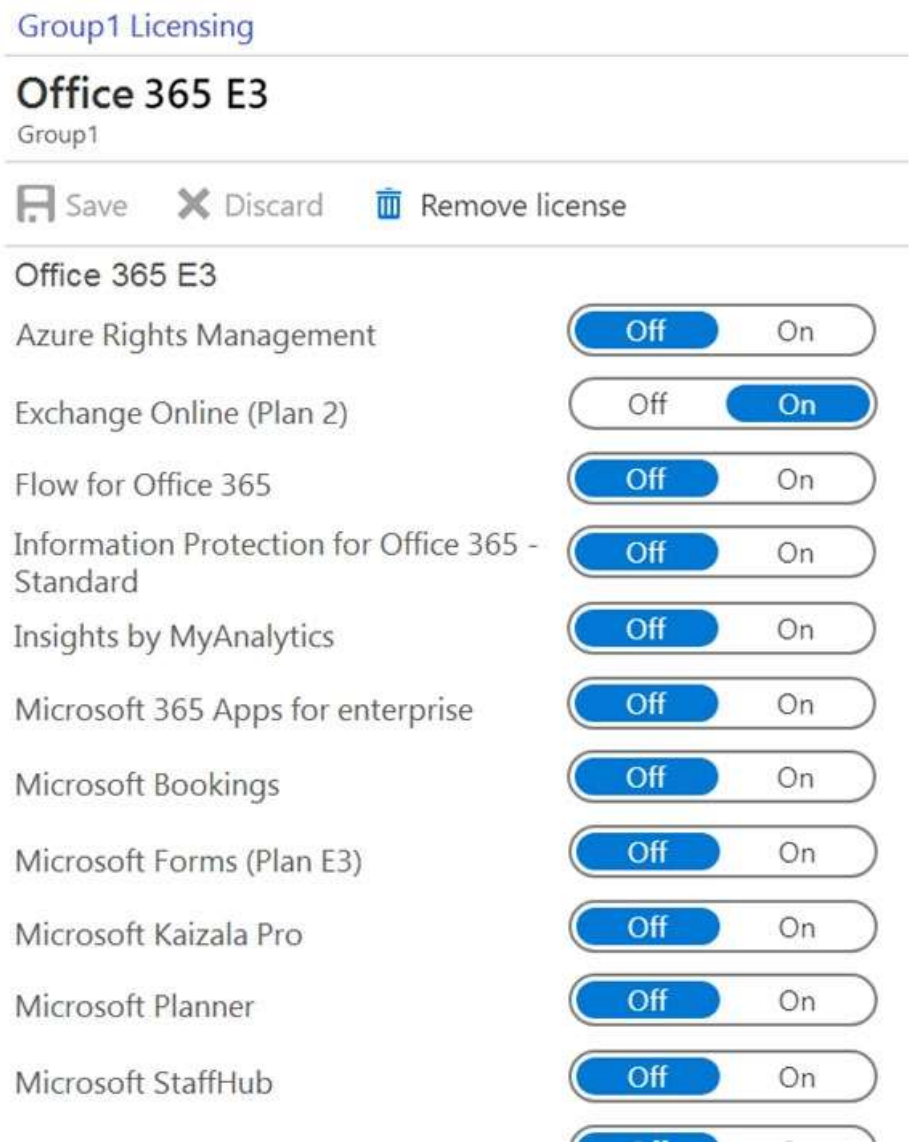
Name	Usage location	Membership
User1	*Not set*	Group1
User2	United States	Group2
User3	United States	*Not applicable*

Group2 is a member of Group1.

You assign Office 365 Enterprise E3 license to User2 as shown in the User2 Licensing exhibit.



You assign Office 365 Enterprise E3 licenses to Group1 as shown in the Group1 Licensing exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 is licensed to use Microsoft Exchange Online.	○	○
User2 is licensed to use Microsoft Exchange Online and Microsoft SharePoint Online.	○	○
If you add User3 to Group2, the user will be licensed to use Microsoft Exchange Online.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 is licensed to use Microsoft Exchange Online.	◯	◯
User2 is licensed to use Microsoft Exchange Online and Microsoft SharePoint Online.	◯	◯
If you add User3 to Group2, the user will be licensed to use Microsoft Exchange Online.	◯	◯

Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.

Therefore, the license granted to Group1 will not filter down to Group2.

Box 1: Yes.

User1 is in Group1 which has been assigned a license to use Exchange Online.

Box 2: No -

User2 has been assigned a license to use SharePoint online. However, the license to use Exchange Online does not apply to User2.

Box 3: No -

The license to use Exchange Online is granted to Group1. However, the license granted to Group1 will not filter down to Group2. Therefore, User3 will not be licensed to use Exchange Online.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-group-advanced

JR_63021 Highly Voted 1 year, 3 months ago

Tested this in my Azure demo environment. Y,N,N is correct

upvoted 10 times

Cheekypoo Most Recent 2 months ago

Was in my exam today 05/08/22.

upvoted 2 times

Contactfornitish 2 months, 2 weeks ago

Nested group membership not supported so user2 would not get any licenses via group2. User1 is part of group1 so would get the license.

upvoted 1 times

davem90 9 months, 1 week ago

Y,N,N - Answer is correct.
Note that any user whose usage location is not specified inherits the location of the Azure AD organization.

upvoted 4 times

tejb 1 year ago

Nested group based licensing is not supported:
Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.

Source: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues

upvoted 4 times

fko1978 1 year, 1 month ago

the trick here is that a group which is a member of another group doesn't get a license... if a license is connected to that other group

upvoted 2 times

spg987 1 year, 1 month ago

it was in my exam

upvoted 2 times

john_gros 1 year, 2 months ago

I think there's an issue here : Group1 has Exchange disabled, thus User1 does not have it and User2 has an "all on" license. If the two pictures were exchanged ("all on" for Group1 and Exchange disabled for User2), the current solution would be right.

I think this should be N,Y,N

upvoted 1 times

Turak64 1 year, 1 month ago

Check again, Exchange is set to "ON"

upvoted 2 times

jjong 1 year ago

its not all ON for group 1... u're seeing it wrongly.. like me. :)

upvoted 1 times

dmillion 1 year, 5 months ago

user2 have the "sharepoint online" selected in the exhibition. not showing in this screenshot.

upvoted 2 times

chaoscreater 1 year, 3 months ago

But not Exchange Online, so answer is still correct.

upvoted 2 times

Eltooth 1 year, 6 months ago

If user location is not set then it will pick up default Azure AD location. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups

upvoted 1 times

kkkeji 1 year, 6 months ago

No/No/No
User1 should fail to assign a license because the usage location is Not set.

upvoted 3 times

syswiz85 1 year, 5 months ago

incorrect, if a usage location is NOT set, it will inherit a location from the group instead.

upvoted 10 times

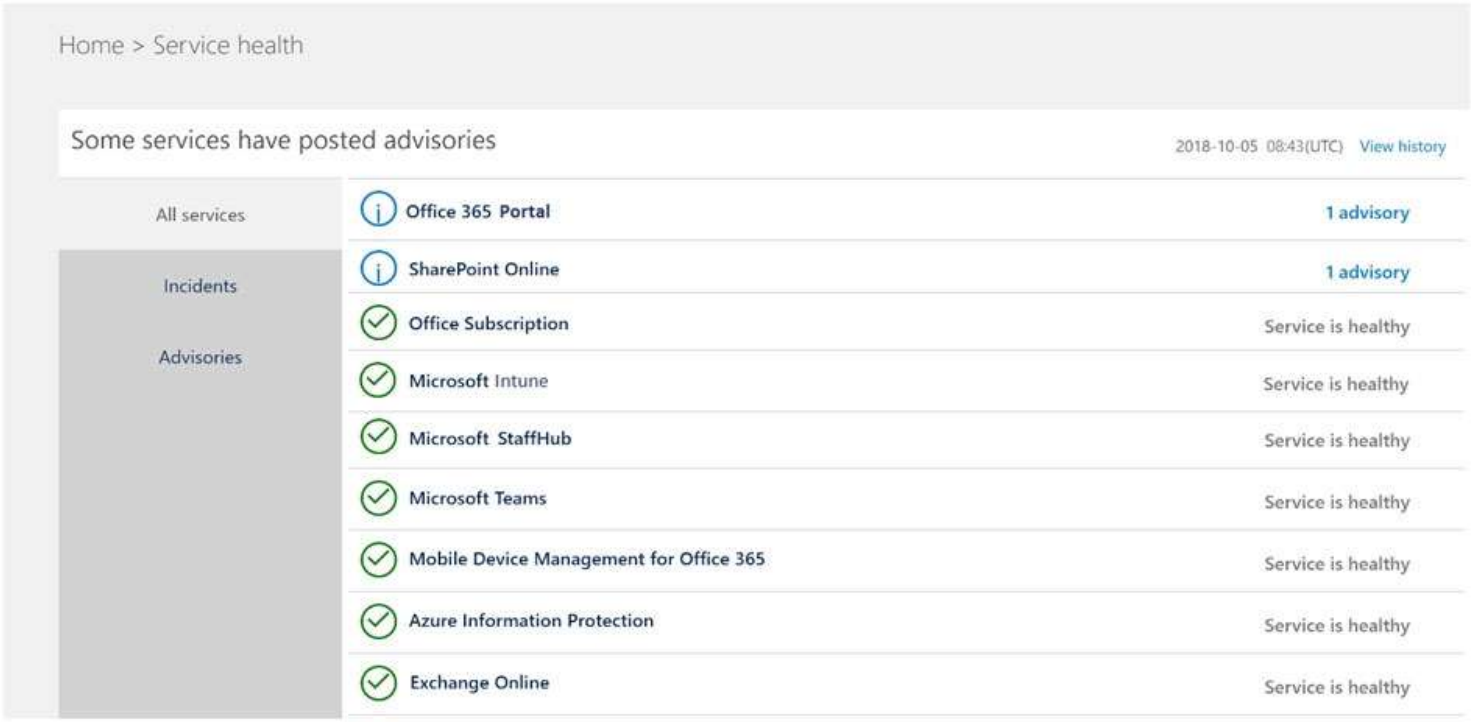
BGM_YKA 1 year, 4 months ago

Location is set with Group membership for that License. Therefore user1 is licensed. Without seeing Sharepoint licensing I believ is beset to assume not licensed. My answer would be Y/N/N

upvoted 5 times

You have a Microsoft 365 subscription.

You view the service advisories shown in the following exhibit.



You need to ensure that users who administer Microsoft SharePoint Online can view the advisories to investigate service health issues.

Which role should you assign to the users?

A. Compliance administrator

B. Message Center reader

C. Reports reader

D. Service administrator

Correct Answer: *D*

People who are assigned the global admin or service administrator role can view service health. To allow Exchange, SharePoint, and Skype for Business admins to view service health, they must also be assigned the Service admin role. For more information about roles that can view service health.

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

Mike3033 Highly Voted 1 year, 2 months ago

The role is actually 'Service Support Administrator'

upvoted 9 times

mic88 1 year ago

It's somehow documented ambiguously...

"People who are assigned the global admin or service support admin role can view service health. To allow Exchange, SharePoint, ar Skype for Business admins to view service health, they must also be assigned the Service admin role. For more information about ro that can view service health, see About admin roles."

upvoted 2 times

trexar Most Recent 6 months ago

Selected Answer: D

A.Compliance admnistrator

Yes, Checking the roles it has read access microsoft.office365.serviceHealth/allEntities/allTasks

Read and configure Office 365 Service Health. BUt it add more muche privilege

B.Message Center Reader

No, it does not show the service Healt

C.Reports reader
No, Checking the role it has read access, I tested It doesn't show the menu
microsoft.azure.serviceHealth/allEntities/allTasks
Read and configure Azure Service Health.

D.Service Administator
Yes, tested
upvoted 2 times

jage01 7 months ago

Selected Answer: D

D.

Service Support admin Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:
- Open and manage service requests
- View and share message center posts
- Monitor service health

https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?preserve-view=true&view=o365-worldwide#commonly-used-microsoft-365-admin-center-roles
upvoted 3 times

trexar 7 months ago

Selected Answer: D

'Service Support Administrator has access to microsoft.azure.serviceHealth/allEntities/allTasks
upvoted 1 times

trexar 7 months ago

Selected Answer: C

Service support administrator have access to microsoft.azure.serviceHealth/allEntities/allTasks
upvoted 1 times

sliix 7 months, 4 weeks ago

Selected Answer: D

https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health. Message center reader can't read service health.
upvoted 4 times

MEC123 8 months, 2 weeks ago

Answer should be D; the role now is Service Support Administrator. The ONLY other role that can do this is the Global Admin. Please se the following link under HOW TO CHECK SERVICE HEALTH. https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide#:~:text=People%20who%20are%20assigned%20the,role%20can%20view%20service%20health.
upvoted 1 times

dumpmaster 8 months, 2 weeks ago

Selected Answer: B

I guess is B: http://shortcutshari.com/o365-update-new-feature-message-center-reader-role/
upvoted 2 times

Claire91 9 months, 4 weeks ago

D for me

Given answer is correct (ish)
Service Administrator is also known as Service Support Administrator
upvoted 1 times

Claire91 9 months, 4 weeks ago

https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide
upvoted 1 times

fofo1960 11 months, 1 week ago

Why not Message Center reader ?
upvoted 1 times

Jubei612 11 months, 2 weeks ago

The users administer. That is the key word to help identify the right answer.
upvoted 1 times

MDLima 11 months, 3 weeks ago

C for me.

It is a tricky answer. As Service Administrator name is changed to Service Support Administrator the answer might be not correct. I wou go as Message Center Reader as I have seen similar question on Measureup (answer was MCR) and although it does not state for least privilege, it wouldn't be incorrect.

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

upvoted 1 times

junior6995 1 year ago

If we follow the least privilege principle the Message Center reader will be more appropriated

upvoted 3 times

Ash473 1 year, 1 month ago

was in exam today

upvoted 2 times

You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. The tenant includes a user named
User1.
You enable Azure AD Identity Protection.
You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.
To which role should you add User1?

A. Security reader

B. User administrator

C. Owner

D. Global administrator

Correct Answer: *A*
The risky sign-ins reports are available to users in the following roles:
- Security Administrator
- Global Administrator
- Security Reader

Of the three roles listed above, the Security Reader role has the least privilege.
Note:
There are several versions of this question in the exam. The question has three possible correct answers:
1. Security Reader
2. Security Administrator
3. Global Administrator

Other incorrect answer options you may see on the exam include the following:
1. Service Administrator.
2. Reports Reader
3. Compliance Administrator

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins

Eltooth Highly Voted 1 year, 6 months ago
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions
upvoted 7 times

dumpmaster Most Recent 8 months, 2 weeks ago
Selected Answer: A
Security reader: View all Identity Protection reports and Overview blade.
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
upvoted 4 times

tejb 1 year ago
Permissions
Identity Protection requires users be a Security Reader, Security Operator, Security Administrator, Global Reader, or Global Administrat
in order to access.

Source: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
upvoted 1 times

fko1978 1 year, 1 month ago
review (=not change) so, Security reader: View all Identity Protection reports and Overview blade
upvoted 2 times

TimurKazan 1 year, 1 month ago

so I would go with Global Admin. User Administrator has nothing to do with Azure Identity Protection
upvoted 1 times

Turak64 1 year, 1 month ago
"The solution must use the principle of least privilege."
upvoted 2 times

TimurKazan 1 year ago
it is actually the least possible privilege to perform such tasks from this list of given roles
upvoted 1 times

Azreal_75 11 months, 4 weeks ago
It isn;t, see role descriptions here: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-ident
protection#permissions
upvoted 3 times

Luiza 1 year, 3 months ago
B. User administrator

"Review" is not "Read"
upvoted 1 times

TimurKazan 1 year, 1 month ago
Correct. but in this case it should be Security Administrator
upvoted 1 times

junior6995 1 year, 4 months ago
Should I consider "Review" and "Read" the same?
upvoted 1 times

airairo 1 year, 4 months ago
This is in ms 101
upvoted 1 times

LouahZA 1 year, 1 month ago
i had this on my first go on ms-100
upvoted 4 times

HOTSPOT -

Your network contains an Active Directory domain and a Microsoft Azure Active Directory (Azure AD) tenant.

You implement directory synchronization for all 10,000 users in the organization.

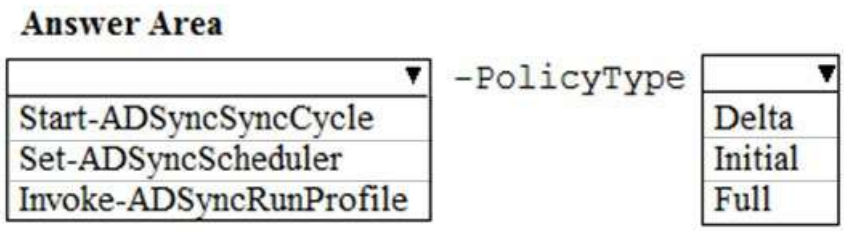
You automate the creation of 100 new user accounts.

You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

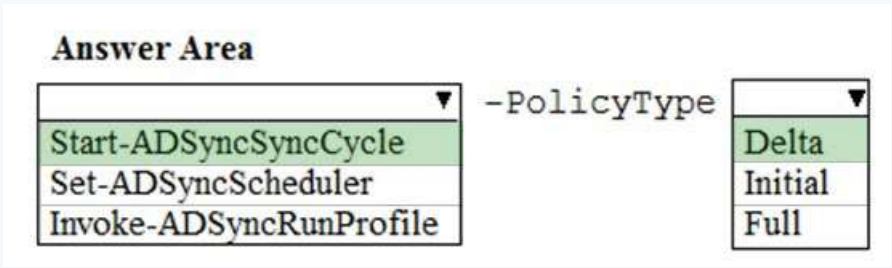
Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Azure AD Connect synchronizes Active Directory to Azure Active Directory on a schedule. The minimum time between synchronizations is 30 minutes.

If you want to synchronize changes to Active Directory without waiting for the next sync cycle, you can initiate a sync by using the Start-AdSyncSyncCycle. The

Delta option synchronizes changes to Active Directory made since the last sync. The Full option synchronizes all Active Directory objects including those that have not changed.

Reference:

https://blogs.technet.microsoft.com/rmilne/2014/10/01/how-to-run-manual-dirsync-azure-active-directory-sync-updates/

mkoprivnj Highly Voted 1 year, 9 months ago

syncsync cycle + delta is correct!

upvoted 12 times

jjong Most Recent 1 year ago

came out today on my exam on 27-sep-21

upvoted 3 times

Ash473 1 year, 1 month ago

in exam today

upvoted 4 times

melatocaroca 1 year, 3 months ago

The fastest method to force Azure AD Connect to synchronize AD and Azure is by running the PowerShell command Start-ADSyncSyncCycle:

Import the ADSync module: Import-Module ADSync
Run the Start-ADSyncSyncCycle command
For delta synchronization use the parameter -PolicyType Delta (used in most situations)
For full synchronization use the parameter -PolicyType Initial (rarely used)
https://www.easy365manager.com/how-to-run-start-adsyncsynccycle/

upvoted 3 times

Alvaroll 2 years ago

2-13 https://www.examtopics.com/exams/microsoft/ms-100/view/12/

upvoted 2 times

saasaa 2 years, 3 months ago

The questions on this page or around are covered by previous pages.
Just mention this so that one can avoid spending and wasting time to rethink the answers s/he's already found out the reasons.

upvoted 3 times

Question #31 *Topic 3*

Your network contains three Active Directory forests.
You create a Microsoft Azure Active Directory (Azure AD) tenant.
You plan to sync the on-premises Active Directory to Azure AD.
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.
What should you include in the recommendation?

A. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

B. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode

C. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode

D. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Correct Answer: *B*
Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

lusis987 Highly Voted 2 years, 7 months ago
If AD can access all 3 forests - enough with one server that syncs everything.
upvoted 17 times

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additio installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom
upvoted 14 times

donathon 2 years ago
Adding on. There's a 1:1 relationship between an Azure AD Connect sync server and an Azure AD tenant. For each Azure AD tenant, need one Azure AD Connect sync server installation. Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan connect-topologies
upvoted 2 times

Cheekypoo Most Recent 2 months ago
Was in my exam today 05/08/22.
upvoted 1 times

charat 4 months, 1 week ago
Selected Answer: B
In exam on 05/22.
upvoted 4 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 1 times

melatocaroca 1 year, 3 months ago
Scenario
Multiple forests, single Azure AD tenant

When you have multiple forests, all forests must be reachable by a single Azure AD Connect sync server. The server must be joined to a domain. If necessary, to reach all forests

Other cases can apply, but question remark
The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies

Answer B
upvoted 1 times

lucidgreen 1 year, 7 months ago
You can only have one AD Connect server active per tenant. So B.
upvoted 3 times

lucidgreen 1 year, 6 months ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies
upvoted 1 times

mkoprivnj 1 year, 9 months ago
B for sure!
upvoted 2 times

kazaki 2 years, 3 months ago
Having more than one Azure AD Connect sync server connected to a single Azure AD tenant is not supported. The exception is the use staging server.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-forests-single-azure-ad-tenant
upvoted 2 times

mmdcert 2 years, 6 months ago
As stated in comments before, but more clearly and with a link:
"Having more than one Azure AD Connect sync server connected to a single Azure AD tenant is not supported. The exception is the use a staging server."
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-forests-single-azure-ad-tenant
upvoted 2 times

VP11 2 years, 6 months ago
When you have multiple forests, all forests must be reachable by a single Azure AD Connect sync server. The server must be joined to a domain. If necessary to reach all forests, you can place the server in a perimeter network (also known as DMZ, demilitarized zone, and screened subnet).
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#staging-server
upvoted 5 times

ibre34 2 years, 7 months ago
Should be A. You can only have 1 ADConnect for forest
upvoted 3 times

WoneSix 2 years, 7 months ago
But ibre, option A has 3 servers. B has only one synch server and one server in staging mode, which is what Microsoft recommends.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#staging-server
upvoted 14 times

WoneSix 2 years, 7 months ago
Sorry, my previous answer wasn't woded right. A TENANT can have only one AAD Connect server. A forest can have as many as necessary, as long as no two of them are synching the same objects. This means that, if there are two AAD Connects, they have t synch to two tenants.
upvoted 4 times

AADapson 1 year, 11 months ago
You can have One Active ADConnect and another one in staging mode. You can't have two active ADConnect
upvoted 1 times

Your network contains an Active Directory domain named adatum.com that is synced to Microsoft Azure Active Directory (Azure AD).
The domain contains 100 user accounts.
The city attribute for all the users is set to the city where the user resides.
You need to modify the value of the city attribute to the three-letter airport code of each city.
What should you do?

A. From Azure Cloud Shell, run the Get-AzureADUser and Set-AzureADUser cmdlets.

B. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.

C. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.

D. From Azure Cloud Shell, run the Get-MsolUser and Set-MSOluser cmdlets.

Correct Answer: *C*
The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.
You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.
Incorrect Answers:
A, D: These answers suggest modifying the city attribute of the users in the Azure Active Directory which is incorrect.
B: This answer has the correct cmdlets but they need to be run on a domain controller, not in the Azure cloud shell.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
Other incorrect answer options you may see on the exam include the following:
1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.
3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser?view=win10-ps

mkoprivnj Highly Voted 1 year, 9 months ago
C for sure. From AD modify city attribute!
upvoted 12 times

lucidgreen 1 year, 5 months ago
Yes, you're modifying the user in AD, not the cloud.
upvoted 4 times

syswiz85 1 year, 5 months ago
100% correct
upvoted 3 times

MomoLomo Most Recent 1 year, 1 month ago
on ms-100
upvoted 1 times

MartiFC 1 year, 2 months ago
C is correct. The change have to from AD on-premises
upvoted 2 times

venwaik 1 year, 2 months ago
Got the question on 19th of July 2021
upvoted 2 times

RAJULROS 1 year, 4 months ago

this question was asked on 28May21

upvoted 3 times

Question #33 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:
- Contoso.com
- East.contoso.com

An Azure AD Connect server is deployed to contoso.com. Azure AD Connect syncs to an Azure Active Directory (Azure AD) tenant.
You deploy a new domain named west.contoso.com to the forest.
You need to ensure that west.contoso.com syncs to the Azure AD tenant.
Solution: From the Azure AD Connect server in contoso.com, you return the setup wizard and include the west.contoso.com domain.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

txrocker13 Highly Voted 1 year, 9 months ago
Since the AADC server lives in contoso.com and that's the forest root, then you add the child domain on west.contoso.com later you jus have to go back and flag that new domain to sync. You can go to 'containers' in the sync manager, or just run the wizard again and che the box for west.contoso.com.
upvoted 17 times

DesertStorm Highly Voted 1 year, 3 months ago
I thought that it should be A (yes) but after deeper investigation in MS documents seems that it B (No) is proper. To add new domain to ADconnect sync you have to execute 2 steps: 1. Change/Modify Adconnect filtering (add new domain). 2. Update Run Profile in Synchronization Service. (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering)
upvoted 9 times

michszym 1 year, 2 months ago
I dont agree with you - read link you provided:
"The installation wizard automates all the tasks that are documented in this topic.
You should only follow these steps if you're unable to run the installation wizard for some reason." --> so you need execute these 2 steps only if you can't run setup wizard.
I think Answer should be A.
we can use Domain-base filtering so there is no need to filter by OU
upvoted 1 times

donb21 Most Recent 1 month, 3 weeks ago
personally i think this should go with A
upvoted 1 times

DenisRossi 3 months, 2 weeks ago
Selected Answer: A
Just run the wizard
upvoted 1 times

Mea988 7 months, 2 weeks ago
Selected Answer: A
Wizard automates everything. A
upvoted 2 times

vnet1 8 months ago
Selected Answer: A
There are two ways to select the domains to be synchronized: - Using the Synchronization Service - Using the Azure AD Connect wizard
upvoted 2 times

VictorPCS 8 months, 1 week ago

Selected Answer: B

Running the wizard again should do the job

upvoted 2 times

kanag1 8 months, 3 weeks ago

Selected Answer: A

The answer is Yes. According to the link below:
The preferred way to change domain-based filtering is by running the installation wizard and changing domain and OU filtering. The installation wizard automates all the tasks that are documented in this topic.

You should only follow these steps if you're unable to run the installation wizard for some reason.
Domain-based filtering configuration consists of these steps:
1. Select the domains that you want to include in the synchronization.
2. For each added and removed domain, adjust the run profiles.
3. Apply and verify changes.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

upvoted 3 times

jkklim 9 months, 1 week ago

answer is yes

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

upvoted 2 times

tejb 1 year ago

Answer is NO. Need to rerun the AAD Connect wizard with "Refresh Schema" option

upvoted 4 times

Chipper 1 year ago

it states that AD connect is already deployed and syncing with the Azure Tenant "An Azure AD Connect server is deployed to contoso.co
Azure AD Connect syncs to an Azure Active Directory (Azure AD) tenant."

So shouldn't the answer be A?

upvoted 2 times

TimurKazan 1 year, 1 month ago

I believe that to sync subdomain it is also required to be added to tenant - no words about it, I would go with B

upvoted 3 times

melatocaroca 1 year, 3 months ago

question is to vague respect,

If you consider High level view the answer must be YES, so A option,

if you consider that they do not provide any further details except inclusion west.contoso.com domain. answer must be B, NO, because
you need the adicional steps, set the account, set the OU to sync, set the features

https://www.smikar.com/second-domain-using-ad-connect/

upvoted 1 times

bwl 1 year, 3 months ago

the ous and all are added in the filter as well.
so even on "high level" you`d only change the filter. as it is a child domain.

upvoted 1 times

F_M 1 year, 4 months ago

You deployed the new subdomain to the forest. If you try to sync with AD Connect an user whose UPN is @west.contoso.com it will app
on AAD with a different domain! As first you have to add the new subdomain to Azure AD. You don't have to verify it since is a subdoma
but you still have to add it!

upvoted 6 times

Comp_technician 1 year, 4 months ago

Answer is A
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

upvoted 2 times

Eltooth 1 year, 6 months ago

A - you are only asked to ensure the new domain syncs to the tenant, not to verify it has been setup in AAD.

upvoted 1 times

james1 1 year, 7 months ago

I agree the answer is NO.
Although the point about a subdomain being automatically verified based on parent domain is correct, you still have to add the domai
Office 365

upvoted 5 times

bake73 7 months, 3 weeks ago

James is the man. Some off you should really rethink your careers.

upvoted 1 times

Question #34 *Topic 3*

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a Microsoft Exchange Server 2019 organization.

You plan to sync the domain to Azure Active Directory (Azure AD) and to enable device writeback and group writeback.

You need to identify which group types will sync from Azure AD.

Which two group types should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. an Office 365 group that uses the Assigned membership type

B. a security group that uses the Dynamic Device membership type

C. an Office 365 group that uses the Dynamic User membership type

D. a security group that uses the Assigned membership type

E. a security group that uses the Dynamic User membership type

Correct Answer: *AC*

Group writeback in Azure AD Connect synchronizes Office 365 groups only from Azure Active Directory back to the on-premise Active Directory.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-preview

VP11 Highly Voted 2 years, 6 months ago

The Group writeback feature does not handle security groups or distribution groups.

upvoted 24 times

sovis29088 Highly Voted 11 months, 3 weeks ago

This question conflicts with a previous one a page or two back where the correct answer indicated that an AzureAD security group wou get written back to local AD as a security group if the group writeback feature was enabled. In the discussion for that question, several people mentioned that only Office 365 groups get written back which seems to be the case here.

upvoted 13 times

RenegadeOrange Most Recent 2 months ago

ABCDE
In AD Connect V2 all are supported.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback-v2

upvoted 7 times

bill1982 2 months, 3 weeks ago

Azure AD Connect group writeback
Article
07/15/2022
7 minutes to read
2 contributors

Group Writeback is the feature that allows you to write cloud groups back to your on-premises Active Directory using the Azure AD Connect Sync client. This feature enables you to manage groups in the cloud, while controlling access to on-premises applications and resources. Group Writeback provides the following capabilities:

Microsoft 365 groups can be written as Distribution groups, Security groups, or Mail-Enabled Security groups.
Azure AD Security groups will be written back as Security groups.
All groups are written back to AD as scope universal.
Allows you to configure group writeback settings for all M365 groups within a tenant.
Nested cloud groups and devices, (if device writeback is also enabled) that are members of groups, enabled for writeback, will be writte back with scope universal.
Now, you can change the common name in an Active Directory group's distinguished name when configuring group writeback in Azure Connect.
You can now configure Azure AD groups to writeback using the Azure AD Admin portal, Graph Explorer, and PowerShell.

upvoted 4 times

trexar 6 months ago

Selected Answer: AC

Groups writeback enables customers to leverage cloud groups for their hybrid needs. If you use the Microsoft 365 Groups feature, ther you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange present your on-premises Active Directory.

upvoted 1 times

Boeroe 7 months, 2 weeks ago

Selected Answer: AC

Only 365 groups are written back if an exchange server is present in the on-premise environment: https://docs.microsoft.com/bs-latn-ba/azure/active-directory/hybrid/how-to-connect-group-writeback

upvoted 2 times

tf444 9 months, 1 week ago

There is an exchange server present.
Groups writeback enables customers to leverage cloud groups for their hybrid needs. If you use the Microsoft 365 Groups feature, ther you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange present your on-premises Active Directory.

upvoted 1 times

tf444 9 months, 2 weeks ago

Q 23 ,topic 3.
https://www.examtopics.com/discussions/microsoft/view/48807-exam-ms-100-topic-3-question-23-discussion/

upvoted 1 times

tf444 9 months, 2 weeks ago

IF the group writeback is enabled in the Azure AD Connect configuration so groups created in Azure Active Directory will be synchroniz to the on-premise Active
Directory. A security group created in Azure Active Directory will be synchronized to the on-premise Active Directory as a security group in another Q in exam topic.

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 1 times

fofo1960 11 months, 4 weeks ago

Tested, and One A & C are correct, Security or Dist groups wont be written back.

upvoted 3 times

Eltooth 1 year, 6 months ago

Agree - A & C.
Exam topic #2, Q22

Group write back has specific requirements before only M365 groups can sync back...including Exchange Hybrid.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback#pre-requisites

upvoted 4 times

MerryWeasel 1 year, 8 months ago

Here are some references: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback https://docs.microsoft.com/en-us/exchange/hybrid-deployment/set-up-microsoft-365-groups#enable-group-writeback-in-azure-ad-connect

upvoted 2 times

mkoprivnj 1 year, 9 months ago

A & C for sure!

upvoted 3 times

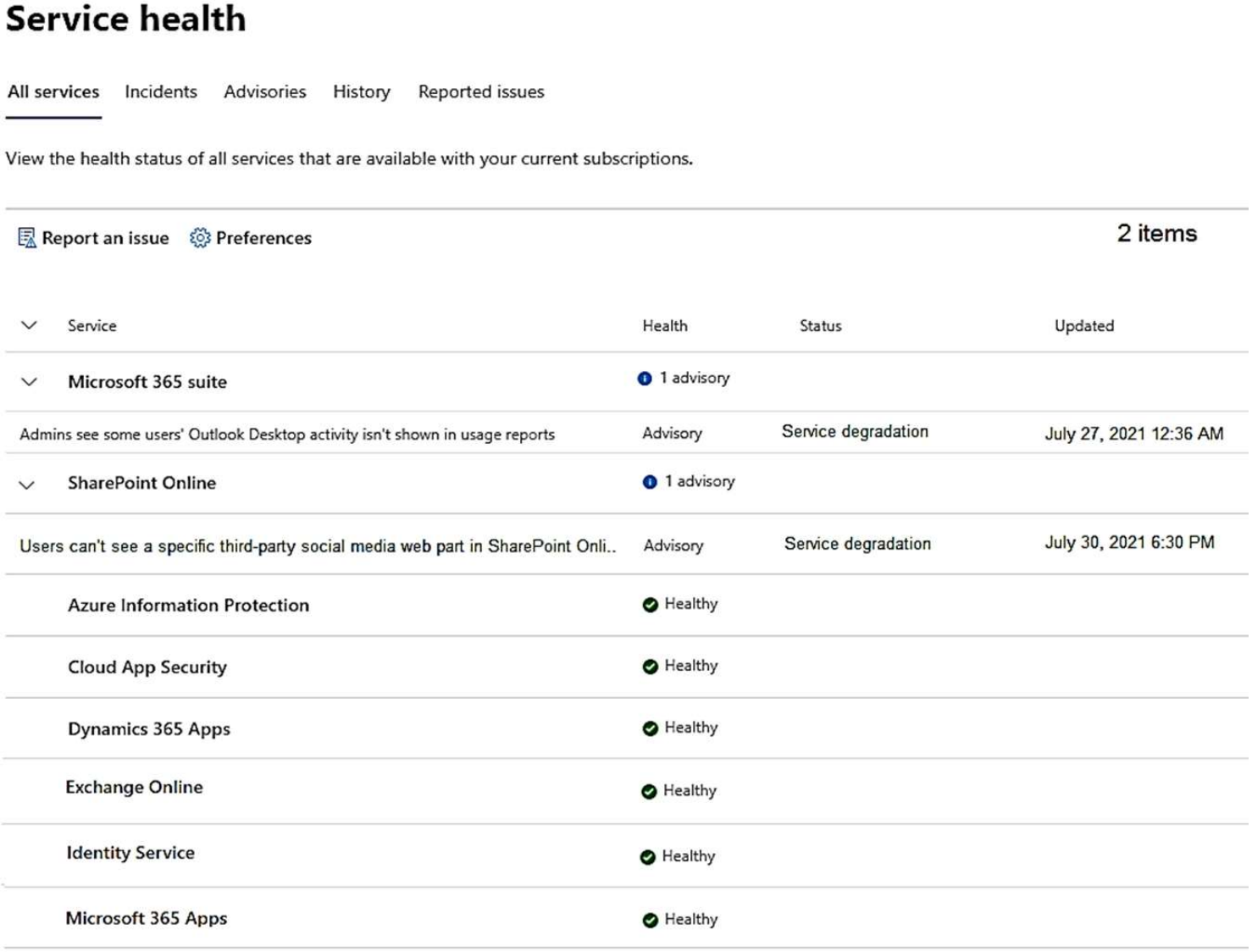
phvogel 1 year, 12 months ago

The question is really asking which of these groups could you use (I read it as "which two groups must be used together" but only one required). Writeback only works with Office 365 groups.

upvoted 4 times

You have a Microsoft 365 subscription.

You view the service advisories shown in the following exhibit.



You need to ensure that a user named User1 can view the advisories to investigate service health issues.

Which role should you assign to User1?

A. Compliance administrator

B. Message Center reader

C. Reports reader

D. Service administrator

Correct Answer: *D*

People who are assigned the global admin or service administrator role can view service health. To allow Exchange, SharePoint, and Skype for Business admins to view service health, they must also be assigned the Service admin role.

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

boxojunk 1 week, 4 days ago

Selected Answer: D

Correct

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

upvoted 1 times

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD).
The on-premises network contains a Microsoft SharePoint Server 2019 farm.
The company purchases a Microsoft 365 subscription.
You have the users shown in the following table

Name	Source
User1	Windows Active Directory
User2	Azure Active Directory

You plan to assign User1 and User2 the required roles to run the SharePoint Hybrid Configuration Wizard.
User1 will be used for on-premises credentials and User2 will be used for cloud credentials.
You need to assign the correct role to User2. The solution must use the principle of least privilege.
Which role should you assign to User2?

A. Application administrator

B. SharePoint farm administrator

C. Global administrator

D. SharePoint administrator

Correct Answer: *C*
To run the SharePoint Hybrid Configuration Wizard, you need to provide credentials of a user (in this case User2) of a Global Administrator account in Azure
Active Directory.
Reference:
https://www.c-sharpcorner.com/article/sharepoint-2019-enable-hybrid-experience/

Eltooth Highly Voted 1 year, 6 months ago
C - https://docs.microsoft.com/en-us/sharepoint/hybrid/accounts-needed-for-hybrid-configuration-and-testing
upvoted 11 times

charat Most Recent 4 months, 1 week ago
Selected Answer: C
Good question. C is the answer
upvoted 2 times

RazielLycas 7 months, 2 weeks ago
Selected Answer: C
maybe a better reference https://docs.microsoft.com/en-us/sharepoint/hybrid/hybrid-picker-in-the-sharepoint-online-admin-center
upvoted 1 times

MomoLomo 1 year, 1 month ago
on ms-100
upvoted 2 times

PlumpyTumbler 1 year, 4 months ago
This is on MS-101.
upvoted 2 times

HOTSPOT -

Your network contains an on-premises Active Directory domain named contoso.com.

Your company purchases a Microsoft 365 subscription and establishes a hybrid deployment of Azure Active Directory (Azure AD) by using password hash synchronization. Password writeback is disabled in Azure AD Connect.

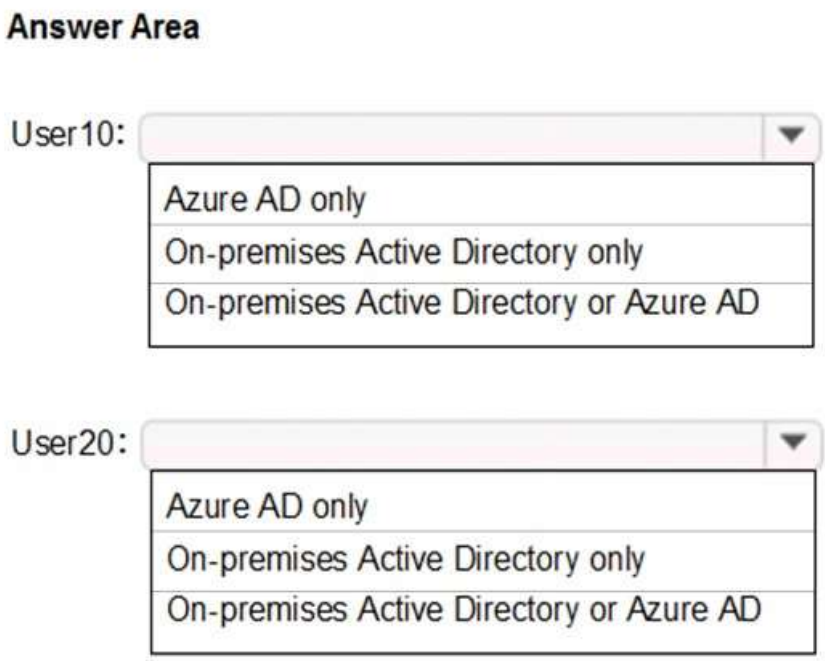
You create a new user named User10 on-premises and a new user named User20 in Azure AD.

You need to identify where an administrator can reset the password of each new user.

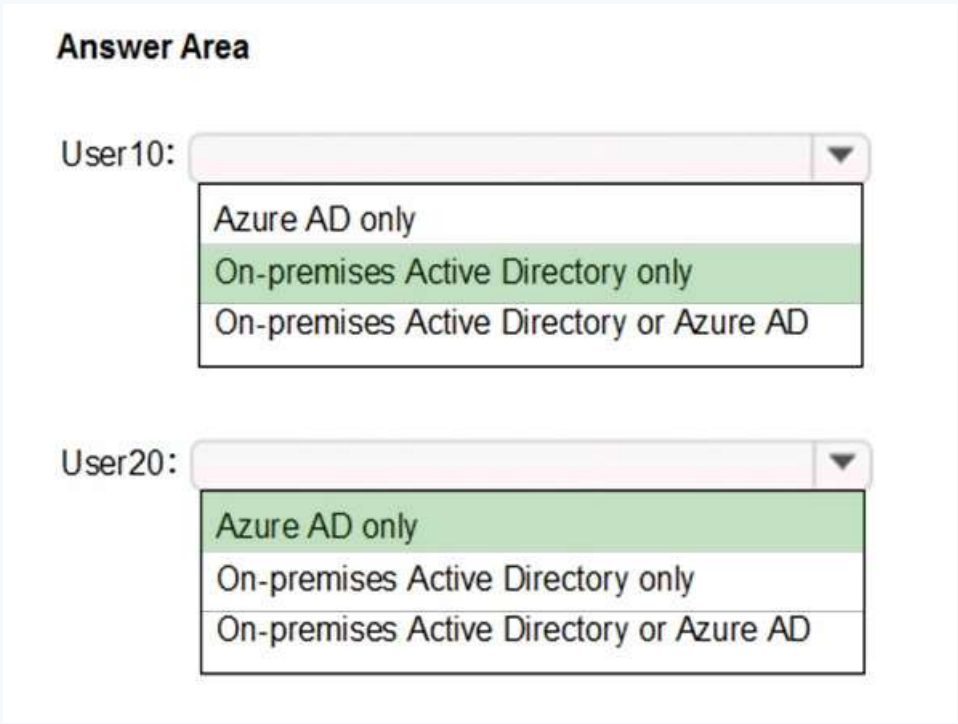
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



If a user account is created in the on-premise Active Directory and synchronized to Azure Active Directory, you can reset the password of the user account in the on-premise Active Directory only.

If a user account is created in Azure Active Directory, you can reset the password of the user account in the Azure Active Directory only.

syswiz85 Highly Voted 1 year, 5 months ago

If you reset a password for a synced user in Azure AD, then yes it will reset, but only for a short period of time until Azure AD syncs bac the on-premise credentials, so this is not a viable solution. Answers provided are 100% correct without a doubt.

upvoted 8 times

Moderator Most Recent 1 month, 2 weeks ago

Question still valid (30th July 2022).

upvoted 1 times

tcmaggio 10 months, 1 week ago

I will stand with given answer BUT, imho, the Admin COULD reset password either using AD (hash sync) or AzAd. Of course, AzAd woul the better way: Yes! But the question says: where you CAN, not which would be the better way to do so.

upvoted 2 times

TimurKazan 1 year, 1 month ago

User 10 - both
Password-writeback - When this option is enabled, password change events cause Azure AD Connect to synchronize the updated credentials back to the on-premises AD DS environment.
user20 - since this is cloud user, the only option is Azure AD

upvoted 2 times

TimurKazan 1 year, 1 month ago

Sorry, User10 - AD only, since password writeback is disabled

upvoted 15 times

Ash473 1 year, 1 month ago

in exam today

upvoted 2 times

chan2013 1 year, 6 months ago

If writeback is enabled then Azure AD password sync to On-Prem. In this case, it is not enabled

upvoted 2 times

prepre 1 year, 6 months ago

Technically you can change the password in Azure AD and the Local AD, but if you change it in AAD they will no longer be synced??

upvoted 1 times

chaoscreater 1 year, 3 months ago

On the next sync, on-prem changes should replicate to AAD and overwrite it. On-prem is the source of authority.

upvoted 2 times

Question #38 *Topic 3*

Your network contains an Active Directory forest named contoso.local.
You have a Microsoft 365 subscription.
You plan to implement a directory synchronization solution that will use password hash synchronization.
From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.
You need to prepare the environment for the planned directory synchronization solution.
What should you do first?

A. From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.

B. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.

C. From the Microsoft 365 admin center, verify the contoso.local domain name.

D. From Active Directory Users and Computers, modify the UPN suffix for all users.

Correct Answer: *B*
The on-premise Active Directory domain is named contoso.local. Therefore, all the domain users accounts will have a UPN suffix of contoso.local by default.
To enable directory synchronization that will use password hash synchronization, you need to configure the domain user accounts to have the same UPN suffix as the verified domain (contoso.com in this case). Before you can change the UPN suffix of the domain user accounts to contoso.com, you need to add contoso.com as a UPN suffix in the domain.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-userprincipalname

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
The on-premise Active Directory domain is named contoso.local. Therefore, all the domain users accounts will have a UPN suffix of contoso.local by default.
To enable directory synchronization that will use password hash synchronization, you need to configure the domain user accounts to h
the same UPN suffix as the verified domain (contoso.com in this case). Before you can change the UPN suffix of the domain user accou
to contoso.com, you need to add contoso.com as a UPN suffix in the domain.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-userprincipalname
upvoted 19 times

DavidSapery Highly Voted 2 years, 3 months ago
Correct answer. It says what do you do FIRST, which is add the .com domain to the UPN suffixes. Only after you do that can you modify users' UPN suffixes.
upvoted 12 times

mikl Most Recent 1 year, 6 months ago
Think "B. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix." is correct.
upvoted 2 times

Parvezg 1 year, 7 months ago
It's B. add contoso.com as a UPN suffix and then update users with new upn (contoso.com) before kicking off AAD connect installation.
upvoted 2 times

mkoprivnj 1 year, 9 months ago
B. add contoso.com as a UPN suffix
upvoted 2 times

ExamTopic 2 years, 4 months ago
https://docs.microsoft.com/en-us/office365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization
upvoted 5 times

Your company has a Microsoft 365 subscription.

Your plan to add 100 newly hired temporary users to the subscription next week.

You create the user accounts for the new users.

You need to assign licenses to the new users.

Which command should you run?

A.

```
$NewStaff = Get-AzureADUser -All -Department "Temp" -UsageLocation "";
$NewStaff | foreach {Set-AzureADUser -LicenseOptions "contoso:ENTERPRISEPACK"}
```

B.

```
$NewStaff = Get-AzureADUser -All -Department "Temp" -UsageLocation "US" -UnlicensedUsersOnly;
$NewStaff | foreach {Set-AzureADUserLicense -AddLicenses "contoso:ENTERPRISEPACK"}
```

C.

```
$NewStaff = Get-AzureADUser -All -Department "Temp" -UsageLocation "";
$NewStaff | foreach {Set-AzureADUserLicense -LicenseOptions "contoso:ENTERPRISEPACK"}
```

D.

```
$NewStaff = Get-AzureADUser -All -Department "Temp" -UsageLocation "US" -UnlicensedUsersOnly;
$NewStaff | foreach {Set-AzureADUser -AddLicenses "contoso:ENTERPRISEPACK"}
```

Correct Answer: *B*

The first line gets all users from the Temp department that have a UsageLocation assigned and stores them in the $NewStaff variable. You cannot use PowerShell to assign a license to a user that does not have a UsageLocation configured.

The second line adds the licenses to each user in the $NewStaff variable.

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/powershell/assign-licenses-to-user-accounts-with-office-365-powershell

hhaywood Highly Voted 1 year, 4 months ago

incorrect syntax - should be Set-AzureADUserLicense -AssignedLicenses "

upvoted 5 times

F_M 1 year, 4 months ago

And Get-ADUser -All -Filter "Department eq 'Temp'"

upvoted 1 times

chaoscreater 1 year, 3 months ago

That's for onprem, not AAD

upvoted 1 times

F_M 1 year, 3 months ago

Sorry, Get-AzureADUser -All -Filter "Department eq 'Temp'"

upvoted 1 times

emanresu Most Recent 5 months, 1 week ago

Answer B is correct but Set-AzureADUserLicense will be retired and replaced with Set-MgUserLicense
https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365
worldwide

upvoted 3 times

Wojer 9 months, 1 week ago

the first part is completely wrong because department and usage location are not a part of that command
that is the proper second part Set-AzureADUserLicense -AssignedLicenses

upvoted 1 times

YClaveria 11 months, 2 weeks ago

B is right if Get-MsolUser and Set-MsolUserLicense have been used.

upvoted 2 times

lafcow 1 year, 1 month ago

♦ C
$userUPN="<user sign-in name (UPN)>"
$planName="<license plan name from the list of license plans>"
$License = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$License.SkuId = (Get-AzureADSubscribedSku | Where-Object -Property SkuPartNumber -Value $planName -EQ).SkuID
$LicensesToAssign = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$LicensesToAssign.AddLicenses = $License
Set-AzureADUserLicense -ObjectId $userUPN -AssignedLicenses $LicensesToAssign
upvoted 1 times

lafcow 1 year, 1 month ago

Actually there are no correct answers listed... "TimurKazan: should be B, but instead of ""-addlicenses" there must be "-assignedlicenses""
upvoted 1 times

TimurKazan 1 year, 1 month ago

should be B, but instead of ""-addlicenses" there must be "-assignedlicenses"
upvoted 3 times

melatocaroca 1 year, 3 months ago

to apply a license to a user using the Azure AD cmdlets (note the prefix):

Create the objects we'll need to add and remove licenses
$license = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$licenses = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses

Find the SkuID of the license we want to add – in this example we'll use the O365_BUSINESS_PREMIUM license
$license.SkuId = (Get-AzureADSubscribedSku | Where-Object -Property SkuPartNumber -Value "O365_BUSINESS_PREMIUM" -EQ).SkuID

Set the Office license as the license we want to add in the $licenses object
$licenses.AddLicenses = $license

Call the Set-AzureADUserLicense cmdlet to set the license.
Set-AzureADUserLicense -ObjectId "Violeta.Collias@drumkit.onmicrosoft.com" -AssignedLicenses $licenses

So only B and C use Set-AzureADUserLicense, but location is only set in B, Answer B
upvoted 4 times

VikingSWE 1 year, 4 months ago

None of the answers seem correct.
https://docs.microsoft.com/en-us/powershell/module/azuread/set-azureaduserlicense?view=azureadps-2.0
upvoted 2 times

Question #40 *Topic 3*

Your network contains an Active Directory domain and a Microsoft Azure Active Directory (Azure AD) tenant.

The network uses a firewall that contains a list of allowed outbound domains.

You begin to implement directory synchronization.

You discover that the firewall configuration contains only the following domain names in the list of allowed domains:

☞ *.microsoft.com

*.office.com

▪

Directory synchronization fails.

You need to ensure that directory synchronization completes successfully.

What is the best approach to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. From the firewall, allow the IP address range of the Azure data center for outbound communication.

B. From Azure AD Connect, modify the Customize synchronization options task.

C. Deploy an Azure AD Connect sync server in staging mode.

D. From the firewall, create a list of allowed inbound domains.

E. From the firewall, modify the list of allowed outbound domains.

Correct Answer: *E*

Azure AD Connect needs to be able to connect to various Microsoft domains such as login.microsoftonline.com. Therefore, you need to modify the list of allowed outbound domains on the firewall.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-ports

Wojer 9 months, 1 week ago

Hybrid Azure AD join requires devices to have access to the following Microsoft resources from inside your organization's network:

https://enterpriseregistration.windows.net
https://login.microsoftonline.com
https://device.login.microsoftonline.com
https://autologon.microsoftazuread-sso.com (If you use or plan to use seamless SSO)

upvoted 2 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

junior6995 1 year ago

It doesn't feel right to only allow outbound connections, what if the tenant has a PHS enabled or a device writeback? I'd allow inbound outbound.

upvoted 1 times

Eggsamine 11 months, 2 weeks ago

PHS, device and password writeback will all use the outbound connection from Azure AD Connect to communicate. No need for an explicit inbound rule as the firewall should handle it.

upvoted 4 times

Rudelke 3 months, 2 weeks ago

You can set up Azure AD Connect from LAN network with no public address, port forwarding or anything like that.
Simple conclusion is that Azure AD Connect does not need inbound connection.

Also notice that changes are written back only as AD Connect does the sync cycle. In other words changes are written back only whe AD Connect reaches out to Azure to gets an update.

upvoted 1 times

maikelb 1 year, 4 months ago

correct!

upvoted 2 times

Question #41 *Topic 3*

Your network contains an on-premises Active Directory forest.
You are evaluating the implementation of Microsoft 365 and the deployment of an authentication strategy.
You need to recommend an authentication strategy that meets the following requirements:
- Allows users to sign in by using smart card-based certificates
- Allows users to connect to on-premises and Microsoft 365 services by using SSO

Which authentication strategy should you recommend?

A. password hash synchronization and seamless SSO

B. federation with Active Directory Federation Services (AD FS)

C. pass-through authentication and seamless SSO

Correct Answer: *B*
Federation with Active Directory Federation Services (AD FS) is required to allow users to sign in by using smart card-based certificates.

Federated authentication -
When you choose this authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises
Active Directory Federation Services (AD FS), to validate the user's password.
The authentication system can provide additional advanced authentication requirements. Examples are smartcard-based authentication or third-party multifactor authentication.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

Jhill777 Highly Voted 2 years, 4 months ago
Smartcard is the key word.
upvoted 16 times

ctfalci Highly Voted 2 years, 2 months ago
Answer: B
Explanation
References:
Federation with Active Directory Federation Services (AD FS) is required to allow users to sign in by using smart card-based certificates.
Federated authentication
When you choose this authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.
The authentication system can provide additional advanced authentication requirements. Examples are smartcard-based authentication or third-party multifactor authentication.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn
upvoted 16 times

NHaikes Most Recent 2 months, 2 weeks ago
Link needs to be updated: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#comparing-methods
upvoted 2 times

Carlo5 1 year, 4 months ago
Update the reference link:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 1 times

mkoprivnj 1 year, 9 months ago
B for sure! ctfalci
upvoted 3 times

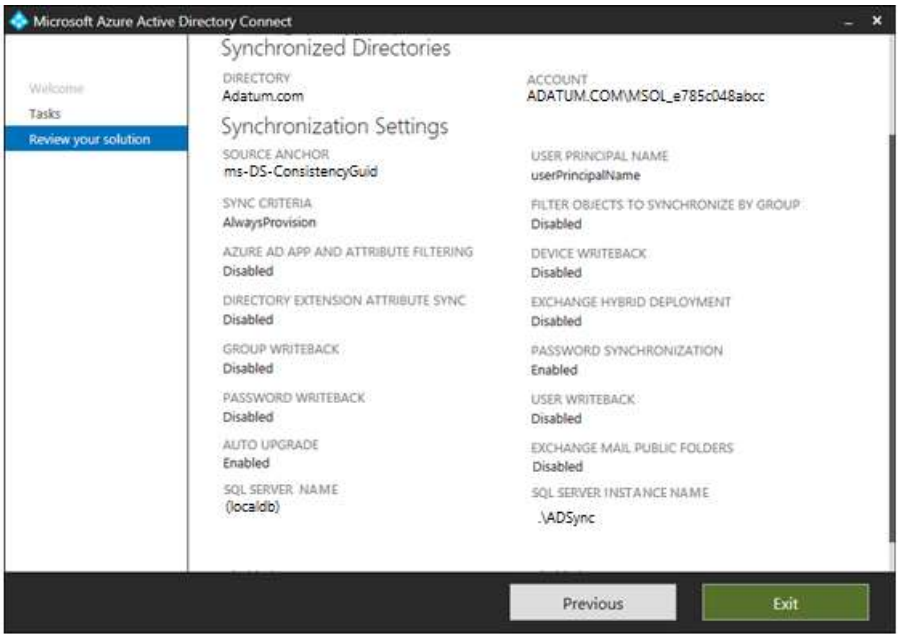
HLBJani 2 years, 4 months ago

Right link:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 4 times

HOTSPOT -

Your network contains an on-premises Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD) as shown in the following exhibit.



An on-premises Active Directory user account named Allan Yoo is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan@adatum.onmicrosoft.com.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	○	○
From the Azure portal, you can configure the job title of Allan Yoo.	○	○
From the Azure portal, you can configure the usage location of Allan Yoo.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	○	○
From the Azure portal, you can configure the job title of Allan Yoo.	○	○
From the Azure portal, you can configure the usage location of Allan Yoo.	○	○

Allan Yoo's user account is synchronized from the on-premise Active Directory. This means that most user account settings have to be configured in the on- premise Active Directory.

In the exhibit, Password Writeback is disabled. Therefore, you cannot reset the password of Allan Yoo from the Azure portal.

You also cannot change Allan Yoo's job title in the Azure portal because his account is synchronized from the on-premise Active Directory.

One setting that you can configure for synchronized user accounts I the usage location. The usage location must be configured on a user account before you can assign licenses to the user.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

fofo1960 Highly Voted 11 months, 4 weeks ago

No - Write Back is disabled
No - Tested on my Tenant, and you cannot change the Job Title
Yes - you can change it from the AAD Portal

upvoted 8 times

ARYMBS Most Recent 5 months, 1 week ago

YNY
Yes you can reset password on AAD but it will never sync - disabled password writeback.

upvoted 1 times

Karvon 4 months, 2 weeks ago

Not right. It displays that the setting is handled by your on premise. N N Y

upvoted 5 times

Wojer 9 months, 1 week ago

first of all, question is not saying about syncing back to AD.
so you can change all of those things because this account is on adatum.onmicrosoft.com
This is how I think

upvoted 1 times

joergsi 8 months, 1 week ago

The question is not saying, but the image does!

upvoted 2 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

zacmzee 1 year ago

Provided answer is correct. You can change the job title in Azure AD but it will get overwritten upon next sync. Only if you take the question literally on wording, than yes, you can change job title for user in Azure AD.

upvoted 3 times

emilianogalati 1 year ago

Maybe I am an idiot but...
The question is if you CAN.

I have not tested (I don't have an on-prem environment to do it), but you should be able to reset password. The only problem is that th it syncs again, because there is no writeback. The same should be for Job Position.

I know, it's subtle.
Is there anyone that tested it?

upvoted 1 times

Comp_technician 1 year, 4 months ago

NO - YES - NO

upvoted 1 times

melatocaroca 1 year, 3 months ago

N,N,Y
Usage Location is assigned based on the location of Azure Active Directory and this will be same for all the users who does not have "UsageLocation" populated in AD
Being literal to the question statement

You also can, modify Allan job title in the Azure portal but because his account is synchronized from the on-premise Active Directory overwrite the Azure AD change,

upvoted 7 times

subbuhotmail 1 year, 2 months ago

I think User Writeback is disable, so it wont update the changes from AAD to AD. It has to be modified in AD only.

upvoted 1 times

gkp_br 1 year, 4 months ago

Username is set @adatum.onmicrosoft.com. I think in this case it is possible change the password from the Azure Portal.

upvoted 1 times

chaoscreater 1 year, 3 months ago

UPN has nothing to do with changing password from either onprem or in AAD. You're missing the point here.

upvoted 3 times

gkp_br 1 year, 3 months ago

Sorry, but you are wrong. Test this and see it.

upvoted 1 times

Turak64 1 year, 1 month ago

The UPN isn't realted to a password change, look up the metaverse and how it connects on-prem to cloud IDs

upvoted 2 times

chaoscreater 1 year, 3 months ago

How about you read your own comment below, which proved my point?

upvoted 3 times

gkp_br 1 year, 4 months ago

bu the password will not be sync with on-premises Active Directory.

upvoted 2 times

wonap 1 year, 5 months ago

In my opinion
1 Yes (writeback enabled)
2 No
3 Yes

upvoted 1 times

sadsadweqr23424dsdqweqwe 1 year, 5 months ago

Password writeback disabled

upvoted 15 times

HOTSPOT -

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).

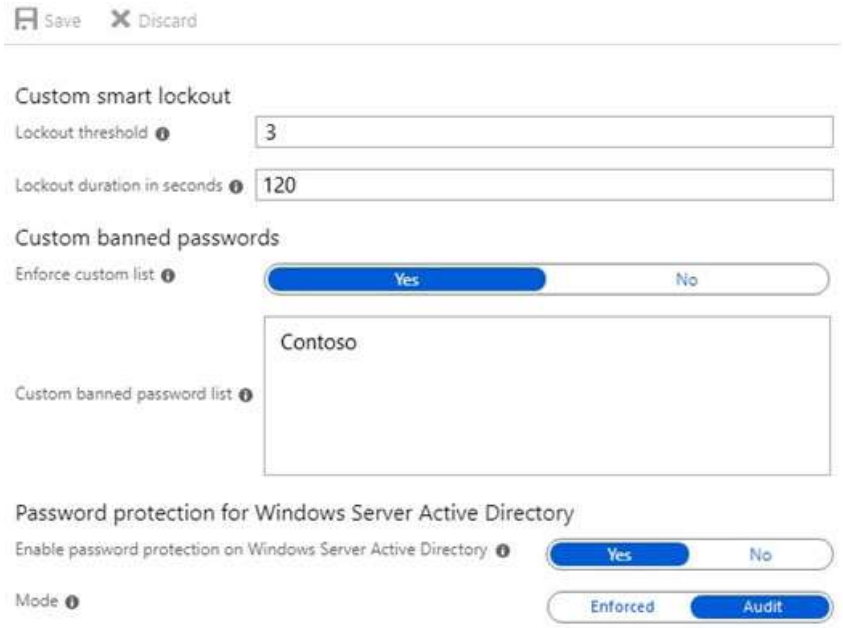
You have users in contoso.com as shown in the following table.

Name	Source
User1	Azure Active Directory
User2	Azure Active Directory
User3	Windows Active Directory

The users have the passwords shown in the following table.

Name	Password
User1	Contoso123
User2	N3w3rT0Gue33
User3	ComplexPassword33

You implement password protection as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

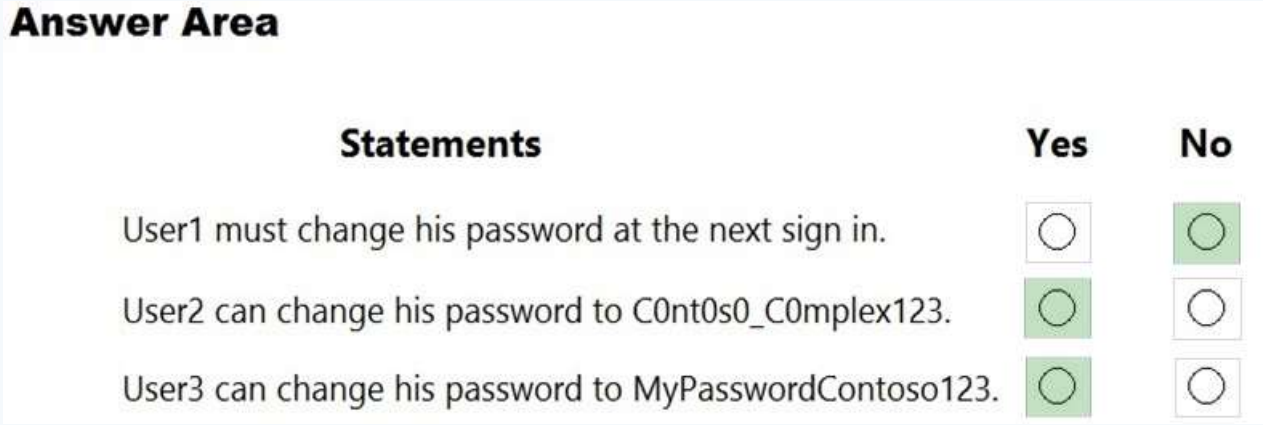
Hot Area:

Answer Area

Statements	Yes	No
User1 must change his password at the next sign in.	◯	◯
User2 can change his password to C0nt0s0_C0mplex123.	◯	◯
User3 can change his password to MyPasswordContoso123.	◯	◯

Correct Answer:

Answer Area



Box 1: No -

User1's password contains the banned password 'Contoso'. However, User1 will not be required to change his password at next sign in. When the password expires or when User1 (or an administrator) changes the password, the password will be evaluated and will have to meet the password requirements.

Box 2: Yes -

Password evaluation goes through several steps including normalization and Substring matching which is used on the normalized password to check for the user's first and last name as well as the tenant name. Normalization is the process of converting common letter substitutes into letters. For example, 0 converts to o. $ converts to s. etc.

The next step is to identify all instances of banned passwords in the user's normalized new password. Then:

1. Each banned password that is found in a user's password is given one point.
2. Each remaining unique character is given one point.
3. A password must be at least five (5) points for it to be accepted.

'C0nt0s0' becomes 'contoso' after normalization. Therefore, C0nt0s0_C0mplex123 contains one instance of the banned password (contoso) so that equals 1 point. After 'contoso', there are 11 unique characters. Therefore, the score for 'C0nt0s0_C0mplex123' is 12. This is more than the required 5 points so the password is acceptable.

Box 3:

The 'Password protection for Windows Server Active Directory' is in 'Audit' mode. This means that the password protection rules are not applied. Audit mode is for logging policy violations before putting the password protection 'live' by changing the mode to 'enforced'.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

lucidgreen Highly Voted 1 year, 5 months ago

The policy is in Audit mode. So it isn't enforced. Passwords can be whatever they want.

upvoted 9 times

Scooter454 1 year, 5 months ago

Audit mode is only for Active Directory accounts. It is enabled for Azure users, so User 1 and User 2 has this policy applied

upvoted 12 times

charat 4 months, 1 week ago

That's incorrect.
"Audit mode is intended as a way to run the software in a "what if" mode. Each Azure AD Password Protection DC agent service evaluates an incoming password according to the currently active policy.

If the current policy is configured to be in audit mode, "bad" passwords result in event log messages but are processed and updated. This behavior is the only difference between audit and enforce mode. All other operations run the same."

upvoted 2 times

TechMinerUK Most Recent 3 months, 3 weeks ago

The answer is correct due to the following:

1. AADPP doesn't assess existing passwords, I can testify to this as when rolling it out if a user has a password deemed unacceptable th will not be automatically forced to reset it.
2. As mentioned here (https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#how-are-passwords-evaluated) even if a password contains words which are banned providing the score is over 5 it will be accepted
3. The picture illustrates that AADPP is not being enforced on prem so if a user has a banned password in AD it will be audited but not banned

upvoted 2 times

PmgCosta 5 months, 1 week ago

From: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection

What are banned password lists?
Azure AD includes a global banned password list. The contents of the global banned password list isn't based on any external data sou
Instead, the global banned password list is based on the ongoing results of Azure AD security telemetry and analysis. When a user or
administrator tries to change or reset their credentials, the desired password is checked against the list of banned passwords. The
password change request fails if there's a match in the global banned password list. You can't edit this default global banned passwor
list.

URL talks, when user Change ou Reset password, if it already set User1 don't need to change their password

upvoted 1 times

PmgCosta 5 months, 1 week ago

More info: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-faq#does
azure-ad-password-protection-validate-existing-passwords-after-being-installed

Does Azure AD Password Protection validate existing passwords after being installed?
No - Azure AD Password Protection can only enforce password policy on cleartext passwords during a password change or set
operation. Once a password is accepted by Active Directory, only authentication-protocol-specific hashes of that password are
persisted. The clear-text password is never persisted, therefore Azure AD Password Protection cannot validate existing passwords.

After initial deployment of Azure AD Password Protection, all users and accounts will eventually start using an Azure AD Password
Protection-validated password as their existing passwords expire normally over time. If desired, this process can be accelerated by a
one-time manual expiration of user account passwords.

Accounts configured with "password never expires" will never be forced to change their password unless manual expiration is done.

upvoted 1 times

musiman 6 months ago

It should be N N Y.

User2 wants to use C0nt0s0 and he uses common letter substitution. Smart lockout also checks for common letter substitutions.

A new password first goes through a normalization process. This technique allows for a small set of banned passwords to be mapped t
much larger set of potentially weak passwords.

Normalization has the following two parts:

All uppercase letters are changed to lower case.

Then, common character substitutions are performed, such as in the following example:
o => 0
s => $
l => 1
etc.

Source: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#how-are-passwords-
evaluated

upvoted 2 times

Ltgoldman 5 days, 9 hours ago

"Even if a user's password contains a banned password, the password may be accepted if the overall password is otherwise strong
enough."

upvoted 1 times

Jcbrow27 10 months, 2 weeks ago

answare : Y,Y,Y

User1 no need change the password :
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-faq#does-azure-ad-
password-protection-validate-existing-passwords-after-being-installed

User 2 : password is valid

User 3 : the password is audit mode.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations#audit-mod

upvoted 1 times

AGill 9 months, 1 week ago

Based on your explanation, the answer is N, Y, Y? First line asks if user 1 must change their password on sign in. But the link says it
takes effect at a password change or set operation - not sign in.

upvoted 2 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 1 times

zorro1 1 year ago

If set to Enforce, users will be prevented from setting banned passwords and the attempt will be logged. If set to Audit, the attempt wil only be logged.

upvoted 3 times

Davidchercm 1 year, 1 month ago

here is the explanation between audit mode and enforced : https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations

upvoted 2 times

Domza 1 year, 6 months ago

So, What is the question? lol

upvoted 1 times

Scooter454 1 year, 5 months ago

Audit mode is only for Active Directory accounts. It is enabled for Azure users, so User 1 and User 2 has this policy applied

upvoted 3 times

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Type	Member of
User1	User	Group1
User2	User	Group1, Group2
User3	User	Group1, Group2
User4	Guest User	Group2

User1 is the owner of Group1. User2 is the owner of Group2.

You create an access review that contains the following configurations:

- Users to review: Members of a group
- Scope: Everyone
- Group: Group1, Group2

Reviewers: Group owners -

▪

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can review access for User2.	○	○
User1 can review access for User3.	○	○
User3 can review access for User4.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can review access for User2.	●	○
User1 can review access for User3.	●	○
User3 can review access for User4.	○	●

Box 1: Yes -

User1 is the owner of Group1. User2 is in Group1 and Group2. Group owners can review access. Therefore, User1 can review User2's membership of Group1.

Box 2: Yes -

User1 is the owner of Group1. User3 is in Group1 and Group2. Group owners can review access. Therefore, User1 can review User3's membership of Group1.

Box 3: No -

Only group owners can review access. User3 is not a group owner. Therefore, User3 cannot review membership of the groups.

References:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

lucidgreen Highly Voted 1 year, 5 months ago

Group owner = Reviewer. User 3 is not a group owner, and therefor, not a reviewer.

upvoted 9 times

Moderator Most Recent 2 months ago

Still a valid question (July 30th 2022).

upvoted 1 times

Ash473 1 year, 1 month ago

in exam today

upvoted 1 times

HOTSPOT -

You need to ensure that a user named User1 can create documents by using Office Online.

Which two Microsoft Office 365 license options should you turn on for User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct section is worth one point.

Hot Area:

Answer Area

Office 365 E5

Microsoft Forms (Plan E5)	Off	On
Microsoft MyAnalytics (Full)	Off	On
Microsoft Planner	Off	On
Microsoft StaffHub	Off	On
Microsoft Stream for O365 E5 SKU	Off	On
Microsoft Teams	Off	On
Office 365 Advanced eDiscovery	Off	On
Office 365 Advanced Threat Protection (Plan 2)	Off	On
Office 365 Cloud App Security	Off	On
Office 365 Privileged Access Management	Off	On
Office 365 ProPlus	Off	On
Office Online	Off	On
Phone System	Off	On
Power BI Pro	Off	On
PowerApps for Office 365	Off	On
SharePoint Online (Plan 2)	Off	On
Skype for Business Online (Plan 2)	Off	On
Sway	Off	On
To-Do (Plan 3)	Off	On
Yammer Enterprise	Off	On

Answer Area

Correct Answer:



You need ג€Office Onlineג€ to be able to create documents by using Office Online. You also need an online location to save and store the documents. For this, you would use SharePoint online.

gbryant1 Highly Voted 1 year, 5 months ago

It's actually "Office for the web" not "Office online"

upvoted 18 times

Stiobhan Most Recent 4 months, 1 week ago

I get the whole storage thing but the question specifically states "Create a document" not "Create and store a document" Typical Microsoft, never give you the full details!!! Still love them though 😁

upvoted 4 times

TashaGirl 8 months, 3 weeks ago

Explanation is off a bit. There is a dependency in licensing. If you try to assign Office for the Web (old Office Online) this is what you get
License operation failed. Make sure that the user has necessary services before adding or removing a dependent service.
The service Office for the Web requires SharePoint (Plan 2) to be enabled as well.

upvoted 4 times

MDol 8 months, 3 weeks ago

Answers are correct. You need the have a storage location for the documents, otherwise you can't create a new document.

upvoted 4 times

Wojer 9 months, 1 week ago

can create documents online that's the question.
in my opinion, you need only an office for the web for that

upvoted 1 times

Minniebeast 11 months ago

why is share point needed

upvoted 2 times

JEricThomas610 10 months ago

According to the explanation, you need a place to store the documents online. Kind of a tricky question.

upvoted 4 times

Your network contains two on-premises Active Directory forests named contoso.com and fabrikam.com. Fabrikam.com contains one domain and five domain controllers. Contoso.com contains the domains shown in the following table.

Name	Number of domain controllers
Contoso.com	2
East.contoso.com	3
West.contoso.com	3

You need to sync all the users from both the forests to a single Azure Active Directory (Azure AD) tenant by using Azure AD Connect.
What is the minimum number of Azure AD Connect sync servers required?

A. 1

B. 2

C. 3

D. 4

Correct Answer: *A*
You can have only one active Azure AD Connect server synchronizing accounts to a single Azure Active Directory (Azure AD) tenant. You can have 'backup'
Azure AD Connect servers, but these must be running in 'staging' mode. Staging mode means the Azure AD Connect instance is not actively synchronizing users but is ready to be bought online if the active Azure AD Connect instance goes offline.
When you have multiple forests, all forests must be reachable by a single Azure AD Connect sync server. The server must be joined to a domain. If necessary, to reach all forests, you can place the server in a perimeter network (also known as DMZ, demilitarized zone, and screened subnet).
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-forests-single-azure-ad-tenant

lucidgreen Highly Voted 1 year, 5 months ago
You can only use one at a time as an active Azure AD Connect server. The rest have to be in standby.
upvoted 22 times

lucidgreen 1 year, 5 months ago
And by standby, I mean staging mode.
upvoted 23 times

Cheekypoo Most Recent 2 months ago
Was in my exam today 05/08/22.
upvoted 1 times

Sh1rub10 4 months, 2 weeks ago
Selected Answer: A
Agreed with lucidgreen. You can only use one at a time as an active Azure AD Connect server
upvoted 3 times

HOTSPOT -

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

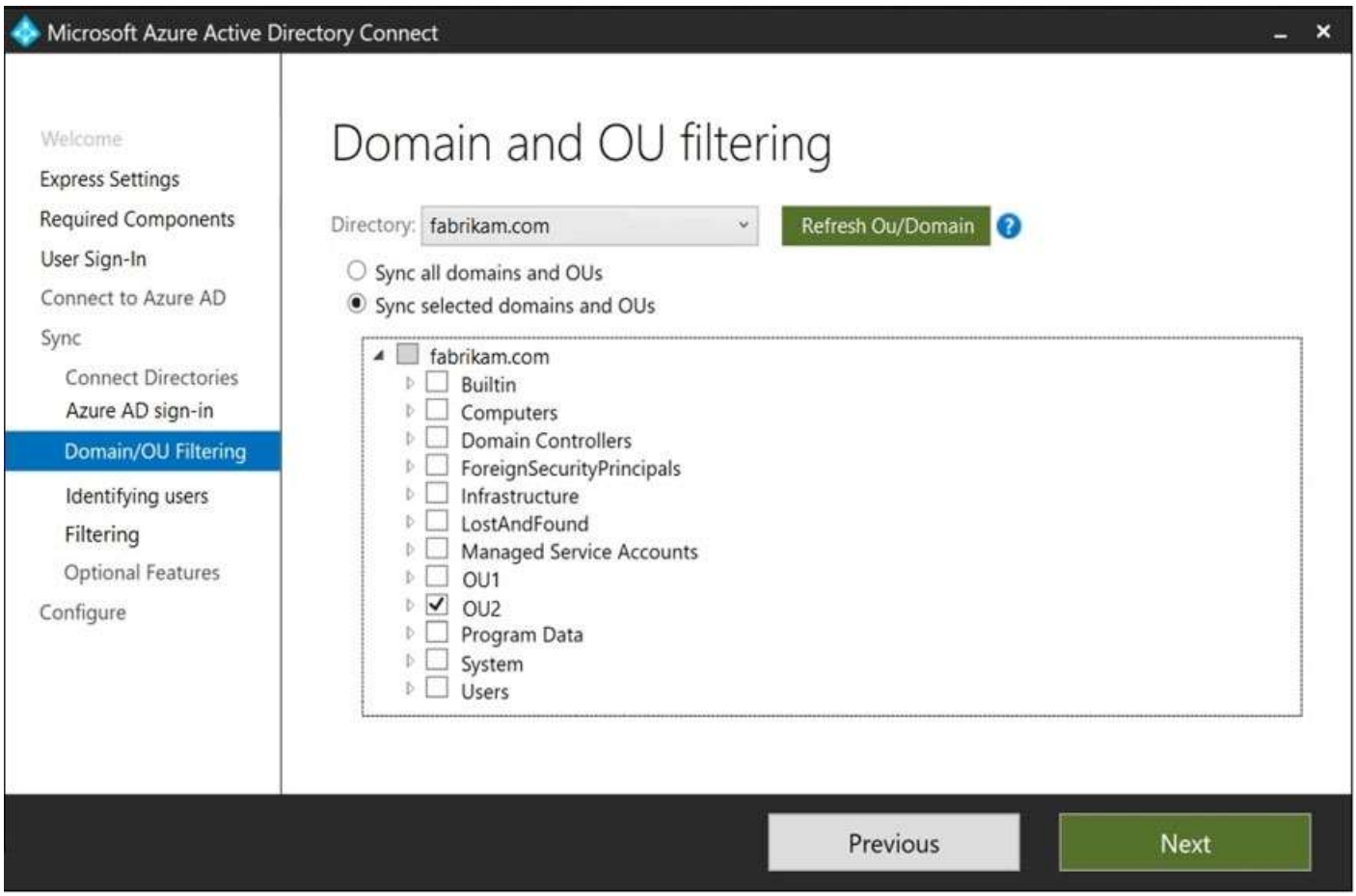
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group – Global	OU1
User3	User	OU2
Group2	Security Group – Global	OU2

The groups have the members shown in the following table.

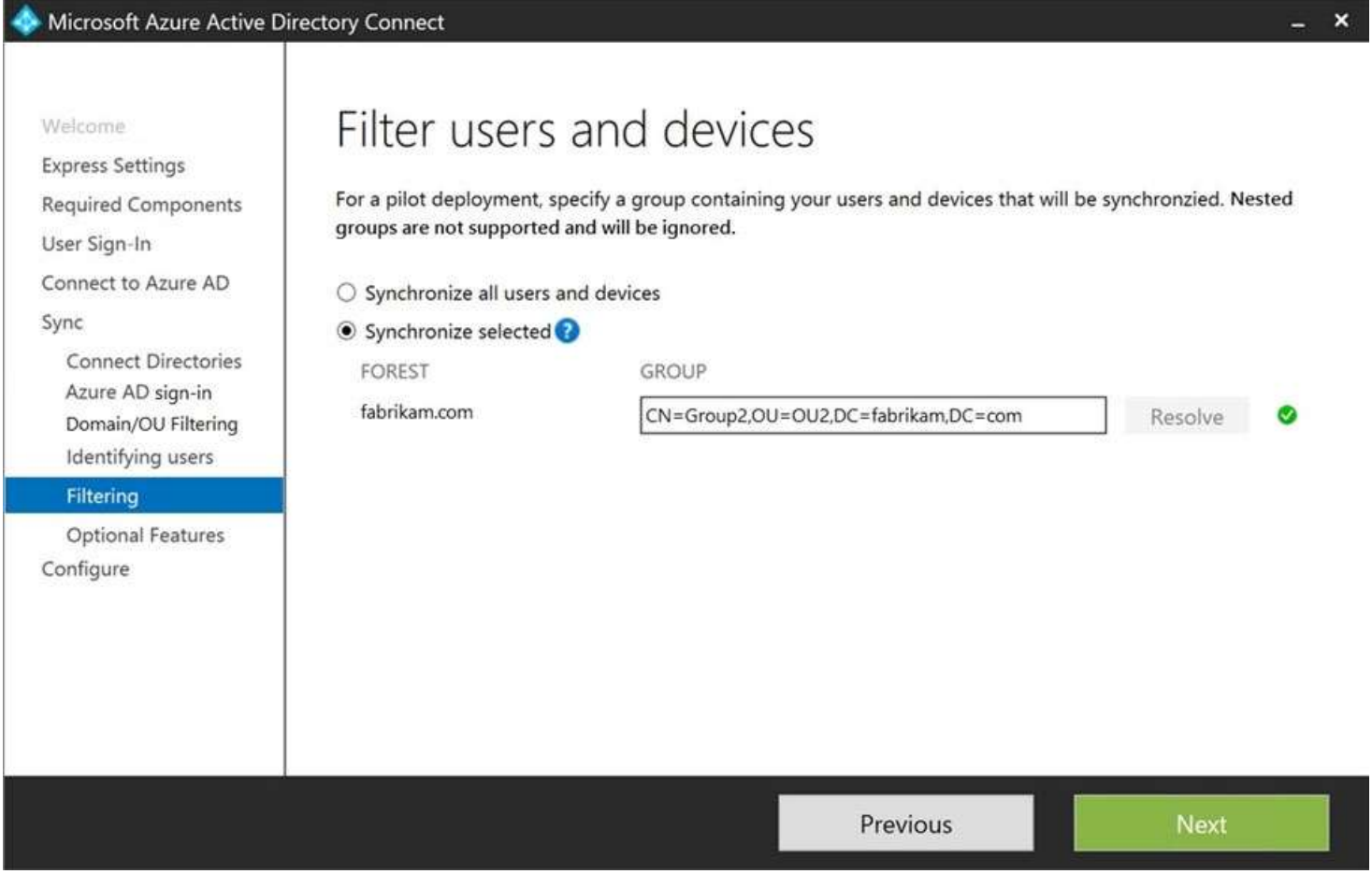
Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and a Microsoft Azure Active Directory (Azure AD) tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit.



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	○	○
Group2 will synchronize to Azure AD.	○	○
User3 will synchronize to Azure Ad.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	○	●
Group2 will synchronize to Azure AD.	●	○
User3 will synchronize to Azure Ad.	●	○

Box 1: No -

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.

User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.

Box 2: Yes -

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes -

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

References:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-based-filtering

Wearsy Highly Voted 1 year, 5 months ago

OU filtering is evaluated before group based filtering, therefore user2 not being synced is correct:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom#sync-filtering-based-on-groups

upvoted 10 times

RenegadeOrange 2 months ago

User 2 is not synced because it's not in an OU that is synced.
User 3 is synced because it is in both a synced OU and Group.
Tested this and confirmed if the user is not in a synced OU they are not synced even if in a group.

upvoted 1 times

Cheekypoo Most Recent 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Nilz76 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 4 times

fofo1960 9 months, 1 week ago

The relation is AND, so the member should be in the OU AND in the filter apply to the user.

upvoted 3 times

stoneface 9 months, 3 weeks ago

i thought that security groups are not syncronized...

upvoted 1 times

PDR 9 months, 1 week ago

security groups are synced from AD to AAD , but group writeback does not support security or distribution groups, only 365 groups from AAD to AD, which is where your confusion might have come from

upvoted 12 times

Jeff8989 8 months, 4 weeks ago

Thanks!

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 1 times

gonick 1 year ago

In exam last week

upvoted 3 times

HOTSPOT -

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the users shown in the following table.

Name	Domain	User UPN suffix
User1	Contoso.com	Fabrikam.com
User2	East.contoso.com	Contoso.com

You create an Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com.

You plan to sync the users in the forest to fabrikam.onmicrosoft.com by using Azure AD Connect.

Which username will be assigned to User1 and User2 in Azure AD after the synchronization? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1: ▼
- User1@contoso.com
- User1@east.contoso.com
- User1@fabrikam.com
- User1@fabrikam.onmicrosoft.com

User2: ▼
- User2@contoso.com
- User2@east.contoso.com
- User2@fabrikam.com
- User2@fabrikam.onmicrosoft.com

Correct Answer:

Answer Area

User1: ▼
- User1@contoso.com
- User1@east.contoso.com
- User1@fabrikam.com
- User1@fabrikam.onmicrosoft.com ✓

User2: ▼
- User2@contoso.com
- User2@east.contoso.com
- User2@fabrikam.com
- User2@fabrikam.onmicrosoft.com ✓

If you added the contoso.com and east.contoso.com domains as custom domains in Microsoft 365, then the users would be assigned their user principle names as Microsoft 365 usernames.

However, the question does not state that you have added the domains as custom domains. Therefore, both users will use the default @fabrikam.onmicrosoft.com domain for their usernames.

Madball Highly Voted 1 year, 1 month ago

Trick question, it doesn't mention adding a custom domain to the tenant, so the user accounts will be using the default domain name.

upvoted 14 times

manis73 Highly Voted 3 months, 2 weeks ago

Terrible question

upvoted 6 times

Jo696 Most Recent 3 months, 4 weeks ago

Key is in the wording, as soon as I read this I noted in the question no mention of any other domain other than fabrican being added, answer is correct.

upvoted 2 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 3 times

emolnes85 1 year, 2 months ago

Trick question

upvoted 4 times

Your network contains an Active Directory domain named adatum.com that is synced to Microsoft Azure Active Directory (Azure AD).
The domain contains 100 user accounts.
The city attribute for all the users is set to the city where the user resides.
You need to modify the value of the city attribute to the three-letter airport code of each city.
What should you do?

A. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.

B. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.

C. From Azure Cloud Shell, run the Get-MsolUser and Set-MSOluser cmdlets.

D. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.

Correct Answer: *A*
The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.
You can modify certain attributes of multiple user accounts simultaneously by selecting them in Active Directory Administrative Center or Active Directory Users and Computers, right clicking then selecting Properties.
The other three options all suggest modifying the city attribute of the users in the Azure Active Directory which is incorrect.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
Other incorrect answer options you may see on the exam include the following:
1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.
3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
Reference:
https://blogs.technet.microsoft.com/canitpro/2015/11/25/step-by-step-managing-multiple-user-accounts-via-active-directory-admin-center/

AlfredHK Highly Voted 2 years, 6 months ago
It is because the user was synced from on-premise domain, we need to modify the user attribute at on-premise domain.
upvoted 24 times

ctfalci Highly Voted 2 years, 2 months ago
The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.
You can modify certain attributes of multiple user accounts simultaneously by selecting them in Active Directory Administrative Center or Active Directory Users and Computers, right clicking then selecting Properties.
The other three options all suggest modifying the city attribute of the users in the Azure Active Directory which is incorrect.
Reference:
https://blogs.technet.microsoft.com/canitpro/2015/11/25/step-by-step-managing-multiple-useraccounts-via-activ
upvoted 10 times

ctfalci 2 years, 2 months ago
Answer A
upvoted 7 times

donathon 2 years ago
The user writeback preview feature was removed in the August 2015 update to Azure AD Connect. If you have enabled it, then yo should disable this feature. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-preview
upvoted 2 times

Cebsiej_28 Most Recent 1 month, 2 weeks ago

There are several versions of this question in the exam. The question has two possible correct answers:
1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
Other incorrect answer options you may see on the exam include the following:
1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.
3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser?view=win10-ps
upvoted 2 times

Cheekypoo 2 months ago
Was in my exam today 05/08/22.
upvoted 1 times

Rudelke 2 months, 4 weeks ago
Selected Answer: A
While I vote A I'd rather use D.

I get what they are asking for and why D is incorrect (azure commands from local domain) but there is nothing preventing you from us
Azure PS module on domain controller.
upvoted 2 times

TechMinerUK 3 months, 3 weeks ago
Selected Answer: A
A is correct as it is using Active Directory Administrative Center as whilst Powershell could also be used the commands specified in D ar
"Get-AzureADUser and Set-AzureADUser cmdlets" which will not work for administrating an on-prem AD
upvoted 1 times

charat 4 months, 1 week ago
On Exam 05/22/22. Great qustion.
upvoted 2 times

jill44 9 months ago
A&D both are correct, but for 100 users I go with D.
upvoted 1 times

Ibraheem 5 months, 2 weeks ago
I don't think D is correct, the command has GetAzureADuser which is a Cloud command and since the users are Synced users, the ri
command would have been GetADuser for on-premises.
upvoted 2 times

tf444 9 months, 1 week ago
A&C both are correct, however, for 100 users, C is more reasonable!
upvoted 1 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 3 times

lucidgreen 1 year, 6 months ago
B and C are targeting the wrong system. These are synced users (unless you use writeback).
D uses the wrong command on a domain controller, unless you load the right module.
A is the right console for the system. It will get the job done.
upvoted 8 times

Razuli 1 year, 5 months ago
always appreciate your comments lucidgreen
upvoted 3 times

lucidgreen 1 year, 7 months ago
It's A because the other answers are all Azure answers and they would get the job done for Azure users, but since they are synced, it's l
to do it from the AD side, unless right-back is enabled.
But still, one of these things is not like the others... That kind of helps to whittle it down.
upvoted 2 times

mkoprivnj 1 year, 9 months ago
A for sure!
upvoted 4 times

mikerss 2 years, 4 months ago

probably D would be a better option since the question specifies that 'all' 100 users need to have the change.

upvoted 5 times

pukke 2 years, 4 months ago

Not D. unless it says Get-ADuser and Set-ADuser rather than Get-AzureADUser & Set-AzureADuser. You need to modify on-premises accounts!

upvoted 10 times

Jokke71 2 years, 6 months ago

Is A correct ? Why is C not a correct answer ?

upvoted 4 times

Question #50 *Topic 3*

Your company has 10,000 users who access all applications from an on-premises data center.
You plan to create a Microsoft 365 subscription and to migrate data to the cloud.
You plan to implement directory synchronization.
User accounts and group accounts must sync to Microsoft Azure Active Directory (Azure AD) successfully.
You discover that several user accounts fail to sync to Azure AD.
You need to resolve the issue as quickly as possible.
What should you do?

A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.

B. Run idfix.exe, and then click Complete.

C. From Windows PowerShell, run the Start-AdSyncCycle ג€"PolicyType Delta command.

D. Run idfix.exe, and then click Edit.

Correct Answer: *D*
IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix

Davidchercm 8 months, 3 weeks ago
Selected Answer: D
D is correct
upvoted 3 times

jkklim 9 months, 3 weeks ago
https://microsoft.github.io/idfix/Step%203%20-%20Query%20and%20fix%20invalid%20attributes/

Answer is D - EDIT to fix it. COMPLETE means take in the error
upvoted 2 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 1 times

densyo 1 year, 3 months ago
https://answers.microsoft.com/en-us/msoffice/forum/msoffice_o365admin-mso_dirservices/directory-synchronization-part-2-using-idf
to/6f09c9d7-8b6e-4d6b-aa0c-630dd2904460
upvoted 2 times

adaniel89 1 year, 4 months ago
You need to ensure the UPN of the users AD accounts are correct. i.e not .local UPN.
upvoted 1 times

chaoscreater 1 year, 3 months ago
FALSE. UPN doesn't matter here. Users will just get @tenant.onmicrosoft.com, where tenant is whatever your tenant name is during the initial O365 tenant setup. I have seen multiple tenants with synced accounts using @tenant.onmicrosoft.com and their onprem UPN is using an internal domain, such as .local. Question is talking about sync issues and UPN does not contribute to a sync issue. S issues are 99% related to attributes.
upvoted 11 times

PDR 9 months, 1 week ago
chaoscreater is correct - just to add a possible issue would be if the usernames in AD have a space in them , which AD supports b AAD does not and would cause them to fail to sync. IDfix can resolve this for you
upvoted 3 times

Question #51 *Topic 3*

Your network contains an Active Directory forest. The forest contains two domains named contoso.com and adatum.com.
Your company recently purchased a Microsoft 365 subscription.
You deploy a federated identity solution to the environment.
You use the following command to configure contoso.com for federation.
Convert-MsolDomaintoFederated `"DomainName contoso.com
In the Microsoft 365 tenant, an administrator adds and verifies the adatum.com domain name.
You need to configure the adatum.com Active Directory domain for federated authentication.
Which two actions should you perform before you run the Azure AD Connect wizard? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Windows PowerShell, run the Convert-MsolDomaintoFederated ‚€"DomainName contoso.com ‚€"SupportMultipleDomain command.

B. From Windows PowerShell, run the New-MsolFederatedDomain ‚€"SupportMultipleDomain -DomainName contoso.com command.

C. From Windows PowerShell, run the New-MsolFederatedDomain -DomainName adatum.com command.

D. From Windows PowerShell, run the Update-MSOLFederatedDomain ‚€"DomainName contoso.com ‚€"SupportMultipleDomain command.

E. From the federation server, remove the Microsoft Office 365 relying party trust.

Correct Answer: *AE*
When the Convert-MsolDomaintoFederated ‚€"DomainName contoso.com command was run, a relying party trust was created.
Adding a second domain (adatum.com in this case) will only work if the SupportMultipleDomain switch was used when the initial federation was configured by running the Convert-MsolDomaintoFederated ‚€"DomainName contoso.com command.
Therefore, we need to start again by removing the relying party trust then running the Convert-MsolDomaintoFederated command again with the SupportMultipleDomain switch.

lucidgreen Highly Voted 1 year, 5 months ago
Convert-MsolDomaintoFederated is for changing the configuration to federated. Update-MsolDomaintoFederated is for making chang
I'm going say D and E.
upvoted 22 times

michszym 1 year, 3 months ago
Agree, read this: https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/hybrid/how-to-connect-install-multiple-domains.md - section "How to update the trust between AD FS and Azure AD" - Remove " Relying Party Trusts" and next Update-MSOLFederatedDomain -DomainName <Federated Domain Name> -SupportMultipleDomain, NOT Convert-MsolDomaintoFederated
upvoted 3 times

ItsMagige Highly Voted 1 year, 3 months ago
D and E
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365
upvoted 6 times

trexar Most Recent 7 months ago
Selected Answer: AE
I recheck and is posible to use:
1.Update-MSOLFederatedDomain -DomainName <Federated Domain Name> -supportmultipledomain
and
2.New-MSOLFederatedDomain -domainname <domain name> -supportmultipledomain
or
Convert-MSOLDomainToFederated -domainname <domain name> -supportmultipledomain

https://docs.microsoft.com/en-US/troubleshoot/azure/active-directory/federation-service-identifier-specified
upvoted 2 times

RenegadeOrange 2 months ago
D & E
Explained exactly in this article.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-multiple-domains

upvoted 1 times

trexar 7 months ago

Selected Answer: DE

To resolve the issue, you must use the -supportmultipledomain switch to add or convert every domain that's federated by the cloud service. This includes federated domains that already exist.

Stee1 and 2: Download the agent and test the update command to check is ok
Step 3: Update the federated trust on the AD FS server
Update-MSOLFederatedDomain -DomainName <Federated Domain Name> -supportmultipledomain
Step 4: Use the -supportmultipledomain switch to add or convert additional federated domains
New-MSOLFederatedDomain -domainname <domain name> -supportmultipledomain

upvoted 2 times

RazielLycas 7 months, 2 weeks ago

Selected Answer: DE

similar question in Measureup.com , DE because the federated domain already exist you gonna update it, before run the wizard you ha to remove the Office365 object from ADFS

upvoted 2 times

JohnHr 8 months ago

Selected Answer: DE

similar question in Measureup.com , D& E were the answer

upvoted 1 times

joergsi 8 months ago

Selected Answer: BD

For me
1. = D
2. = B

upvoted 1 times

joergsi 8 months ago

OK, need to correct my vote:
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365#:~:text=To%20do%20this%2C%20click%20Start,Office%20365%20Identity%20Platform%20entry.

Log on to the AD FS server. To do this, click Start, point to All Programs, point to Administrative Tools, and then click AD FS (2.0) Management.
In the left navigation pane, click AD FS (2.0), click Trust Relationships, and then click Relying Party Trusts.
In the rightmost pane, delete the Microsoft Office 365 Identity Platform entry.

In the Windows PowerShell window that you opened in step 1, re-create the deleted trust object. To do this, run the following command, and then press Enter:
Update-MSOLFederatedDomain –DomainName: <Federated Domain Name> –supportmultipledomain

So it would be, in the correct order: E then D!

upvoted 1 times

Glorence 8 months, 2 weeks ago

Selected Answer: DE

D and E for sure!
Check out this link https://docs.microsoft.com/en-US/troubleshoot/azure/active-directory/federation-service-identifier-specified

upvoted 1 times

joergsi 8 months, 1 week ago

Thank you for the link.
If you check the commands you will find:
Steps:
1. Update-MSOLFederatedDomain -DomainName <Federated Domain Name> -supportmultipledomain
2. New-MSOLFederatedDomain -domainname <domain name> -supportmultipledomain

For me
1. = D
2. = B

upvoted 1 times

kanag1 8 months, 3 weeks ago

Selected Answer: DE

According the link below, the right answers are : Step "E" first and then "D".
1. Remove the "Relying Party Trusts"
2. Update-MsolFederatedDomain -DomainName contoso.com -SupportMultipleDomain
3. New-MsolFederatedDomain –SupportMultipleDomain –DomainName <Newdomainname>

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-multiple-domains
upvoted 2 times

fofo1960 8 months, 3 weeks ago

Selected Answer: DE
Agree with Lucidgreen
upvoted 2 times

FumerLaMoquette 9 months ago

Selected Answer: CE
I'm with the minority on this. It has to be C and E, because in the text, it described that adatum.com was added after federation.

I believe we need to then add a new msol federation for adatum.com.
upvoted 2 times

Aesam 1 year ago

D & E for sure, below link gives exact steps for scenario in question.
https://docs.microsoft.com/en-US/troubleshoot/azure/active-directory/federation-service-identifier-specified
upvoted 4 times

Linux09 1 year ago

A+E is correct. "The Convert-MSOLDomainToFederated cmdlet converts the specified domain from standard authentication to single sign on. This includes configuring the relying party trust settings between the Active Directory Federation Services 2.0 server and Microsoft Online. Single sign-on is also known as identity federation."

https://docs.microsoft.com/en-us/powershell/module/msonline/convert-msoldomaintofederated?view=azureadps-1.0
upvoted 1 times

fko1978 1 year, 1 month ago

difference convert or update-msoldomaintofederated explained https://docs.microsoft.com/en-us/powershell/module/msonline/convert-msoldomaintofederated?view=azureadps-1.0
upvoted 1 times

lengySK 1 year, 1 month ago

I think D E
upvoted 1 times

venwaik 1 year, 2 months ago

It is D & E for sure, because the question states that the Convert-MsolDomainToFederated is already executed. Therefore we need the update command to change the MsolFederatedDomain.
So D & E is my choice here.
upvoted 1 times

F_M 1 year, 4 months ago

It's D and E!
It's true you have to remove the federation trust but once did that the right command to use is Update-MSOLFederatedDomain!
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-multiple-domains#how-to-update-the-trust-between-ad-fs-and-azure-ad
upvoted 4 times

You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. The tenant includes a user named
User1.
You enable Azure AD Identity Protection.
You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.
To which role should you add User1?

A. Compliance administrator

B. Global administrator

C. Owner

D. Security administrator

Correct Answer: *D*
Either one of the following three roles can review the list in Azure AD Identity Protection of users flagged for risk:
- Security Administrator
- Global Administrator
- Security Reader

Using the principle of least privilege, we should add User1 to the Security Administrator role.
Note:
There are several versions of this question in the exam. The question has three possible correct answers:
1. Security Reader
2. Security Administrator

Global Administrator -
Other incorrect answer options you may see on the exam include the following:
1. Service Administrator.
2. Reports Reader
3. User Administrator

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins

melatocaroca Highly Voted 1 year, 3 months ago
Using the principle of least privilege, we should add User1 to the Security Administrator role.
Security administrator Can read security information and reports and manage configuration in Azure AD and Office 365.
Compliance administrator Can read and manage compliance configuration and reports in Azure AD and Microsoft 365.
Global administrator Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities. No match principle of lea
privilege
Owner SharePoint related
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
upvoted 8 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You need to modify Christie Cline to meet the following requirements:
- Christie Cline must be able to view the service dashboard and the Microsoft Office 365 Message center.
- Christie Cline must be able to create Microsoft support requests.
- The solution must use the principle of least privilege.

Correct Answer: *See explanation below.*
You need to assign Christie the 'Service Support Admin' role.
1. In the Microsoft 365 Admin Center, click 'Roles'.
2. Scroll down to the Service Support Admin role and click on the role name.
3. Click the 'Assigned Admins' link.
4. Click the 'Add' button.
5. Start typing the name Christie then select her account when it appears.
6. Click Save.
References:
https://docs.microsoft.com/en-US/azure/active-directory/users-groups-roles/directory-assign-admin-roles

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
Your organization has an office in Seattle.
You plan to create 100 users who will work in the Seattle office. The city attribute for all the users will be Seattle.
You need to create a group named Group1 that will automatically contain all the Seattle office users.

Correct Answer: *See explanation below.*
You need to create a Dynamic group. User accounts with the city attribute set to 'Seattle' will automatically be added to the group.
1. Go to the Azure Active Directory admin center.
2. Select Azure Active Directory then select Groups.
3. Click on the New Group link.
4. Give the group a name such as Seattle Users.
5. Select Users as the membership type.
6. Select 'Add dynamic query'.
7. Select 'City' in the Property drop-down box.
8. Select 'Equals' in the Operator drop-down box.
9. Enter Seattle as the Value. You should see the following text in the Expression box: user.city -eq "Seattle"
10. Click Save to create the group.
References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
A user named Johanna Lorenz recently left the company. A new employee named Ben Smith will handle the tasks of Johanna Lorenz.
You need to create a user named Ben Smith. Ben Smith must be able to sign in to http://myapps.microsoft.com and open Microsoft Word Online.

Correct Answer: *See explanation below.*
You need to create a user account and assign a license to the account. You then
To create the user account and mailbox:
1. In the Microsoft 365 admin center, go to User management, and select Add user.
2. Enter the name Ben Smith in the First Name and Last Name fields.
3. Enter Ben.Smith in the username field and click Next.
4. Assign a Microsoft 365 license to the account.
5. Click Next.
6. Click Next again.
7. Click 'Finish adding'.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You hire a new Microsoft 365 administrator named Nestor Wilke. Nestor Wilke will begin working for your organization in several days.
You need to ensure that Nestor Wilke is prevented from using his account until he begins working.

Correct Answer: *See explanation below.*
You need to sign-in status for the account to 'Blocked'. Blocking doesn't stop the account from receiving email and it doesn't delete any data.
1. On the home page of the Microsoft 365 admin center, type the user's name into the Search box.
2. Select the Nestor Wilke account in the search results.
3. In the 'Sign-in status' section of the account properties, click the Edit link.
4. Select 'Block the user from signing in' and click the Save button.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You need to create a group named Group2. Users who are added to Group2 must be licensed automatically for Microsoft Offline 365.

Correct Answer: *See explanation below.*
You need to create the group and assign a license to the group. Anyone who is added to the group will automatically be assigned the license that is assigned to the group.
1. Go to the Azure Active Directory admin center.
2. Select the Azure Active Directory link then select Groups.
3. Click the New Group link.
4. Select 'Security' as the group type and enter 'Group2' for the group name.
5. Click the Create button to create the group.
6. Back in the Groups list, select Group2 to open the properties page for the group.
7. Select 'Licenses'.
8. Select the '+ Assignments' link.
9. Tick the box to select the license.
10. Click the Save button to save the changes.
References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You have a user named Grady Archie. The solution must meet the following requirements:
- Grady Archie must be able to add payment methods to your Microsoft Office 365 tenant.
- The solution must minimize the number of licenses assigned to users.
- The solution must use the principle of least privilege.

Correct Answer: *See explanation below.*
You need to assign the 'Billing Administrator' role to Grady Archie.
1. Go to the Azure Active Directory admin center.
2. Select Users.
3. Select the Grady Archie account to open the account properties page.
4. Select 'Assigned roles'.
5. Click the 'Add Assignments' button.
6. Select Billing Administrator then click the Add button.

Reference:
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
Your organization plans to open an office in New York, and then to add 100 users to the office. The city attribute for all new users will be New York.
You need to ensure that all the new users in the New York office are licensed for Microsoft Office 365 automatically.

Correct Answer: *See explanation below.*
You need create a dynamic group based on the city attribute. You then need to assign a license to the group. User accounts with the city attribute set to 'New
York will automatically be added to the group. Anyone who is added to the group will automatically be assigned the license that is assigned to the group.
1. Go to the Azure Active Directory admin center.
2. Select Azure Active Directory then select Groups.
3. Click on the New Group link.
4. Give the group a name such as New York Users.
5. Select Users as the membership type.
6. Select 'Add dynamic query'.
7. Select 'City' in the Property drop-down box.
8. Select 'Equals' in the Operator drop-down box.
9. Enter 'New York' as the Value. You should see the following text in the Expression box: user.city -eq "New York"
10. Click Save to create the group.
11. In the Groups list, select the new group to open the properties page for the group.
12. Select 'Licenses'.
13. Select the '+ Assignments' link.
14. Tick the box to select the license.
15. Click the Save button to save the changes.

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

Question #60 *Topic 3*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
Alex Wilber must be able to reset the password of each user in your organization. The solution must prevent Alex Wilber from modifying the password of global administrators.

Correct Answer: *See explanation below.*
You need to assign the 'Password Administrator' role to Alex Wilber. A user assigned the Password Administrator role can reset passwords for non-administrators and Password administrators.
1. Go to the Azure Active Directory admin center.
2. Select Users.
3. Select the Alex Wilber account to open the account properties page.
4. Select 'Assigned roles'.
5. Click the 'Add Assignments' button.
6. Select Password Administrator then click the Add button.
References:
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You plan to migrate data from an on-premises email system to your Microsoft 365 tenant.
You need to ensure that Debra Berger can import a PST file.

Correct Answer: *See explanation below.*
Debra will need the Mailbox Import Export and Mail Recipients roles to be able to import PST files. These roles cannot be assigned directly to a user account. The way to assign just those two roles to a user is to create a new role group, assign the roles to the role group and add the user as a member.
1. Go to the Exchange admin center.
2. Select Permissions.
3. In the Admin roles section, click the plus (+) sign to create a new role.
4. Give the role group a name such as PST Import.
5. In the roles section, click the plus (+) sign.
6. Select the Mailbox Import Export and Mail Recipients roles and click Add to add the roles.
7. In the Members section, click the plus (+) sign.
8. Select Debra Berger then click Add then Ok to add Debra as a member of the new role group.
9. Click the Save button to save the new role group.

HOTSPOT -

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
User1	Password administrator
User2	Security administrator
User3	User administrator
User4	*None*

You need to identify which users can perform the following administrative tasks:

- Reset the password of User4.
- Modify the value for the manager attribute of User4.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Reset the password of User4: [▼]
- User1 only
- User2 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3

Modify the value for the manager attribute of User4: [▼]
- User2 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Correct Answer:

Answer Area

Reset the password of User4: [▼]
- User1 only
- User2 only
- User1 and User2 only
- **User1 and User3 only**
- User1, User2, and User3

Modify the value for the manager attribute of User4: [▼]
- User2 only
- **User3 only**
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Box 1:

A Password Administrator or a User Administrator can reset the password non-administrative users.

Box 2: A User Administrator can configure other attributes such as the Manager attribute of non-administrative users.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

Cheekypoo 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Moderator 3 months, 2 weeks ago

Correct answers given.

upvoted 1 times

itmaster 6 months ago

I have tested to create a guest user from Azure AD portal with a user with "sec admin" role, I found create user is grayed out and only invite user is there. The provided answer is correct, only "user admin" can create guest users. Referecne: https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal#:~:text=A%20role%20that%20allows%20you%20to%20create%20users%20in%20your%20tenant%20directory%2C%20like%20the%20Global%20Administrator%20role%20or%20any%20of%20the%20limited%20administrator%20directory%20roles%20such%20as%20guest%20inviter%20or%20user%20administrator

upvoted 1 times

itmaster 6 months ago

sorry this comment is for Q62 not for this Question

upvoted 1 times

trexar 6 months ago

Attribute Definition Administrator (It is not an option)
Users with this role can define a valid set of custom security attributes that can be assigned to supported Azure AD objects. This role can also activate and deactivate custom security attributes https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#attribute-definition-administrator

upvoted 1 times

trexar 6 months ago

By default, Global Administrator and other administrator roles do not have permissions to read, define, or assign custom security attributes.

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 3 times

M19 1 year ago

Reset the password of user 4 : User 1 and User 3.
Link - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-reset-password-azure-portal

upvoted 1 times

Ash473 1 year, 1 month ago

IN exam today

upvoted 1 times

itstudy369 1 year, 3 months ago

Password Administrator CAN'T modify user attribute fields

upvoted 1 times

itstudy369 1 year, 3 months ago

Reset password only user1

upvoted 1 times

itstudy369 1 year, 3 months ago

Sorry, reset password user 1 and 3.

upvoted 3 times

melatocaroca 1 year, 4 months ago

Security Administrator can not reset user passwords
Users with this role have permissions to manage security-related features in the Microsoft 365 security center, Azure Active Directory Identity Protection, Azure Active Directory Authentication, Azure Information Protection, and Office 365 Security & Compliance Center. More information about Office 365 permissions is available at Permissions in the Security & Compliance Center.

Password Administrator Can reset passwords for non-administrators and Password Administrators.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

upvoted 3 times

melatocaroca 1 year, 3 months ago

additional

Box 1: User 1 and user 3
Password Administrator Can reset passwords for non-administrators and Password Administrators. User Administrator Can manage aspects of users and groups, including resetting passwords for limited admins users.

Box 2: User 3, User Administrator Can manage all aspects of users and groups, including resetting passwords for limited admins us
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

upvoted 5 times

HOTSPOT -

Your company has offices in several cities and 100,000 users.

The network contains an Active Directory domain named contoso.com.

You purchase Microsoft 365 and plan to deploy several Microsoft 365 services.

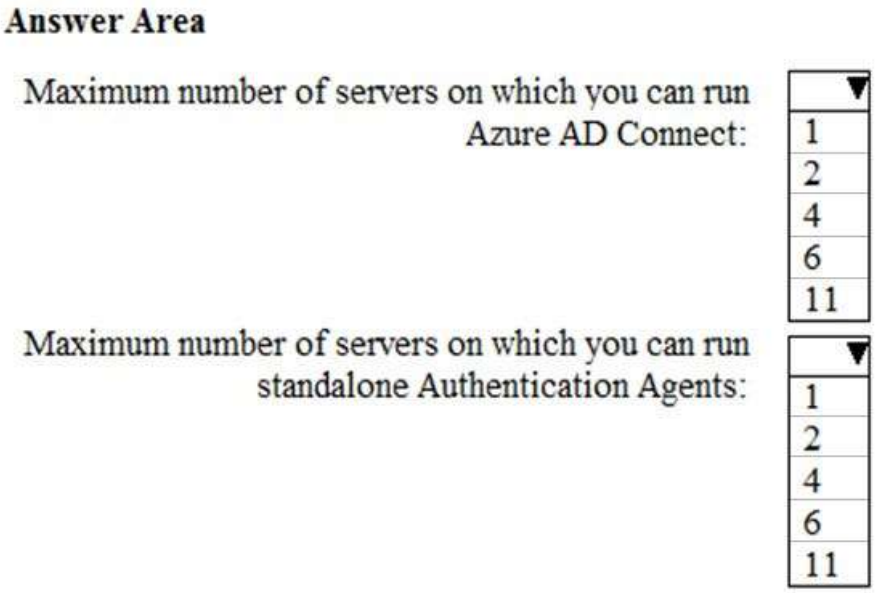
You are evaluating the implementation of pass-through authentication and seamless SSO. Azure AD Connect will NOT be in staging mode.

You need to identify the redundancy limits for the planned implementation.

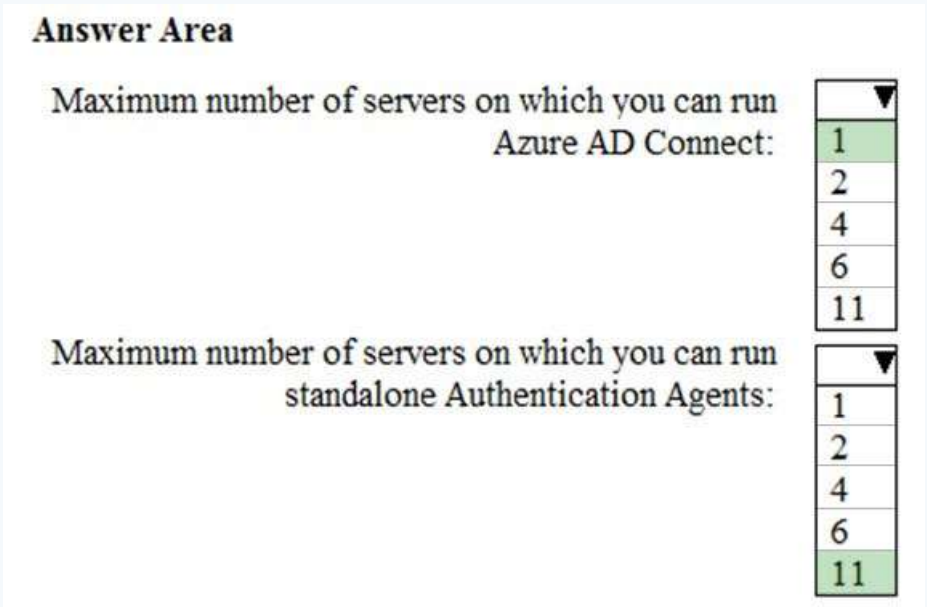
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.

Azure authentication agents can be installed on as many servers as you like.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

MartinSt Highly Voted 2 years, 10 months ago

In production environments, we recommend that you have a minimum of 3 Authentication Agents running on your tenant. There is a system limit of 40 Authentication Agents per tenant.
see https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

upvoted 14 times

lucidgreen 1 year, 5 months ago

I think we're overthinking this one. Only 1 agent can be installed if staging mode cannot be used. They have a requirement of NOT putting any of the Azure AD Connect servers in Staging Mode. Therefore, the answer is 1 and 1. Isn't it?

upvoted 2 times

Turak64 1 year, 1 month ago

Is an Auth Agent an Azure Connect server?

upvoted 1 times

Goofer Highly Voted 2 years, 8 months ago

One Azure AD Connect server.
Max 40 PTA servers

upvoted 11 times

Mr01z0 1 year, 4 months ago

Indeed: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start#in-your-on-premises-environment

Quote from site: "In production environments, we recommend that you have a minimum of 3 Authentication Agents running on you tenant. There is a system limit of 40 Authentication Agents per tenant."

upvoted 1 times

melatocaroca Most Recent 1 year, 3 months ago

Please may be is a good idea to include that there is a system limit of 40 Authentication Agents per tenant.

Reference
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start#step-4-ensure-high-availability

upvoted 2 times

adaniel89 1 year, 4 months ago

Azure authentication agents can be installed on as many servers as you like - Unlimited(there is no need to specify 11)

upvoted 3 times

Turak64 1 year, 1 month ago

There's a system limit of 40, but either way this is a horrible question

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

upvoted 2 times

mkoprivnj 1 year, 9 months ago

1 & 11 is correct. Only one AAD connect per server if staging not configured!

upvoted 3 times

[Removed] 2 years, 2 months ago

double question again

upvoted 2 times

Alvaroll 2 years ago

2-9 https://www.examtopics.com/exams/microsoft/ms-100/view/11/

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

- Contoso.com
- East.contoso.com

An Azure AD Connect server is deployed to contoso.com. Azure AD Connect syncs to an Azure Active Directory (Azure AD) tenant.
You deploy a new domain named west.contoso.com to the forest.
You need to ensure that west.contoso.com syncs to the Azure AD tenant.
Solution: You create an Azure DNS zone for west.contoso.com. On the on-premises DNS servers, you create a conditional forwarder for west.contoso.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Kipperson Highly Voted 1 year, 4 months ago
B - You would also need to add the custom doing in the 365 Portal
upvoted 8 times

Jo696 Most Recent 3 months, 4 weeks ago
As below, need to add the domain then set the users upn to pick up this domain

https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide
upvoted 1 times

HOTSPOT -

Your company has a Microsoft Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Role
User1	Privileged role administrator
User2	User administrator
User3	Security administrator
User4	Billing administrator

The tenant includes a security group named Admin1. Admin1 will be used to manage administrative accounts. External collaboration settings have default configuration.

You need to identify which users can perform the following administrative tasks:

- Create guest user accounts
- Add User3 to Admin1

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create guest user accounts: ▼
- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Add User3 to Admin1: ▼
- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Correct Answer:

Answer Area

Create guest user accounts: ▼
- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Add User3 to Admin1: ▼
- User4 only
- User2 only
- User3 only
- User2 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

A User Administrator is the only role listed that can create user accounts included Guest user accounts. A Global Administrator can also create user accounts.

A User Administrator is also the only role listed that can modify the group membership of users.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

kkkeji Highly Voted 1 year, 6 months ago

It is possible to create a guest user without a User Administrator.
Therefore, guest creation is possible for all users.

upvoted 7 times

adaniel89 1 year, 6 months ago

correct!

All users can create guest user accounts, so should be User 1,2.3 &4

upvoted 6 times

melatocaroca 1 year, 3 months ago

you may need to rethink about it, any Members can invite if tenant is under default settings, invite is not create
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

upvoted 5 times

J0J0 1 year, 3 months ago

But technically, once invite has been accepted it will create a guest user account. so by inviting, you can create guest account a
that is considering the default settings.

upvoted 4 times

allesglar 10 months, 4 weeks ago

exactly and this is why it is wrong. You cannot "create" the guest user to your preference, just replicate the default behavio
The answer is imo correct.

upvoted 6 times

alex_p 6 months ago

Please, explain how can you create Guest Users without inviting them?

upvoted 2 times

marckinez 1 year, 2 months ago

creating guest users and inviting guest users is not the same, I think it's not possible to create Guest users without a User Administrator

upvoted 2 times

Bobalo 1 year, 2 months ago

I would agree, but I think it's not really the same. An account with rights to create guest accounts can physically create the accounts
AzureAD, inviting just sends the create request to the AzureAD internal authority, which creates the guest user for you. the effect is
same, but the means are quite different.

upvoted 5 times

mitsios96 1 year ago

Invite is different than create

upvoted 7 times

vicentsp84 Highly Voted 1 year, 4 months ago

1,2,3 & 4, https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide default setting

upvoted 7 times

Chetithy Most Recent 1 week ago

I'm not sure how noone has referenced this: https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstar
add-guest-users-portal#add-a-new-guest-user-in-azure-ad

Add a new guest user in Azure AD:
Sign in to the Azure portal with an account that's been assigned the Global administrator, Guest, inviter, or User administrator role.

upvoted 1 times

Claire91 2 months, 2 weeks ago

The answers are correct.
Any admin can invite a gues but only the Global Admin, Guest inviter or User administrator can create a guest.

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

upvoted 2 times

Moderator 3 months, 2 weeks ago

Correct answers given.

upvoted 3 times

itmaster 6 months ago

I have tested to create a guest user from Azure AD portal with a user with "sec admin" role, I found create user is grayed out and only invite user is there. The provided answer is correct, only "user admin" can create guest users. Referecne:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal#:~:text=A%20role%20that%20allows%20you%20to%20create%20users%20in%20your%20tenant%20directory%2C%20like%20the%20Global%20Administrator%20role%20or%20any%20of%20the%20limited%20administrator%20directory%20roles%20such%20as%20guest%20inviter%20or%20user%20administrator

upvoted 2 times

Ogabs 8 months ago

"External collaboration settings have default configuration."
Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
I've tried logging in to portal.azure.com as a regular (non-admin) account, I was able to create a guest user (invite).
Users 1,2,3 & 4 can create Guest Users and only User 2 can add User 3 to Admin1.

upvoted 1 times

joergsi 8 months, 1 week ago

To cut a long story short for all the guessing and discussion about the Guest User Accounts:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

=> Prerequisites
A role that allows you to create users in your tenant directory, like the Global Administrator role or any of the limited administrator directory roles such as guest inviter or user administrator.

upvoted 2 times

Moderator 2 months ago

Correct, great link.

upvoted 1 times

tf444 9 months, 1 week ago

External collaboration settings have default configuration.
Anyone can invite guest
https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide

upvoted 1 times

tf444 9 months, 1 week ago

External Collaboration setting is set to default :
Guest invite settings Anyone in the organization can invite guest users including guests and non-admins
Enable guest self-service sign up via user flows No
Collaboration restrictions Allow invitations to be sent to any domain
1- All the users
2-User 2

upvoted 1 times

FreddyLao 10 months ago

the answer is correct. both User 2 only.
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal
Prerequisites:
To complete the scenario in this tutorial, you need:
A role that allows you to "create" users in your tenant directory, like the "Global Administrator" role or any of the limited administrator directory roles such as "guest inviter" or "user administrator".
A valid email account that you can add to your tenant directory, and that you can use to receive the test invitation email.

upvoted 2 times

suketet 10 months, 1 week ago

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

upvoted 1 times

Jcbrow27 10 months, 2 weeks ago

many people says that invite is not the same that create where is the reference ? by default all users can "invite".

upvoted 1 times

David_2211 10 months, 3 weeks ago

if any user in tenant invites guest user - guest user is created
this is default External collaboration setting! - and it's pointed out in question.
"By default, all users and guests in your directory can invite guests even if they're not assigned to an admin role." reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/delegate-invitations

upvoted 1 times

Chipper 1 year ago

If you "invite" a guest user, don't you have to create the guest user account first? So doesn't that mean "inviting" a guest user is creatin guest user?

upvoted 2 times

Chipper 1 year ago

To add to this, I should clarify. What I mean is, if you have to create the user account first to invite a guest user, it should just be Use so I agree with the answer that it is User 2 for both drop downs.

upvoted 1 times

TimurKazan 1 year, 1 month ago

i would go with user administrator (because I think invite is nit the same as create)
and I would go with all 4 (because I have tested it and any of mentione roles grants access for group management)

upvoted 1 times

TimurKazan 11 months ago

incorrect

upvoted 1 times

lengySK 1 year, 1 month ago

If they mean "invite" same as create guest user then anyone in the organization can create guest account. https://docs.microsoft.com/ us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide

upvoted 1 times

You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.
Corporate policy states that user passwords must not include the word Contoso.
What should you do to implement the corporate policy?

A. From the Azure Active Directory admin center, configure the Password protection settings.

B. From the Microsoft 365 admin center, configure the Password policy settings.

C. From Azure AD Identity Protection, configure a sign-in risk policy.

D. From the Azure Active Directory admin center, create a conditional access policy.

Correct Answer: *A*
The Password protection settings allows you to specify a banned password list of phrases that users cannot use as part of their passwords.
References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-configure https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#custom-banned-password-list

james1 Highly Voted 1 year, 7 months ago
Yep A for sure
upvoted 8 times

trexar Most Recent 6 months, 4 weeks ago
Selected Answer: A
Yes. A
upvoted 1 times

joergsi 8 months, 1 week ago
Answer (A):
AZURE AD => Security => Authentication Methods | Policies => Password Protection => Custom banned password list
upvoted 3 times

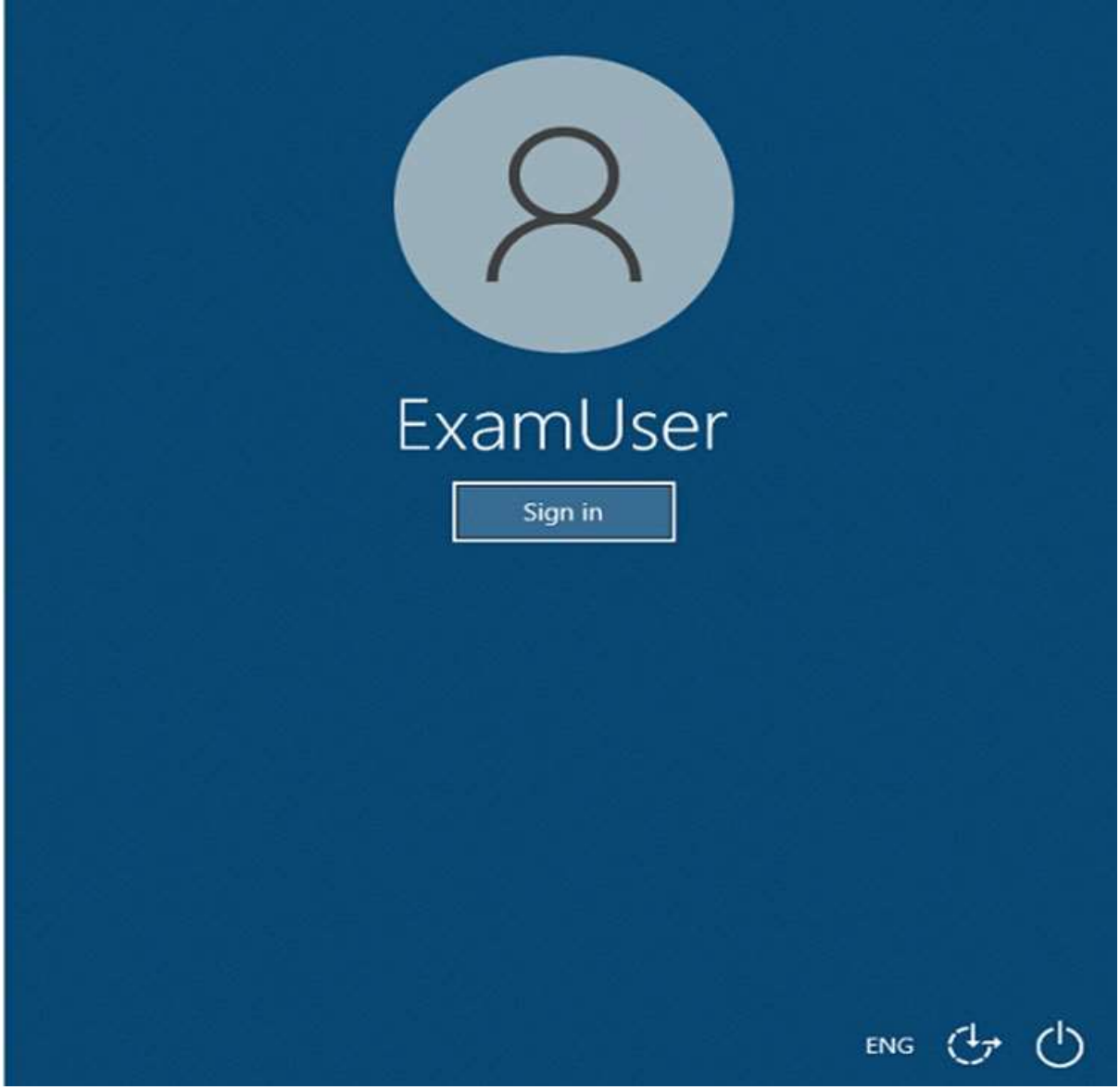
DaBummer 1 year ago
it is A!
upvoted 2 times

Ahema 1 year, 1 month ago
Correct answer
upvoted 1 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You recently discovered that several users in your organization have permissions on the mailbox of another user in the organization.

You need to ensure that Lee Gu receives a notification when a user is granted permissions on another user's mailbox.

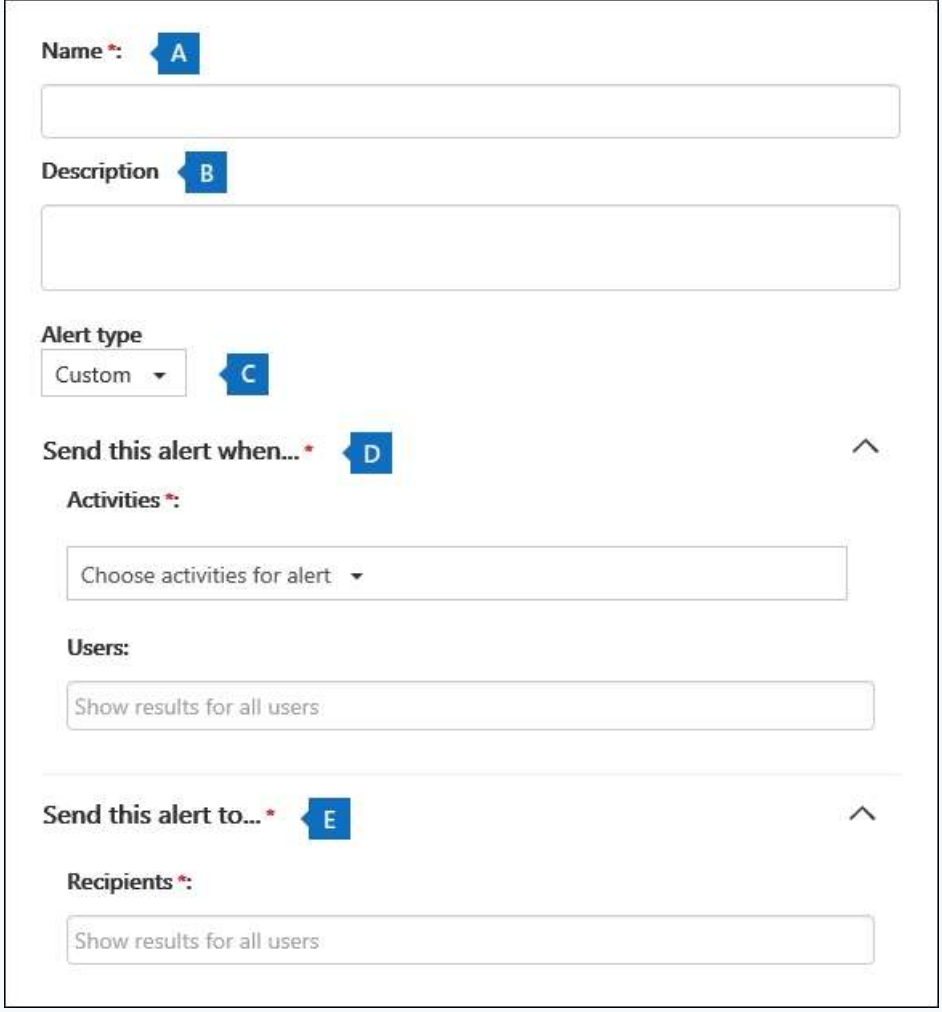
To answer the question, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*

Create an activity alert -

1. Go to https://protection.office.com/managealerts.
2. Sign in to Office 365 using your work or school account.
3. On the Activity alerts page, click + New.

The flyout page to create an activity alert is displayed.



4. Complete the following fields to create an activity alert:

⇨ Name - Type a name for the alert. Alert names must be unique within your organization.

⇨ Description (Optional) - Describe the alert, such as the activities and users being tracked, and the users that email notifications are sent to. Descriptions provide a quick and easy way to describe the purpose of the alert to other admins.

⇨ Alert type - Make sure the Custom option is selected.

⇨ Send this alert when ג€" Click Send this alert when and then configure these two fields:

- Activities - Click the drop-down list to display the activities that you can create an alert for. This is the same activities list that's displayed when you search the Office 365 audit log. You can select one or more specific activities or you can click the activity group name to select all activities in the group. For a description of these activities, see the "Audited activities" section in Search the audit log. When a user performs any of the activities that you've added to the alert, an email notification is sent.

- Users - Click this box and then select one or more users. If the users in this box perform the activities that you added to the Activities box, an alert will be sent. Leave the Users box blank to send an alert when any user in your organization performs the activities specified by the alert.

⇨ Send this alert to ג€" Click Send this alert, and then click in the Recipients box and type a name to add a users who will receive an email notification when a user (specified in the Users box) performs an activity (specified in the Activities box). Note that you are added to the list of recipients by default. You can remove your name from this list.

5. Click Save to create the alert.

The new alert is displayed in the list on the Activity alerts page.



The status of the alert is set to On. Note that the recipients who will received an email notification when an alert is sent are also listed.

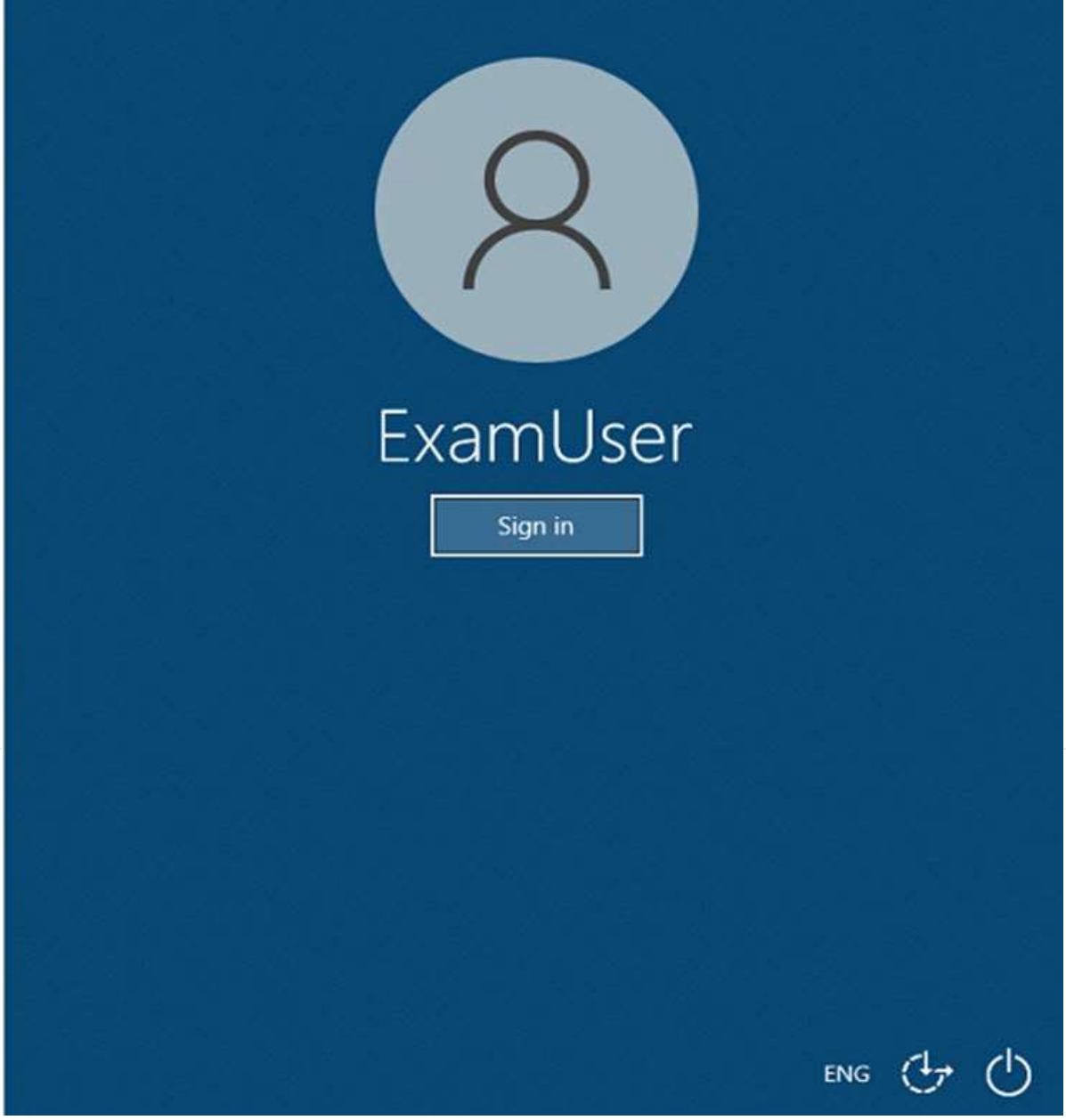
References:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-activity-alerts?view=o365-worldwide

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to ensure that all the users in your organization are prompted to change their password every 180 days.

To answer the question, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*

You need to configure the Password Expiration Policy.

1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Settings section then select the Settings option.
3. Click on Security and Privacy.
4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled ز€Set user passwords to expire after a number of daysز€ is ticked.
6. Enter 180 in the ز€Days before passwords expireز€ field.
7. Click the 'Save changes' button.

HOTSPOT -

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD) by using the Azure AD

Connect Express Settings. Password writeback is disabled.

You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



The Azure AD password policy is configured as shown in the following exhibit.

Hot Area:

Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	○	○
User1 can change the password immediately by using the My Apps portal.	○	○
From Azure AD, User1 must change the password every 90 days.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	○	○
User1 can change the password immediately by using the My Apps portal.	○	○
From Azure AD, User1 must change the password every 90 days.	○	○

Box 1: Yes -

The question states that User1 is synced to Azure AD. This tells us that the short password (Pass) meets the on-premise Active Directory password policy and you were able to create the on-premise account for User1. The on-premise Active Directory password policy applies over the Azure AD password policy for synced user accounts.

Box 2: No -
Self-Service Password Reset would need to be configured.

Box 3: Yes -
The password for the Azure AD User1 account will expire after 90 days according to the Azure AD password policy. If the on-premise password policy has a shorter password expiration period, User1 would have the change his/her on-premise AD password. The new password would then sync to Azure AD.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express

adaniel89 Highly Voted 1 year, 4 months ago
There is no second exhibit! How can you guys answer this question ?
upvoted 23 times

Bobalo 1 year, 2 months ago
Guessing that the policy is fairly default. An on prem policy would win over a policy in AzureAD and password writeback is disabled, already tells you a lot about the possible answers.
upvoted 1 times

TheWallPTA Highly Voted 1 year, 6 months ago
Should this not be YNN?
On-prem Password policy should apply...
upvoted 23 times

BoxGhost 5 months, 1 week ago
I think cloud password expiration for a synced account would be ignored unless you enable a specific feature. So I would be inclined go for YNN

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization#enforcecloudpasswordpolicyforpasswordsyncedusers

When EnforceCloudPasswordPolicyForPasswordSyncedUsers is disabled (which is the default setting), Azure AD Connect sets the PasswordPolicies attribute of synchronized users to "DisablePasswordExpiration". This is done every time a user's password is synchronized and instructs Azure AD to ignore the cloud password expiration policy for that user.
upvoted 2 times

Moderator Most Recent 1 month, 2 weeks ago
Valid question (30th July 2022).
upvoted 1 times

Moderator 2 months ago
Still a valid question (July 30th 2022).
upvoted 1 times

Contactfornitish 2 months, 1 week ago
I would go ynn since the wording says #from Azure ad#. You can't reset from Azure ad without write back
upvoted 1 times

TechMinerUK 3 months, 2 weeks ago
Based on the information provided (Where we can't see the ADDS password policy which means we must assume it is set to no expiry) answer is Y, N, N

This is because:

1. The users password is still valid as it is enabled in ADDS as we do not know if a password policy is applied in ADDS
2. Password writeback is not enabled so the user cannot reset their password in AzureAD
3. Microsoft 365 Password Expiry policies do not apply to on-premises synchronised accounts as stated here https://docs.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide under "Synchronize user passwords hashes from an on-premises Active Directory to Azure AD (Microsoft 365)"
upvoted 1 times

trexar 6 months ago
1.y
2.n
3.n Express installation just perform PHS it means just send the hash.
upvoted 1 times

KSvh53 7 months ago

Where is the 2nd photo? I believe it is missing, which is very important for understanding the question....

upvoted 1 times

Durden871 7 months, 2 weeks ago

This is why I have trust issues:

Password expiry duration (Maximum password age)
Default value: 90 days.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#:~:text=Default%20value%3A%2014%20days%20(before,using%20the%20Set%2DMsolPasswordPolicy%20cmdlet.

As an admin, you can make user passwords expire after a certain number of days, or set passwords to never expire. By default, passwo
are set to never expire for your organization.

Current research strongly indicates that mandated password changes do more harm than good.
https://docs.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide

upvoted 1 times

Durden871 7 months, 2 weeks ago

Looking at the first link further:
The Azure AD password policy doesn't apply to user accounts synchronized from an on-premises AD DS environment using Azure AI
Connect, unless you enable EnforceCloudPasswordPolicyForPasswordSyncedUsers.

So, let's look at it this way:
1. Yes. The user is created on-prem and it will sync to Azure AD
2. No. Password write-back is disabled.
3. Probably No. There is no second exhibit, password write-back is disabled and most importantly, if the user is created on-prem and
sync'd to AzureAD, then the password defaults in Azure should not be applicable to the sync'd users. Doesn't matter if the default po
is 90 days if the directory is sync'd to Azure, and again, how would that even work if writeback is disabled?

This, of course, is assuming EnforceCloudPasswordPolicyForPasswordSyncedUsers wasn't enabled. Since we don't have an image fo
exhibit 2, who knows?

upvoted 2 times

Durden871 7 months, 2 weeks ago

From another source on this very question:
Box 3: Yes -

The password for the Azure AD User1 account will expire after 90 days according to the Azure AD password policy. If the on-premise
password policy has a shorter password expiration period, User1 would have the change his/her on-premise AD password. The new
password would then sync to Azure AD.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express

I looked at the provided article, but see no mention of password policy in the article. Again, I think there's a missing image. Default i
set to 90 days in AzureAD, the policy doesn't apply to accounts synchronized from AD DS unless the enforced cloud password policy
applied.

Really hate this question.

upvoted 1 times

Storm 9 months ago

Default AAD Policy is password never expires (not enabled)...
but lets guess that the missing exhibit shows that this is set to 90 days.
Password Writeback is disabled, which means that if the user tries to change password in Azure he will be told that this is not possible.
To be able for him to change his password in the cloud, he would have to register for SSPR (Self Service Password Reset), whitch he
cannot, as password Writeback is disabled.
Box3 is 100% No

upvoted 2 times

jkklim 9 months, 3 weeks ago

YNY is correct.

For item 3, if no one make any changes (forget about whatever exhibit), azure ad default password policy is 90 days

upvoted 1 times

lengySK 1 year, 1 month ago

If Password Write-Back is disabled, Azure password protection policies won't affect any users that are synced from your directory.
Y, N, N

upvoted 2 times

emilianogalati 1 year, 1 month ago

YNY.

Password is by default set on 90 days before expiration and with a reminder 14 days before.

upvoted 2 times

emilianogalati 1 year ago

Also YNN if you consider writeback is disabled.

upvoted 2 times

AZalan 1 year, 2 months ago

Y,N,N.
There is no password Writeback & by default Password expiration policy is disabled on MS365 admin center. Microsoft recommendatio to have strong password with no expiration policy.

upvoted 3 times

stromnessian 1 year, 2 months ago

EnforceCloudPasswordPolicyForPasswordSyncedUsers
If there are synchronized users that only interact with Azure AD integrated services and must also comply with a password expiration policy, you can force them to comply with your Azure AD password expiration policy by enabling the EnforceCloudPasswordPolicyForPasswordSyncedUsers feature.

When EnforceCloudPasswordPolicyForPasswordSyncedUsers is disabled (which is the default setting), Azure AD Connect sets the PasswordPolicies attribute of synchronized users to "DisablePasswordExpiration".

upvoted 1 times

melatocaroca 1 year, 3 months ago

By default, passwords expire every 90 days, and users are notified to change their password 14 days before that expiration.
From a password history point of view, the system restricts the last password that was used—so a user has to come up with a new password rather than just cycling the same one over and over again.
Reference
https://blog.netwrix.com/2016/10/25/complete-guide-to-azure-active-directory-password-policy/

upvoted 1 times

lucidgreen 1 year, 5 months ago

If Password Write-Back is disabled, Azure password protection policies won't affect any users that are synced from your directory.

upvoted 3 times

lucidgreen 1 year, 5 months ago

Y, N, N.

upvoted 2 times

lucidgreen 1 year, 5 months ago

In our tenant, we have password policies enabled and it only affects non-synced users, possibly because password write-back in disabled.

upvoted 2 times

lucidgreen 1 year, 5 months ago

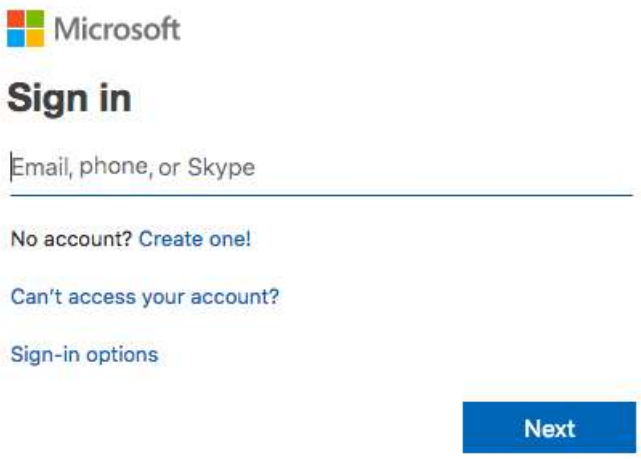
And where's the second exhibit?

upvoted 8 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to add Adele Vance to a group named Managers. The solution must ensure that you can grant permissions to Managers.
To answer, sign in to the Microsoft 365 portal.

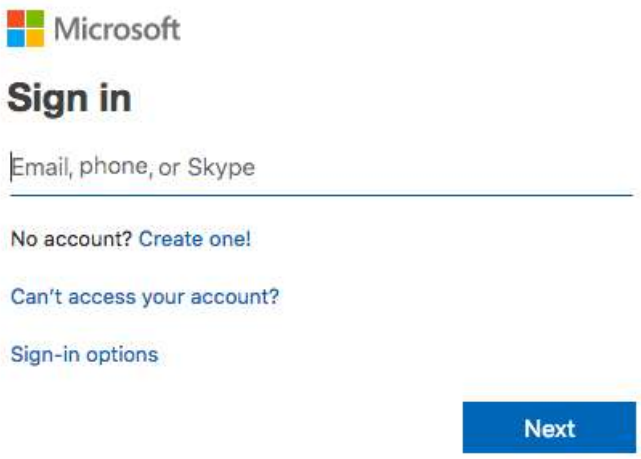
Correct Answer: *See explanation below.*
You need to create a group named Managers and add Adele Vance to the group. To ensure that you can grant permissions to the Managers group, the group needs to be a Security Group.
1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Groups section then select Groups.
3. Click the 'Add a group' link.
4. For the group type, select Security and click Next.
5. Enter 'Managers' in the Name field and click Next.
6. Click the 'Create Group' button to create the Managers group.
7. In the list of groups, select the Managers group.
8. Click the Members link.
9. Click the 'View all and manage members link'.

10. Click the 'Add Members' button.
11. Select Adele Vance and click the Save button.
12. Click the Close button to close the group page.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to create a policy that allows a user named Lee Gu to use Outlook Web App to review 50 percent of the outbound email messages sent by a user named Joni Sherman.
To answer, sign in to the Microsoft 365 portal.

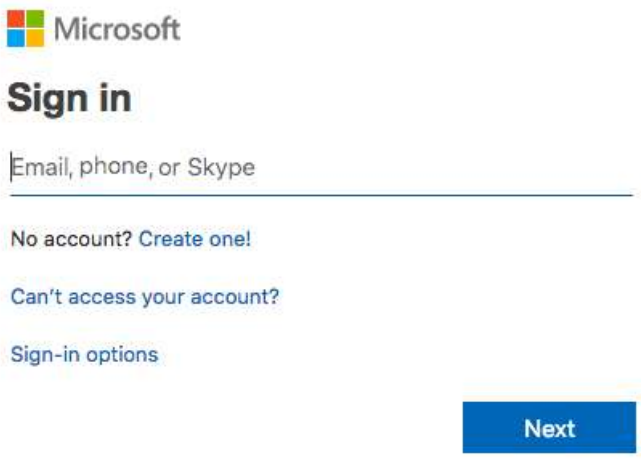
Correct Answer: *See explanation below.*
You need to configure a Supervision Policy.
1. Go to https://protection.office.com or navigate to the Security & Compliance admin center.
2. In the left navigation pane, select Supervision.
3. Click the '+Create' button to create a new supervision policy.
4. Give the policy a name such as 'Joni Sherman' and click Next.
5. In the 'Supervised users' section, click '+Add users or groups'.
6. Select Joni Sherman from the users list and click the Add button.
7. Deselect the 'Teams chats' and 'Skype for Business Conversations' checkboxes leaving only the 'Exchange Email' checkbox ticked and click Next.
8. Under 'Direction is', deselect Inbound leaving only Outbound selected and click Next.

9. In the 'Percentage to review' section, enter 50 and click Next.
10. In the 'Reviewers' section, start typing Lee Gu then select his account when it appears.
11. Click Next.
12. On the 'Review your settings' page, check the settings are correct the click the Finish button to create the policy.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to ensure that all the users in your organization are prompted to change their password every 60 days. The solution must ensure that the users are reminded that their password must be changed 10 days before the required change.
To answer, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*
You need to configure the Password Expiration Policy.
1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Settings section then select the Settings option.
3. Click on Security and Privacy.
4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled ג€Set user passwords to expire after a number of daysג€ is ticked.
6. Enter 60 in the ג€Days before passwords expireג€ field.
7. Enter 10 in the ג€Days before a user is notified about expirationג€ field.
8. Click the 'Save changes' button.

johnyb 1 week, 6 days ago

At the moment I can't see the option for reminding the password expiration.

upvoted 2 times

hufflepuff 3 days, 5 hours ago

Tested and I only see "Days before passwords expire", no reminder options.

upvoted 1 times

OscarGir 1 week, 3 days ago

Agree, I don't see this option

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:
- Contoso.com
- East.contoso.com

An Azure AD Connect server is deployed to contoso.com. Azure AD Connect syncs to an Azure Active Directory (Azure AD) tenant.
You deploy a new domain named west.contoso.com to the forest.
You need to ensure that west.contoso.com syncs to the Azure AD tenant.
Solution: You install a new Azure AD Connect server in west.contoso.com and set AD Connect to active mode.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You can only have one the AD Connect per tenant and one is already located in the root domain. Instead, run the wizard and add the new child domain to sync.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies

SinghG Highly Voted 2 years, 1 month ago
This is incorrect. Right answer is to run the AAD Connect setup wizard to include the newly created sub-domain.
upvoted 37 times

kuuser Highly Voted 2 years, 1 month ago
Is this really true? I thought you should only have one AD Connect server per tenant!
upvoted 20 times

Razuli 1 year, 4 months ago
Exactly, you can't have more than one per tenant
upvoted 9 times

Contactfornitish Most Recent 2 months, 1 week ago
Selected Answer: B
There is only one Azure AD Tenant, for which AAD Connect already deployed. How can one chose A?
upvoted 2 times

Contactfornitish 2 months, 2 weeks ago
Selected Answer: B
Can't be A
upvoted 1 times

Rudelke 2 months, 3 weeks ago
Selected Answer: B
I'm voting B but the question is to vague to answer.

Simply ask your self: do you want west.contoso.com to sync to the same tenant as the rest? And remember: you can have ONE active A connect per tenant BUT you can have MULTIPLE active AAD connect's per domain (OU filtering and what not).

Have fun passing the exam!
upvoted 1 times

aaron_roman 2 months, 4 weeks ago
Selected Answer: B
Incorrect A.
upvoted 1 times

mikaiwhodakno 3 months, 2 weeks ago

Selected Answer: B

No. Can only have one active AD Connect active at a time, and setting this one to active breaks the existing sync for the existing one. Al connect is already deployed in the root domain which can see all child domains. Therefore re-running the wizard and adding the new c domain to sync is the correct answer.

upvoted 1 times

BoxGhost 5 months, 1 week ago

Pretty unfair question. Technically it will sync the new domain but break the other two. So you shouldn't do it but it does meeting the g of syncing the new domain and the question doesn't state that all domains 3 need to sync. I would go for B since it's such a ridiculous solution.

upvoted 4 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 1 times

Creations 1 year, 1 month ago

There is no "active mode " we only have staging mode setting

upvoted 1 times

Nasser 1 year, 1 month ago

It is impossible to do that because one Azure Connect server can be active at a time.

upvoted 1 times

Carlo5 1 year, 3 months ago

"set AD Connect to active mode", I think it is the key word.

upvoted 3 times

melatocaroca 1 year, 4 months ago

According with pure text question, they deploy a new one and set as active, so this action will broke previous sync from father and will setup the new sync from child active mode You deploy a new domain named west.contoso.com to the forest.
You need to ensure that west.contoso.com syncs to the Azure AD tenant.
Solution: You install a new Azure AD Connect server in west.contoso.com and set AD Connect to active mode.
So tricky answer A, real world NO, B

upvoted 2 times

chaoscreater 1 year, 3 months ago

I agree. Correct answeer should be B, but technically if you set the AD Connect on the new server as active, then it'll sync the new domain.

upvoted 1 times

TimNov 1 year, 4 months ago

The answer should be no. east.contoso.com is a child domain of contoso.com and only one active AD connect server is allowed per ten

upvoted 3 times

egdeeptha 1 year, 4 months ago

The correct answer is NO.
AAD connect deployed in the root domain can see all child domains, hence re-running the wizard and adding the new child domain to s is the correct answer.

upvoted 2 times

Mlt1865 1 year, 4 months ago

probably, they deliberately put the wrong answer so there will be discussions. They didn't even put a source to the answer.

upvoted 1 times

Prates_BR 1 year, 5 months ago

No way. NO

upvoted 3 times

Mujja 4 months ago

So, not a No = Yes?

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

- Contoso.com
- East.contoso.com

An Azure AD Connect server is deployed to contoso.com. Azure AD Connect syncs to an Azure Active Directory (Azure AD) tenant.
You deploy a new domain named west.contoso.com to the forest.
You need to ensure that west.contoso.com syncs to the Azure AD tenant.
Solution: You install a new Azure AD Connect server in west.contoso.com and set AD Connect to staging mode.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
When Azure AD Connect is set to staging mode, this action makes the server active for import and synchronization, but it does not run any exports. A server in staging mode is not running password sync or password writeback, even if you selected these features during installation.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-staging-server

txrocker13 Highly Voted 1 year, 9 months ago
All that solution does is setup an additional AADC server which doesn't do any exports. You have to actually change the config to add th new domain into the sync. You can do it through the wizard or just flag that domain inside the sync manager.
upvoted 7 times

tf444 Most Recent 9 months, 2 weeks ago
1AAD 1ADDC, rerun the wizard, and include the new domain.
there is no other option.
upvoted 1 times

MerryWeasel 1 year, 8 months ago
Provided answer is correct.
Explanation: When ADDC is set to staging mode, this action makes the server active for import and synchronization, but it does not run any exports. A server in staging mode is not running password sync or password writeback, even if you selected these features during installation.
References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-staging-server
upvoted 4 times

MerryWeasel 1 year, 8 months ago
typo: *AADC
upvoted 1 times

melatocaroca 1 year, 3 months ago
You install a new Azure AD Connect server in west.contoso.com and set AD Connect to staging mode. Staging without rerun the wiz In the master, will not set the other domain objects https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom
upvoted 1 times

chaoscreater 1 year, 3 months ago
Completely WRONG. A server in staging mode will not do any sync. That's what the active mode is for. You need to read the question "You need to ensure that west.contoso.com syncs to the Azure AD tenant.". A staging mode server will not be able to do a sync.
upvoted 4 times

melatocaroca 1 year, 3 months ago
Agree, they do not tell first was previously down to staging, new can not set new one as active first as staging

During installation, you can select the server to be in staging mode. This action makes the server active for import and synchronization, but it does not run any exports. A server in staging mode is not running password sync or password writeback,

even if you selected these features during installation. When you disable staging mode, the server starts exporting, enables password sync, and enables password writeback.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-staging-server

upvoted 1 times

mkoprivnj 1 year, 9 months ago

No for sure!

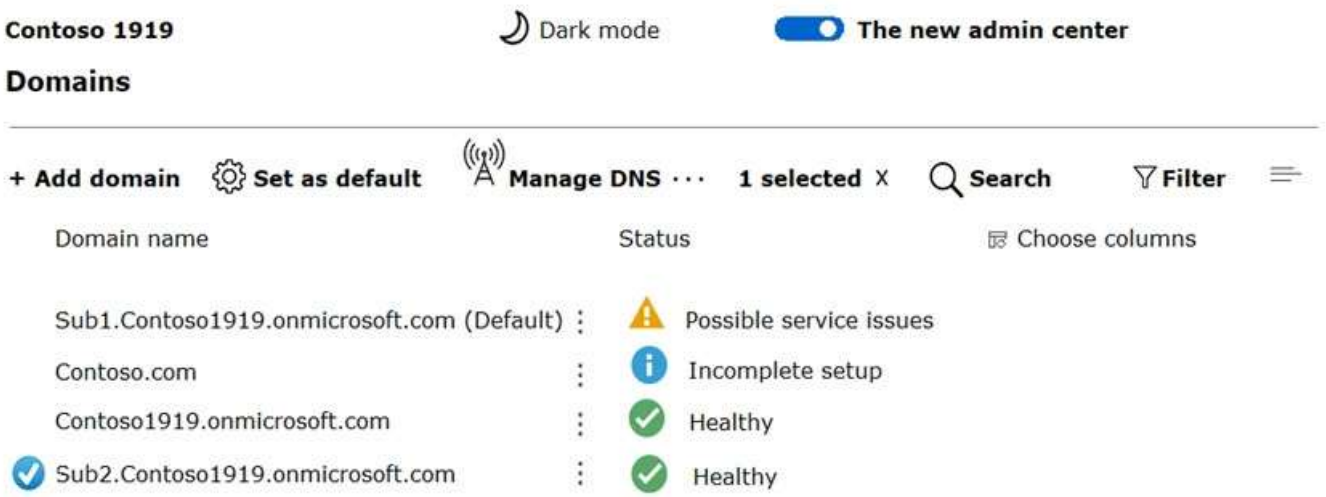
upvoted 3 times

phvogel 1 year, 12 months ago

You do get to add a second AD Connect if the second one is in staging mode...but it doesn't help with the new domain.

upvoted 4 times

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.



Which domain name suffixes can you use when you create users?

A. only Sub1.Contoso1919.onmicrosoft.com

B. only Contoso1919.onmicrosoft.com and Sub2.Contoso1919.onmicrosoft.com

C. only Contoso1919.onmicrosoft.com, Sub1.Contoso1919.onmicrosoft.com, and Sub2.Contoso1919.onmicrosoft.com

D. all the domains in the subscription

Correct Answer: *C*

adaniel89 Highly Voted 1 year, 5 months ago
You can use all three domains to create a user in Microsoft 365 - tried and tested.
upvoted 15 times

PeterC 1 year, 4 months ago
C - is correct, incomplete setup domains can't be used
upvoted 12 times

tochno 1 year, 2 months ago
Agree. Incomplete setup domain is not verified, so it can't be used. Just tested this behavior.
C is correct.
upvoted 3 times

Cheekypoo Most Recent 2 months ago
Was in my exam today 05/08/22.
upvoted 1 times

Sh1rub10 4 months, 2 weeks ago
Selected Answer: C
Incomplete setup domain is not verified, so it can't be used. Others yes
upvoted 1 times

Nilz76 6 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 4 times

glabidi 9 months, 2 weeks ago
In exam today
upvoted 2 times

JakeH 10 months, 3 weeks ago
In exam today

upvoted 2 times

zul_n 1 year ago

I'd say C as well....

Contoso.com - we all know this one is a no
Contoso1919.onmicrosoft.com - we all know this one is good
Sub2.Contoso1919.onmicrosoft.com - we all know this one is good
Sub1.Contoso1919.onmicrosoft.com - possible service issue, but it's the default so most likely it has been verified before.

upvoted 3 times

lengySK 1 year, 1 month ago

I think C

upvoted 1 times

Ash473 1 year, 1 month ago

In exam today

upvoted 2 times

Ash473 1 year, 1 month ago

in exam today

upvoted 2 times

tejb 1 year, 2 months ago

I confirm all domains. When it says "Incomplete Setup", there must be some DNS entries not yet validated. This does not mean i canno create users with the domain.

upvoted 4 times

Turak64 1 year, 1 month ago

Another horrible trick question from MS here. I just tested this as well for a domain that was showing "Incomplete setup" and I was able to create an account using that domain.

upvoted 2 times

iu1942 1 year, 2 months ago

got this question on the exam today

upvoted 2 times

davem90 1 year, 3 months ago

if you add a custom domain the status is: "incomplete setup" whether the domain is verified or not; a new user can only use the domai it has at least been verified. C is definitely the correct answer, because we don't know if contoso.com has been verified or not.

upvoted 1 times

itstudy369 1 year, 3 months ago

all domains

upvoted 2 times

Sprinqfield 1 year, 4 months ago

If we are only going to create a user, all the domains can create users. But if you want to use spesific services you have to complete set So answer is C.

upvoted 1 times

Sprinqfield 1 year, 4 months ago

I cant edit my answers :) answers has to be D

upvoted 2 times

J0J0 1 year, 4 months ago

+1 on this

upvoted 1 times

supaman 1 year, 4 months ago

contoso.com can't be used for sure as incomplete setup. Contoso1919 and Sub2 can surely be used as in 'healthy' status. Sub1 should OK to use otherwise it won't be able to set as default, possible service issues is just fine

upvoted 4 times

Josephsmith 1 year, 5 months ago

The should be B.

upvoted 4 times

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
User1	Global admin	*None*
User2	Exchange admin	*None*
User3	Service support admin	*None*
User4	*None*	Organization Management

You plan to use Exchange Online to manage email for a DNS domain.

An administrator adds the DNS domain to the subscription.

The DNS domain has a status of incomplete setup.

You need to identify which user can complete the setup of the DNS domain. The solution must use the principle of least privilege.

Which user should you identify?

A. User1

B. User2

C. User3

D. User4

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide

melatocaroca Highly Voted 1 year, 3 months ago

The built-in DNS Zone Contributor role enables full control over a DNS resource. It's possible to build your own custom Azure roles to provide finer-grained control. Because no answer provide this option Global administrator User1 Answer A

upvoted 7 times

JakeH Highly Voted 10 months, 3 weeks ago

In exam today

upvoted 5 times

Question #77 *Topic 3*

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure Active Directory.

Which objects will sync to Azure AD?

A. Group1, User1, and User2

B. Group1 and User1 only

C. User1 and User2 only

D. Group1 only

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/concept-azure-ad-connect-sync-user-and-contacts

acamfox224 Highly Voted 1 year, 6 months ago

This should be A. Disabled users are synced by default.

upvoted 43 times

syswiz85 1 year, 5 months ago

100% correct. Disabled users get synced but have a sign in block status of true

upvoted 14 times

NHaikes 2 months, 2 weeks ago

Global Security Group is a scope for the group and is set for created groups:
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups#group-scop

upvoted 1 times

RenegadeOrange 2 months ago

Tested and confirm A is correct and both a Global and Universal group synced to M365.

upvoted 2 times

wilmatic81 Highly Voted 1 year, 5 months ago

Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for examp
conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azur
AD.

The assumption is that if a disabled user account is found, then we will not find another active account later and the object is provision
to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse objec
then its userPrincipalName and sourceAnchor will be used.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/concept-azure-ad-connect-sync-user-and-contacts

upvoted 20 times

PlumpyTumbler 1 year, 4 months ago

Nice source article. Helpful, thank you.

upvoted 3 times

vivekrc7 2 months, 2 weeks ago

Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.

very correct A it is

upvoted 1 times

Contactfornitish Most Recent 2 months, 2 weeks ago

Selected Answer: C

Disabled accounts do sync
Groups would not sync unless it's mail enabled

upvoted 2 times

samstorm10 1 week, 5 days ago

Couldn't be more from the truth i'm afraid. This group would sync.

upvoted 1 times

Rudelke 3 months ago

Selected Answer: A

Global security group - YES - tested
Enabled User - YES
Disabled User (such as SHARED MAILBOX) - YES YES YES

upvoted 1 times

DenisRossi 3 months, 2 weeks ago

Selected Answer: A

A. Disabled users and global groups are synced.

upvoted 1 times

manis73 3 months, 2 weeks ago

Selected Answer: A

It is A, AADC does not sync built in security groups but this group is not a built in security group, it has been created

upvoted 1 times

mikaiwhodakno 3 months, 2 weeks ago

Selected Answer: C

C. Disabled users ARE synced, global security groups are NOT.

upvoted 1 times

TechMinerUK 3 months, 2 weeks ago

Selected Answer: A

The answer should be A as although in-built security groups are not synchronised a global security group is merely a type of security group and as such could be an additional group create by the organisation which would synchronise via AD Connect.

Both users sync to AzureAD since it does not matter if they are disabled or enabled, the user and their status will synchronise across

upvoted 1 times

gaem 3 months, 3 weeks ago

Selected Answer: C

C, sec groups are excluded.

upvoted 1 times

gaem 4 months ago

Selected Answer: C

C...
"Azure AD Connect excludes built-in security groups from directory synchronization.

Azure AD Connect does not support synchronizing Primary Group memberships to Azure AD.

Azure AD Connect does not support synchronizing Dynamic Distribution Group memberships to Azure AD."

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/concept-azure-ad-connect-sync-user-and-contacts

upvoted 2 times

Stiobhan 4 months ago

Answer is C. Global Security Group is a built in group in AD and built in groups are not synced.
Disabled users are synced.

upvoted 1 times

gaem 4 months, 1 week ago

Selected Answer: C

C is the answer!

upvoted 1 times

M_kuttan 4 months, 1 week ago

Selected Answer: A

Disabled user account should sync
upvoted 1 times

gaem 4 months, 2 weeks ago

Selected Answer: C

Answer C.
No sync for group, see reference in others comments
upvoted 1 times

CantStopWontStop 4 months, 3 weeks ago

It's A. BUILT-IN security groups are NOT synced, global security groups are CREATED, thus would sync.
upvoted 1 times

Batman160591 5 months, 3 weeks ago

Selected Answer: C

security groups will not be synced.
"Azure AD Connect excludes built-in security groups from directory synchronization."
Refrence:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/concept-azure-ad-connect-sync-user-and-contacts#:~:text=Azure%20AD%20Connect%20excludes%20built%2Din,Distribution%20Group%20memberships%20to%20Azure%20AD
upvoted 1 times

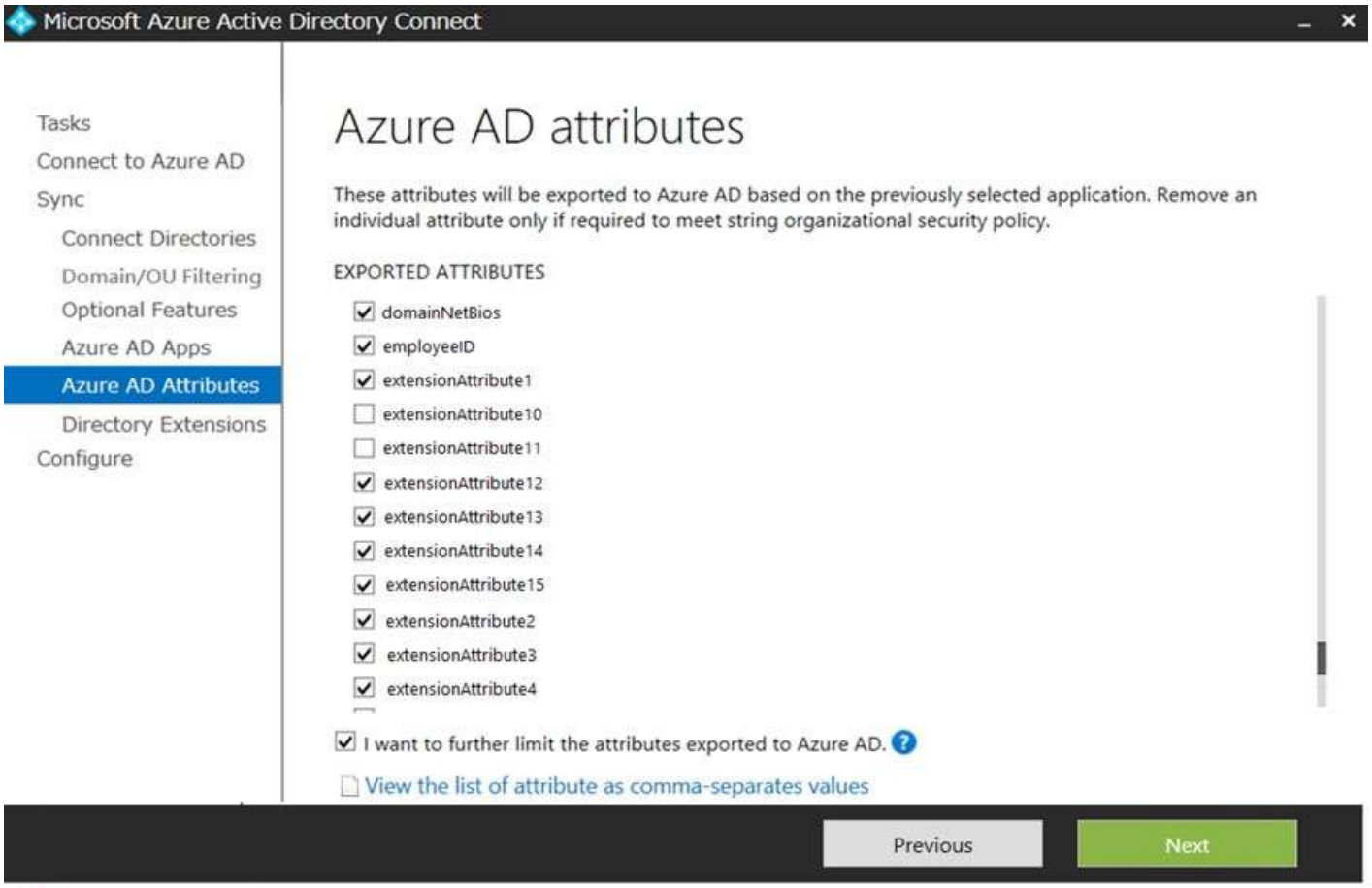
itmaster 6 months ago

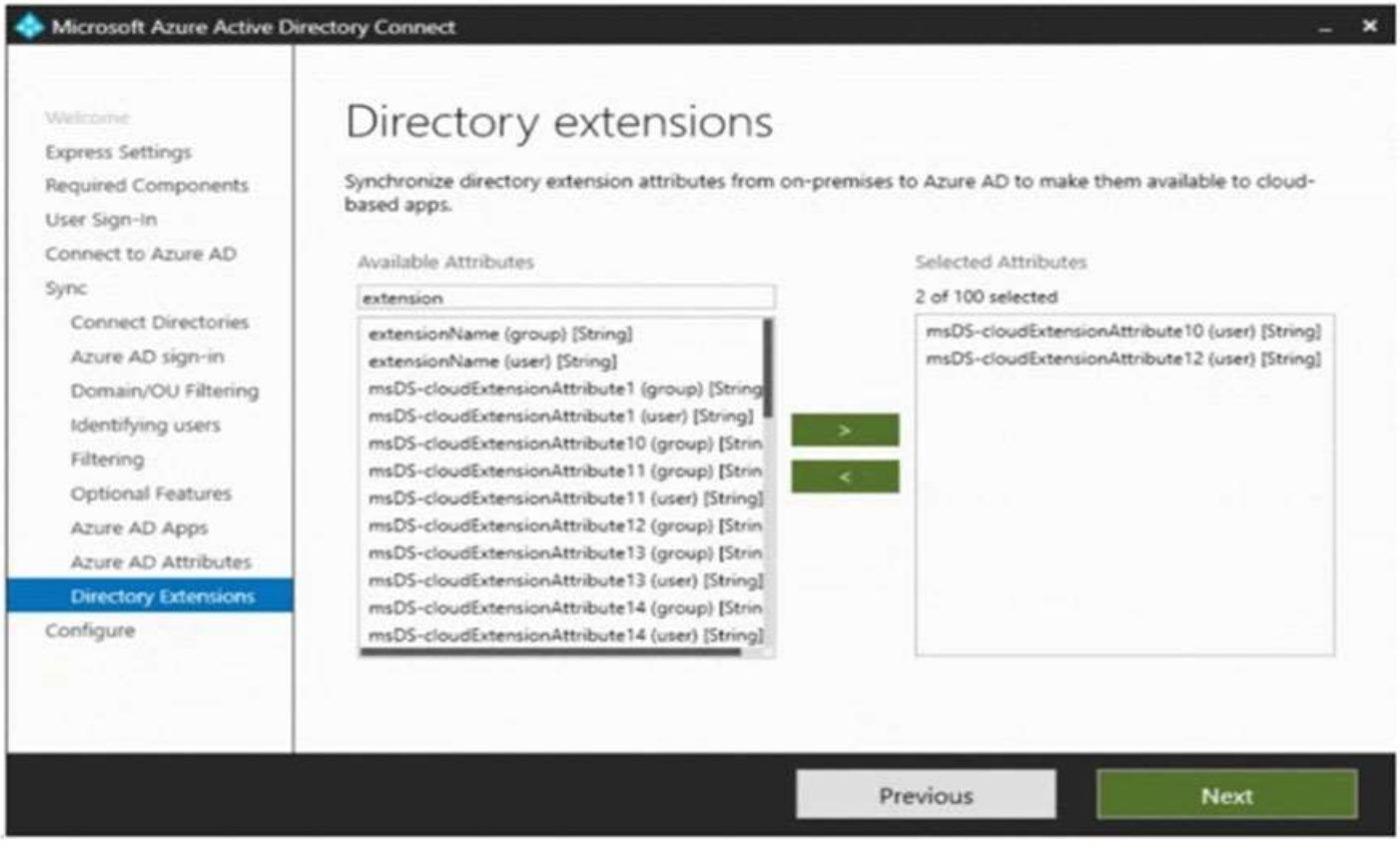
Selected Answer: C

Correct answer is C
Groups are excluded from syncing. Referance:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/concept-azure-ad-connect-sync-user-and-contacts#:~:text=Azure%20AD%20Connect%20excludes%20built%2Din,Distribution%20Group%20memberships%20to%20Azure%20AD
upvoted 2 times

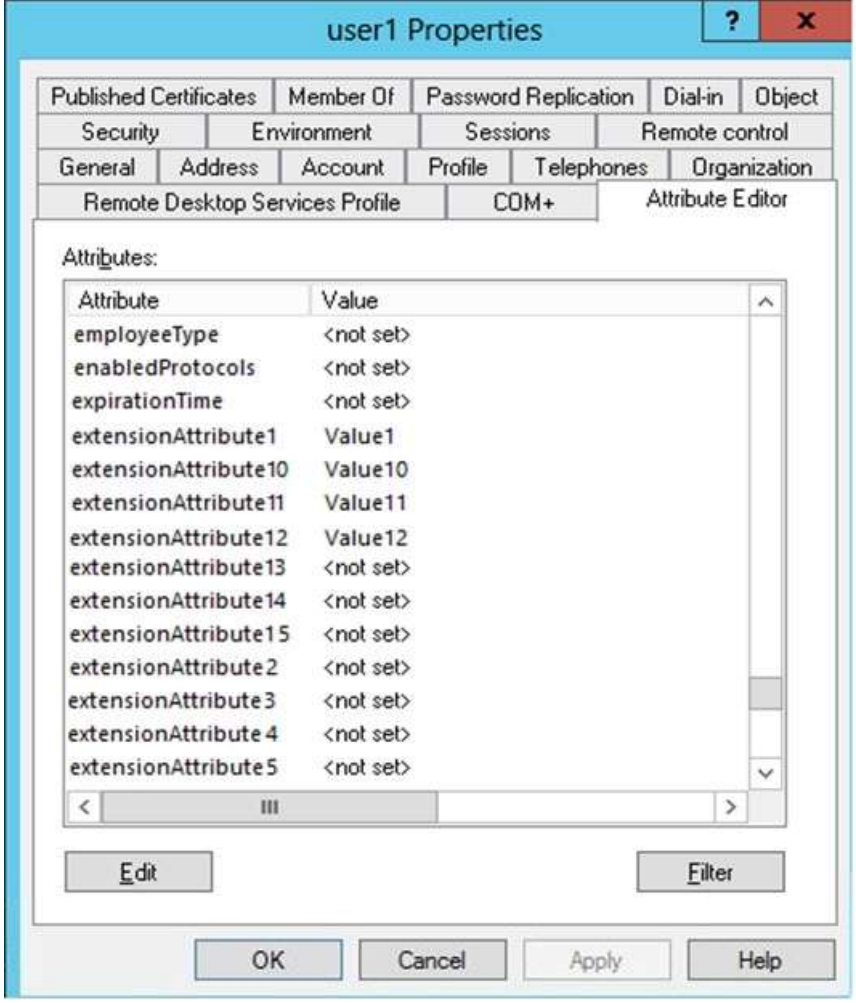
HOTSPOT -

Your network contains an on-premises Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD) as shown in the following two exhibits.





You create a user named User1 in Active Directory as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The value of extensionAttribute1 is synchronized to Azure AD.	○	○
The value of extensionAttribute10 is synchronized to Azure AD.	○	○
The value of extensionAttribute11 is synchronized to Azure AD.	○	○
The value of extensionAttribute12 is synchronized to Azure AD.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The value of extensionAttribute1 is synchronized to Azure AD.	○	○
The value of extensionAttribute10 is synchronized to Azure AD.	○	○
The value of extensionAttribute11 is synchronized to Azure AD.	○	○
The value of extensionAttribute12 is synchronized to Azure AD.	○	○

The Azure AD Attributes page shows which attributes will be synchronized based on the Office 365 services you are using (Exchange, SharePoint etc). We can see that ExtenstionAttribute10 and ExtensionAttribute11 have been deselected.

The Directory Extensions page shows which additional attributes will be synchronized (additional to the list in the Azure AD Attributes page).

ExtensionAttribute1:

Will be synchronized because it is ticked in the Azure AD Attributes page.

ExtensionAttribute10.

Will be synchronized because although it is unticked in the Azure AD Attributes page, it is added again in the Directory Extensions page.

ExtensionAttribute11.
Will not be synchronized because it is unticked in the Azure AD Attributes page and it is not added again in the Directory Extensions page.
ExtensionAttribute12:
Will be synchronized because it is ticked in the Azure AD Attributes page. It is also added again in the Directory Extensions page but this will have no effect as it is already ticked in the Azure AD Attributes page.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-directory-extensions
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

VictorSaiz Highly Voted 9 months, 3 weeks ago
Answer is YNNY. msDS-cloudExtensionAttribute10 or ExtensionAttribute10 are both different attributes. Link: https://www.examtopics.com/discussions/microsoft/view/11557-exam-ms-100-topic-2-question-17-discussion/
upvoted 28 times

FumerLaMoquette 9 months ago
This should be voted to be higher. Indeed they are different attributes.
upvoted 2 times

manis73 3 months, 2 weeks ago
I can't work out why you think this is an msds attribute? Where does it say that? It looks just like a user attribute and the fact its in a option in the azure ad attribute sync seems to imply that it is?
upvoted 1 times

mkoprivnj Highly Voted 1 year, 9 months ago
Yes, Yes, No, Yes is correct answer.
upvoted 9 times

KSvh53 7 months ago
extensionAttribute10 =/= msDS-cloudExtensionAttribute10. Should be Y, N, N, Y.
upvoted 2 times

Rudelke Most Recent 3 months ago
In exam last month
upvoted 2 times

glabidi 9 months, 2 weeks ago
In exam today
upvoted 1 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 1 times

syswiz85 1 year, 5 months ago
Answer provided is correct. The trick question is extensionAttribute10, it's deselected but included in scope in the second screenshot.
upvoted 6 times

[Removed] 2 years, 2 months ago
double question again
upvoted 3 times

Alvaroll 2 years ago
2-17 https://www.examtopics.com/exams/microsoft/ms-100/view/13/
upvoted 4 times

HOTSPOT -

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator, Guest inviter
User3	None
User4	Password administrator

External collaboration settings have default configuration.

You need to identify which users can perform the following administrative tasks:

- Modify the password protection policy.
- Create guest user accounts.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Modify the password protection policy: ▼
- User1 only
- User1 and User2 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Create new guest users in Microsoft Azure Active Directory (Azure AD): ▼
- User1 only
- User1 and User2 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Correct Answer:

Answer Area

Modify the password protection policy: ▼
- User1 only
- User1 and User2 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Create new guest users in Microsoft Azure Active Directory (Azure AD): ▼
- User1 only
- User1 and User2 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Only a Global Admin can modify the password protection policy.

A Global Admin or a user with the Guest Inviter role can create guest accounts.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations

itstudy369 Highly Voted 1 year, 3 months ago

Answer for the 1st question is User1 and User2.
2nd question is all users.

upvoted 25 times

tf444 9 months, 1 week ago

Do you realize User 2 is also a guest inviter?

upvoted 1 times

Ronger 1 year, 3 months ago

Create new guests users, not invite!

"You must be a global administrator to perform this task."

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

upvoted 12 times

Ogabs 8 months ago

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

Creating new guest user in Azure AD can be done by any user if the External Collaboration setting is default.

I've tested this myself:
1. I've logged in to portal.azure.com using a regular (non-admin) account
2. I navigated to Azure AD > Users
3. Clicked New guest user
4. Select Invite user > Type email address
5. Click Invite

This is how you create a guest user in Azure AD. Answer is U1,2,3 & 4

upvoted 2 times

jage01 6 months, 3 weeks ago

Invite with Global admin account vs the other 3 is different.

Just created a guest account with the Global Account, and here to have access to give them access to Groups and Roles.

But with 2,3,4 - you can just invite with no options.

upvoted 1 times

michszym 1 year, 3 months ago

See link you provided: A role that allows you to create users in your tenant directory, like the Global Administrator role or any of t
limited administrator directory roles such as guest inviter or user administrator.

upvoted 8 times

densyo 1 year, 3 months ago

Correct. Global Administrator and Security administrator can modify password protection.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

"External collaboration settings have default configuration."
By default, all users, including guests, can invite guest users.
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/delegate-invitations

upvoted 3 times

girikedar 1 year ago

Exactly You are absolutely Rigth.. Only Global Administrator & Security Administrator are Eligible to perform Password Protection
but i am in doubt that there is Guest Inviter

upvoted 2 times

Turak64 1 year, 1 month ago

Inviting a guest user is not the same as creating one!

upvoted 9 times

BoxGhost 5 months, 1 week ago

Agreed. I would go with User 1 and User 2 only based on the article below.

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

To complete the scenario in this tutorial, you need:

A role that allows you to create users in your tenant directory, like the Global Administrator role or any of the limited administrator directory roles such as guest inviter or user administrator.

upvoted 1 times

TimurKazan Highly Voted 1 year ago

Q1- user 1 and 2
Q2 - user 1
create guest users is different from invite users

upvoted 21 times

MEG Most Recent 4 months, 1 week ago

User1 only can modify the password protection policy.

Check this url: https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator AND search "password protection policy".

upvoted 1 times

briandavisrtr 5 months, 1 week ago

B, B - Why user2 only for "create guest user accounts"? See Prerequisites in this article. https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

upvoted 1 times

RazielLycas 7 months, 2 weeks ago

When is "create" gueast is always mispelled, if you try to "Create" a guest user in AAD it brings you to INVITE it, the same if you perform the task on Powershell https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-invite-powershell Th question is mispelled at the root, if default values are left in place every user is able to invite guest https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide .. if only Microsoft could stops spraying in multiple plac the same thing and collect them in one damn place

upvoted 1 times

Senzokuhle 7 months, 4 weeks ago

The answer is correct. It is currently appearing on AZ 104 as well.

upvoted 1 times

joergsi 8 months, 1 week ago

About Question 1:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

Security Admin can change policies

Question 2
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

Prerequisites
A role that allows you to create users in your tenant directory, like the Global Administrator role or any of the limited administrator directory roles such as guest inviter or user administrator.

upvoted 1 times

LillyLiver 8 months, 1 week ago

So, I had to look at this in my tenant.

Q1: Modify the password protection policy: User1 and User2 only.
Global admins and Security Admins can change the password policy. As well as user administrators, but none of these users are user admins, aside from the GA.

Q2: Create new guest users in Microsoft Azure Active Directory (Azure AD): User1/2/3/4.
External collaboration settings have the default settings. That means all users are allowed to invite guests to the domain. When you inv a guest, it creates a guest account. So they are one-in-the-same. User2 has the Guest Inviter role assigned, which is not needed due to default collaboration settings. The only time you need to use the Guest Inviter role is when you have restricted who can invite others.

upvoted 3 times

Wojer 8 months, 2 weeks ago

A role that allows you to create users in your tenant, like Global Administrator role or any of the limited administrator directory roles su as guest inviter or user administrator will allow you to create Guest Account

upvoted 1 times

TashaGirl 8 months, 2 weeks ago

It is:
Modify password policy - Global Admin, Security Admin.
Create (Invite!) users in Azure AD - Global Admin, Security Admin, Password Admin.
User with no admin role assigned will be denied access to Azure AD blade.

upvoted 1 times

jill44 9 months ago

External collaboration settings have a default configuration, everyone can invite guest users.
User 1, User 2 can modify ,creat PPP

upvoted 1 times

trackexam01 9 months, 1 week ago

answer for 2nd question : user1 and user2 only
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

upvoted 1 times

Jeff8989 9 months, 1 week ago

Security admin can modify password protection.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

upvoted 1 times

tf444 9 months, 1 week ago

The external collaboration setting is set to default, so everyone can invite guests.
https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide

upvoted 1 times

glabidi 9 months, 2 weeks ago

In exam today

upvoted 1 times

wisdom001 9 months, 3 weeks ago

Answer is correct

upvoted 1 times

ferdi3652 10 months, 1 week ago

There is a difference between creating and inviting a guest user. By default all users can invite guest but creating guest users is only assigned to certain roles. Security administrator cannot create guests. Screenshots provided: https://imgur.com/a/sNe1tXy

upvoted 2 times

ferdi3652 10 months, 1 week ago

The same applies to Guest inviter. With this role you cannot create guests, only invite.

upvoted 1 times

Question #80 *Topic 3*

Your network contains a single Active Directory domain and two Microsoft Azure Active Directory (Azure AD) tenants.
You plan to implement directory synchronization for both Azure AD tenants. Each tenant will contain some of the Active Directory users.
You need to recommend a solution for the planned directory synchronization.
What should you include in the recommendation?

A. Deploy two servers that run Azure AD Connect, and then filter the users for each tenant by using organizational unit (OU)-based filtering.

B. Deploy one server that runs Azure AD Connect, and then specify two sync groups.

C. Deploy one server that runs Azure AD Connect, and then filter the users for each tenant by using organizational unit (OU)-based filtering.

D. Deploy one server that runs Azure AD Connect, and then filter the users for each tenant by using domain-based filtering.

Correct Answer: *A*
There's a 1:1 relationship between an Azure AD Connect sync server and an Azure AD tenant. For each Azure AD tenant, you need one Azure AD Connect sync server installation.
Therefore, we need to deploy two servers that run Azure AD Connect for the two Azure AD tenants.
Each user account can only be synchronized to one Azure AD tenant. Therefore, we need a way of splitting the users between the two Azure AD tenants. Azure
AD Connect offers three ways to filter which users get synchronized to an Azure AD tenant. You can use domain-based filtering if you have multiple domains in a forest, attribute-based filtering or OU-based filtering.
Note:
Other incorrect answers for this question include:
1. Deploy one server that runs Azure AD Connect, and then filter the users for each tenant by using attribute-based filtering.
2. Deploy one server that runs Azure AD Connect, and then specify two sync groups.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-azure-ad-tenants
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

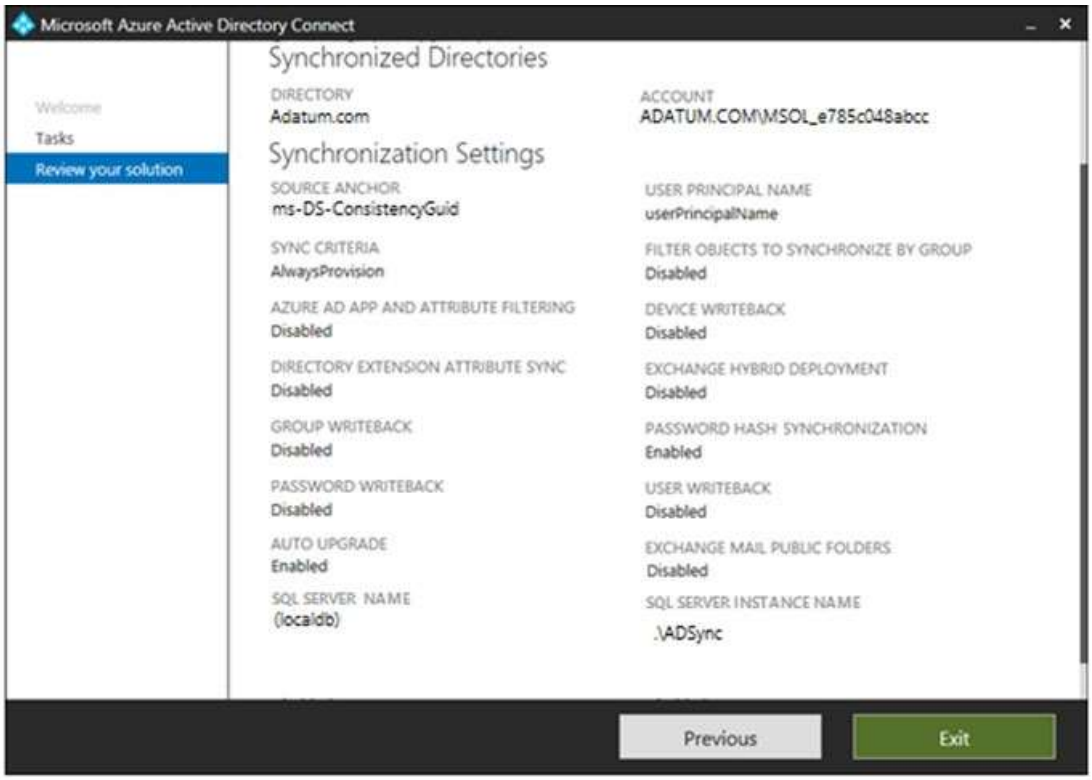
BoxGhost 5 months, 1 week ago
Correct, you can only synchronise AD connect with a single Azure AD tenant so having two servers running AD connect is the only optio that works here.
upvoted 3 times

HOTSPOT -

Your company has a hybrid deployment of Microsoft 365.

An on-premises user named User1 is synced to Microsoft Azure Active Directory (Azure AD).

Azure AD Connect is configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1 **[answer choice]**.

- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory, **[answer choice]**.

- the password hash will be synchronized to Azure AD
- a new randomly generated password will be assigned to User1
- the password hash in Azure AD will be unchanged

Correct Answer:

Answer Area

User1 **[answer choice]**.

- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory, **[answer choice]**.

- the password hash will be synchronized to Azure AD
- a new randomly generated password will be assigned to User1
- the password hash in Azure AD will be unchanged

User1 cannot change her password from any Microsoft portals because Password Writeback is disabled in the Azure AD Connect configuration.

If the password for User1 is changed in Active Directory, the password hash will be synchronized to Azure AD because Password Synchronization is enabled in the Azure AD Connect configuration.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

Ash473 Highly Voted 1 year, 1 month ago

In Exam today

upvoted 5 times

Moderator Most Recent 3 months, 1 week ago

Yes, correct answers given.

upvoted 1 times

chaoscreater 1 year, 3 months ago

Password can be changed from M365 portal, just that password writeback won't work. These are 2 mutually exclusive and different thi

upvoted 2 times

Turak64 1 year, 1 month ago

Test changing the password for an AD sync user in the 365 portal, it won't work.

upvoted 2 times

Chipper 1 year, 2 months ago

While that may be true, if you end up with 2 different passwords because the password doesn't write back, it kind of defeats the purpose of allowing users to change their password.
The way the question was written, I say the given answers are right.

upvoted 4 times

ItsMagige 1 year, 4 months ago

Correct answer because password writeback is disabled, user cannot change his password in any Microsoft portal. Hash synchronizatio enabled therefore the hashes will be synched

upvoted 4 times

maikelb 1 year, 4 months ago

correct!

upvoted 4 times

HOTSPOT -

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Type	Source	Member of
User1@contoso.com	Member	Azure AD	Group1
User2@contoso.com	Member	Windows Server Active Directory	Group1
User3@outlook.com	Guest	Microsoft account	Group1

Password writeback is disabled in Azure AD Connect.

You enable self-service password reset (SSPR) for Group1.

You configure password protection for contoso.com as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can use SSPR to set his password to VeRYC0MplexPa55w.rd.	○	○
User2 can use SSPR to set his password to VeRYC0MplexPa55w.rd.	○	○
User3 can use SSPR to set his password to VeRYC0MplexPa55w.rd.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can use SSPR to set his password to VeRYC0MplexPa55w.rd.	○	○
User2 can use SSPR to set his password to VeRYC0MplexPa55w.rd.	○	○
User3 can use SSPR to set his password to VeRYC0MplexPa55w.rd.	○	○

With the password policy, VeRYC0MplexPa55w.rd. is an acceptable password.

Box 1: Yes -

User1 is an Azure AD account so User1 can reset his password.

Box 2: No -
User2 is a Windows Server Active Directory Account. User2 could change the password for the Azure AD account. However, as Password Writeback is disabled, the password change will not be written back to the Windows Server Active Directory account.

Box 3: No -
The Azure AD Tenant is named contoso.com. User3 is a guest account from a different directory named outlook.com. You cannot use SSPR in one directory to change the password for an account in a different directory.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr-writeback

Arargnum Highly Voted 1 year, 4 months ago
Answer is Y,N,N
User 1 is: Yes because Azure only so can use SSPR
User 2 No: Password write back is disabled, so if the password were reset it wont sync back and if changes made local AD would sync b the password to what it was..
User 3: is out side of tenant control etc @outlook.com, we cannot control passwords for domains outside of our own even if a guest account.
upvoted 18 times

F_M 1 year, 4 months ago
The system prevents User2 from using SSPR. A message saying that password writeback is disabled appeard and the procedure enc
upvoted 4 times

joergsi Highly Voted 8 months, 1 week ago
Question 1 = Who can use SSPR (Self Service Password Reset)? AAD and AD User-Accounts!
Question 2 = If Password Writeback is disabled, who can change the password? AAD User-Accounts!

User1 => AAD => Rule Applys => P55w.rd => Valid Password => YES!
User2 => AD => end of story! => No
User3 => Neither AAD nor AD account => end of story! => No

Correct me where I'm wrong.
upvoted 5 times

fofo1960 Most Recent 9 months, 1 week ago
Wait, Is Password Write Back is disabled, how the SSPR will works to reset users password !
upvoted 1 times

manis73 3 months, 2 weeks ago
user1 is not synced from AD
upvoted 1 times

klosinskil 1 year, 1 month ago
Question doesn't specify from where can user reset his password. All users are allowed to reset their password, 1st from Azure SSPF, 2r from domain PC, 3rd from Outlook OWA.
upvoted 1 times

klosinskil 1 year, 1 month ago
nvrmind read wrong
upvoted 4 times

Flacky_Penguin32 1 year, 3 months ago
Answer: Y, N, N

Microsoft accounts that have been granted guest access to your Azure AD tenant, such as those from Hotmail.com, Outlook.com, or ot personal email addresses, aren't able to use Azure AD SSPR.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#:~:text=Microsoft%20accounts%20that%20have%20been,to%20use%20Azure%20AD%20SSPR.
upvoted 4 times

lucidgreen 1 year, 5 months ago
Y, N, Y
The password policy only applies to User 2.
upvoted 3 times

syswiz85 1 year, 5 months ago

I agree. This is a very tricky question.

upvoted 3 times

Goseu 1 year, 5 months ago

Does SSPR work for Outlook.com accounts ?
Tried and i got :
Microsoft Accounts or personal email addresses don't work here. Make sure you enter your work or school account (e.g. user@contoso.com).

upvoted 4 times

DiNOINYourHead 1 year, 5 months ago

I think you can use SSPR for outlook.com accounts, because the identity tenancy is MSA (Microsoft Account), it will uses the MSA SSPR mechanism.
So, yes, User3 can use SSPR and set the new password.
It is not the SSPR from contoso.com tenant, but however it is not defined in the question.

upvoted 2 times

Question #83 *Topic 3*

You have a Microsoft 365 E5 subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You purchase 100 Microsoft 365 Business Voice add-on licenses.
You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically.
What should you do?

A. From the Azure Active Directory admin center, modify the settings of the Voice group.

B. From the Microsoft 365 admin center, modify the settings of the Voice group.

C. From the Licenses page of the Microsoft 365 admin center, assign the licenses.

Correct Answer: *A*

Fegoseen Highly Voted 1 year, 6 months ago
This can be done only in Azure AD.
The correct answer is A.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign
Manage User Identity and Roles
upvoted 41 times

eknnob 1 year, 6 months ago
I agree correct answer is A
upvoted 7 times

TheWallPTA 1 year, 6 months ago
Agree A. Just tested
upvoted 8 times

Arargnum 1 year, 4 months ago
A for sure.
as this is generally a Azure task.
upvoted 3 times

N4rco101 Highly Voted 1 year, 5 months ago
But e5 has voice included 🤷 🤷
upvoted 7 times

ubt 1 year, 3 months ago
Yes, but the only have 1 E5 licence, they are using that licence to purchase 100 more voice licences
upvoted 2 times

morito Most Recent 3 months, 1 week ago
Selected Answer: A
A is the correct answer.
upvoted 2 times

DenisRossi 3 months, 2 weeks ago
Selected Answer: A
A. You only can do a group license assignment in the Azure AD Portal.
upvoted 2 times

francescoc 3 months, 3 weeks ago
You can do it only in Azure AD. In Microsoft 365 admin center you can assign licenses only to users, and you can assign to a maximum
20 users at a time.
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign
(Assign licenses to users by group membership in Azure Active Directory)
upvoted 2 times

Stiobhan 3 months, 4 weeks ago
What's astonishing is that the link provided by this lot to endorse their "wrong" answer actually points to an article that shows how it's
done in Azure!!! Answer is defo A!
What are we paying for here? Who are the "experts" verifying these answers?

upvoted 1 times

manis73 3 months, 2 weeks ago

And yet we all come back for more :)

upvoted 2 times

Mujja 4 months ago

Selected Answer: A

Correct answer is A.

For C not possible because from M365 you can only assign licences to users.
"Manage and view licenses and apps for your users. Manage group-based licenses in the Azure portal."

upvoted 1 times

Mika_M 4 months, 1 week ago

It's not possible assign to security group license trough M365 admin center, there is a text "... You can assign to a maximum of 20 users a time". You need to use AAD portal. Correct answer is "A"!

upvoted 1 times

gaem 4 months, 2 weeks ago

Selected Answer: A

AAD only

upvoted 1 times

itmaster 6 months ago

Selected Answer: C

I would choose C for the answer.
From Azure portal, you cannot assign license under group settings, so all provided answers are wrong, but the closest one is C, becaus you go to licenses under 365 Admin portal, you cannot assign a license to a group, but there is the following option there:
"Manage and view licenses and apps for your users. Manage group-based licenses in the Azure portal" with hyperlink for "Azure portal you just need to click on it and do the group assignement.

upvoted 1 times

ARYMBS 5 months, 1 week ago

Tried AAD -> Groups -> GroupNameXXX-> Licenses blade??

upvoted 1 times

KSvh53 7 months ago

The reference link provided says Azure AD....Whoever chose that answer must have meant to choose A bc their own source says otherwise...

upvoted 1 times

dumbo_trash 7 months ago

Selected Answer: A

Only can be done in AAD

upvoted 1 times

Zaorac 7 months, 3 weeks ago

Selected Answer: A

Answer should clearly be A.

Read the mission statement carefully:
"You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatica

There is already a group created with the name Voice. The goal is to have these licenses assigned automatically to its members, curren new. The key word is automatically.

This can only be accomplished by editing said group in Azure AD. What you have to do is go to the group in question -> Licenses -> Assignments and assign the license Microsoft 365 Business Voice add-on.

upvoted 1 times

Ogabs 8 months ago

Cannot be done in Licenses page of the Microsoft 365 admin center - I've just tested it. Answer is A

upvoted 1 times

joergsi 8 months, 1 week ago

Correct Answer: C
You can assign licenses to a user or a group from the Licenses page of the Microsoft 365 admin center.

=> Wrong, have tried it in my lab environment, you are only able to assign licenses to a group in the AAD Admin center. On the License page of the Microsoft 365 admin center, you are only able to assign licenses to user accounts!

upvoted 1 times

LillyLiver 8 months, 1 week ago

Selected Answer: A

Yeah, "C" is not automated.

upvoted 1 times

antoniofig62 8 months, 3 weeks ago

Selected Answer: A

answer A

upvoted 1 times

Question #84 *Topic 3*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains a user named User1.
You suspect that an imposter is signing in to Azure AD by using the credentials of User1.
You need to ensure that an administrator named Admin1 can view all the sign in details of User1 from the past 24 hours.
To which three roles should you add Admin1? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Security administrator

B. Password administrator

C. User administrator

D. Compliance administrator

E. Reports reader

F. Security reader

Correct Answer: *AEF*
Users in the Security Administrator, Security Reader, Global Reader, and Report Reader roles can view the sign in details.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Golo Highly Voted 2 years, 11 months ago
Regarding https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins#prerequisites the correct ans
should be Security Administrator, Security Reader, and Report Reader roles
upvoted 51 times

Hamster5000 2 years, 8 months ago
Surely you dont need Security reader role if you already have Security administrator
upvoted 8 times

Kaylewis 2 years ago
Hamster500, you need a security reader role to be assigned to Admin1. The question says each of the role should serve as a complete solution. Answers are Security administrator, report reader and security reader. I am still wondering why a password administrator will be able to view sign-in logs. Any help will be appreciated
upvoted 2 times

treanor 2 years, 9 months ago
the question should be "To which three roles _could_ you add Admin1?". The user does not need to be added to all roles
upvoted 7 times

WoneSix 2 years, 7 months ago
treanor, agreed. It should be one of those "What is the role you -should- add Admin1 to so he can view the logon activity?"
upvoted 1 times

SMHH 2 years, 7 months ago
Question specifically states Each correct answer presents a complete solution.
upvoted 6 times

joergsi 8 months, 1 week ago
In the link above the following information can be found:

Who can access Sign-in logs in Azure Active Directory?
You can always access your own sign-ins history using this link: https://mysignins.microsoft.com

To access the sign-ins log, you need to be:
- A global administrator

A user in one of the following roles:
- Security administrator
- Security reader

- Global reader
- Reports reader

upvoted 1 times

lusis987 Highly Voted 2 years, 7 months ago

Answers: A,E,F

upvoted 24 times

Nilz76 Most Recent 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 1 times

adaniel89 1 year, 4 months ago

If you have Security Administrator role, you dont need Security Reader role! https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

upvoted 1 times

asthmaticninja 1 year, 6 months ago

AEF as per https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

upvoted 2 times

ppolychron 1 year, 7 months ago

A, E, F

Read sign-in logs: Reports reader, Security Reader, Security administrator
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#monitoring---sign-ins

upvoted 7 times

lucidgreen 1 year, 6 months ago

This seems to be the best source I've seen.

upvoted 2 times

[Removed] 1 year, 8 months ago

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Who can access the data?
Users in the Security Administrator, Security Reader, Global Reader, and Report Reader roles
Global Administrators
Any user (non-admins) can access their own sign-ins

upvoted 1 times

mkoprivnj 1 year, 9 months ago

A, E, F for sure!

upvoted 4 times

dibdoank 1 year, 9 months ago

It's definitely A E F > Report reader, security reader and Security Administrator, source: Read sign-in logs > Reports reader, Security Rea
Security administrator

upvoted 1 times

Jayatheerthan 1 year, 11 months ago

It says "You need to ensure that an administrator named Admin1 can view all the sign in details". This means he is only going to view th
sign-in report. Then the answer will be A,E,F. Only these role have the permission to view the Sign-in reports.

upvoted 3 times

h3nk13 2 years, 1 month ago

Tricky question: Admin1 can view all the sign in "details".

upvoted 1 times

emil568 2 years, 1 month ago

Sign-in activity reports in the Azure Active Directory portal:

Who can access the data?
Users in the Security Administrator, Security Reader, Global Reader, and Report Reader roles
Global Administrators
Any user (non-admins) can access their own sign-ins

upvoted 1 times

M0S1 2 years, 1 month ago

i agree with answer being A,E,F

upvoted 1 times

ctfalci 2 years, 2 months ago

Answer: A E F
Explanation
Users in the Security Administrator, Security Reader, Global Reader, and Report Reader roles can view the sign in details.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

upvoted 14 times

shark1 2 years, 3 months ago

Tricky, AEF, if you follow the microsoft.directory/auditLogs/allProperties/read permission to be exacted.

upvoted 3 times

kazaki 2 years, 3 months ago

Users in the Security Administrator, Security Reader, Global Reader, and Report Reader roles
Global Administrators
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins#prerequisites
this is totally wrong answer

upvoted 1 times

TonySuccess 2 years, 3 months ago

AEF, ridiculous question though.

upvoted 2 times

Question #85 *Topic 3*

You have Microsoft 365 tenant that contains a Microsoft Power Platform environment named Environment1 (default). Environment1 contains a Microsoft
Dataverse database.
In the tenant, you create a user named User1. You assign a Microsoft Power Apps license to User1.
Which security role for Environment1 is assigned automatically to User1?

A. Environment maker

B. System customizer

C. Delegate

D. Environment admin

Correct Answer: *A*

junior6995 Highly Voted 1 year ago
Microsoft says: A user is automatically associated with the Environment Maker role when they are added to an environment.

https://docs.microsoft.com/en-us/learn/modules/get-started-security-roles/2-roles
upvoted 13 times

Aps123 1 year ago
Correct
upvoted 1 times

Highgate Most Recent 6 months ago
From the reference link (https://docs.microsoft.com/en-us/power-platform/admin/database-security#predefined-security-roles) "Environment Maker and Environment Admin are the only predefined roles for environments that have no Dataverse database" as this environment contains a database, it doesn't sound like the answer is A.
upvoted 1 times

jage01 6 months, 3 weeks ago
Selected Answer: A
A.

The default environment
A single default environment is automatically created by Power Apps for each tenant and shared by all users in that tenant. Whenever a new user signs up for Power Apps, they're automatically added to the Maker role of the default environment. The default environment is created in the region closest to the default region of the Azure AD tenant.

https://docs.microsoft.com/en-us/power-platform/admin/environments-overview
upvoted 1 times

massimo_bartalotta 8 months ago
Selected Answer: A
Dataverse
upvoted 1 times

LeoGS182 8 months, 4 weeks ago
Selected Answer: A
https://docs.microsoft.com/en-us/power-platform/admin/assign-security-roles

In the Finance and Operations linked Dataverse environment, Finance and Operations Basic User and Environment Maker security roles are automatically assigned to all active users in Dataverse.
upvoted 1 times

glabidi 9 months, 2 weeks ago
In exam today
upvoted 1 times

AlexLiourtas 10 months, 1 week ago

A

A

For the Default environment type, “BasicUser” and “EnvironmentMaker” roles will be assigned automatically to all users added in Dataverse.

https://docs.microsoft.com/en-us/power-platform/admin/assign-security-roles

upvoted 3 times

Mavula 10 months, 2 weeks ago

So why is the answer still B -System customizer? which one is which?

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

allesglar 10 months, 3 weeks ago

Selected Answer: A

We have this exact problem in our tenant. We do not want to use the Power Platform and every user gets on default the enviroment maker role.
The answer is A

upvoted 4 times

Archie_Bunker 11 months, 4 weeks ago

According to this link the answer should be: A. Environment Maker

https://docs.microsoft.com/en-us/power-platform/admin/assign-security-roles

upvoted 4 times

Tuno 1 year ago

It is not about any role, it is about “Which —-— security ——-role for Environment1”

upvoted 1 times

Tuno 1 year ago

However, I don’t think it is automatically assigned: “ System customizer is a Microsoft Power Platform security role. This role has full permissions to customize a Microsoft Power Platform environment.
To assign a user the System administrator Power Platform role, go to Configure user security to resources in an environment.”

upvoted 1 times

AS007 1 year ago

Correct

upvoted 1 times

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	On-premises Active Directory group membership
User1	Cloud application administrator	*None*
User2	Application administrator	*None*
User3	Service administrator	*None*
User4	*None*	Domain Admins

You plan to provide access to an on-premises app named App1 by using Azure AD Application Proxy. App1 will be managed by User4.

You need to identify which user can install the Application Proxy connector.

Which user should you identify?

A. User1

B. User2

C. User3

D. User4

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application

hhaywood Highly Voted 1 year, 4 months ago

I disagree, the admin role to install the connector is on-prem therefore should be User4

upvoted 21 times

hjumaa Highly Voted 1 year, 4 months ago

Connector installation requires local admin rights to the Windows server that it's being installed on. It also requires a minimum of an Application Administrator role to authenticate and register the connector instance to your Azure AD tenant.
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deployment-plan

upvoted 12 times

KSvh53 7 months ago

You are correct. So since the question asked who can install it, the answer is D. If it asked who could register it in Azure AD, the answ would then be B.

upvoted 6 times

Claire91 Most Recent 2 months, 2 weeks ago

Answer D
It needs to install on the server, so would need domain admin rights

upvoted 1 times

Sh1rub10 4 months, 2 weeks ago

Selected Answer: D

refer to KSvh53 comment

upvoted 2 times

KSvh53 7 months ago

For those that are not aware, domain admins are by design given local admin access to a domain controller and all member servers an workstations on a domain. Domain admin = local admin of that server. Azure AD admin =/= local admin to server. An Azure AD admin h absolutely no connection whatsoever to the local admin on that server.

"Domain Admins are, by default, members of the local Administrators groups on all member servers and workstations in their respecti domains. This default nesting should not be modified for supportability and disaster recovery purposes."

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory

upvoted 2 times

KSvh53 7 months ago

Selected Answer: D

This is a tricky one. The keyword in the question is "install". A local admin on the server (aka a domain admin) would be needed to insta
Therefore the only correct answer for this question is D. If, however, the question asked who would be able to register it in Azure AD, th
only correct answer would be B. Both installing it on the server and registering it in Azure AD are necessary to make it work, but that's
what the question asks. It only asks who is able to install it on the server. See link below.

"Connector installation requires local admin rights to the Windows server that it's being installed on. It also requires a minimum of an
Application Administrator role to authenticate and register the connector instance to your Azure AD tenant."

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deployment-plan

upvoted 2 times

KSvh53 7 months ago

This is a tricky one. The keyword in the question is "install". A local admin on the server (aka a domain admin) would be needed to insta
Therefore the only correct answer for this question is D. If, however, the question asked who would be able to register it in Azure AD, th
only correct answer would be B. Both installing it on the server and registering it in Azure AD are necessary to make it work, but that's
what the question asks. It only asks who is able to install it on the server. See link below.

"Connector installation requires local admin rights to the Windows server that it's being installed on. It also requires a minimum of an
Application Administrator role to authenticate and register the connector instance to your Azure AD tenant."

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deployment-plan

upvoted 2 times

JamesM9 7 months, 1 week ago

The answer is B, Application Administrator -
"Prerequisites. To add an on-premises application to Azure AD, you need:

A Microsoft Azure AD premium subscription
An application administrator account"

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

upvoted 1 times

RazielLycas 7 months, 2 weeks ago

Selected Answer: B

B is correct https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application#install-
and-register-a-connector .We have to suppose that this user is Local Admin on the server where the connector will be installed or is in a
group of admins that can perform such installation on server but are not domain admins.

upvoted 1 times

KSvh53 7 months ago

That is incorrect. If it asked which user could register it in Azure AD, you would be correct, but it is instead asking who can install it o
the server. Only a local admin of the server (aka a domain admin) can install it. It is wrong to assume that Azure AD role is a local ad
on the server, especially when they're not in the domain admins group or any security group on the server.

upvoted 2 times

Zaorac 7 months, 3 weeks ago

Selected Answer: D

The answer should be D.

"You need to identify which user can _INSTALL_ the Application Proxy connector."

If it were to authenticate and register I would agree with B being the correct answer but it clearly asks for which user is able to install th
connector. User4 has Domain Admin rights which means they have local admin rights on the server. User2 has the role Application
Administrator but it's not stated they have local admin rights.

"Connector installation requires local admin rights to the Windows server that it's being installed on. It also requires a minimum of an
Application Administrator role to authenticate and register the connector instance to your Azure AD tenant."
From the link:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deployment-plan

Obviously everyone knows that you don't need domain admin to have local admin rights to a server, but nowhere in the question is it
stated that any of them have local admin rights, except for User4 with admin rights to all servers in the domain.

I'm quite shocked that there exists any doubt here when it's one of the more straightforward questions.

upvoted 3 times

KSvh53 7 months ago

100% agreed. Read the question more carefully, people, and know how administrators on a server work. We don't just assume an Az
AD admin account is automatically going to have local admin rights to the on-prem server. That's not how it works.

upvoted 1 times

joergsi 8 months, 1 week ago

Selected Answer: B

I found this information:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deployment-plan

Administrative rights and roles:

=> Connector installation requires local admin rights to the Windows server that it's being installed on. It also requires a minimum of a Application Administrator role to authenticate and register the connector instance to your Azure AD tenant.

=> Application publishing and administration require the Application Administrator role. Application Administrators can manage all applications in the directory including registrations, SSO settings, user and group assignments and licensing, Application Proxy setting and consent. It doesn't grant the ability to manage Conditional Access. The Cloud Application Administrator role has all the abilities of t Application Administrator, except that it does not allow management of Application Proxy settings.

The correct answer is (B)

upvoted 1 times

KSvh53 7 months ago

Read the question again. It's not asking about the registering in Azure AD. It's only asking about the installation piece. Since B is not the domain admins group, we can't just assume that role will have local admin rights on that server. The only one we know for sure have local admin rights is D. And since we aren't being asked about the registration, only the installation, D is the only correct answe

upvoted 1 times

LillyLiver 8 months, 1 week ago

Selected Answer: D

As I just went through the steps, the App Proxy Connector is a downloadable file that will need to be installed locally. The App Admin m have to setup the external application to get the proxy connector, but the only user that can install the connector here is User4, the domain admin.

upvoted 4 times

Storm 9 months ago

Only user4 can install the connector, and only user2 can connect it...
Stupid question, but they ask which user can install the Application Proxy connector, so I'm going with User4

upvoted 2 times

jkklim 9 months, 2 weeks ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application#prerequisites

it states that plan to PROVIDE ACCESS TO ON-PREMISES apps. They are asking for apl;ication proxy connector which is USER2 (APPLICATION ADMIN)

fOR INSTALLATION OF connector on servers, SERVERS installer user can be LOCAL ADMINISTRATOR, not necessary domain admins. Remember servers is member joined, thus in real life, many people use server local administrator to install software

upvoted 3 times

LillyLiver 8 months, 1 week ago

See, you and I were thinking the same thing. But, as I just went through the steps, the App Proxy Connector is a downloadable file t will need to be installed locally. The App Admin may have to setup the external application to get the proxy connector, but the only u that can install the connector here is User4, the domain admin.

upvoted 1 times

sliix 7 months, 3 weeks ago

Local admin doesn't necessarily be a domain admin user on the on premise environment.

upvoted 1 times

bake73 7 months, 3 weeks ago

Domain Admins get Local admin rights by default. Nowhere in the question it is state that any other user as local admin rights

Dont listen to those bozos up here and never assume more than what is in the question.

User4

upvoted 2 times

KSvh53 7 months ago

That is a wrong assumption to make. Just because the Azure AD account exists doesn't mean they'll have a local account on the serv let alone a local admin account on the server. If the question didn't say they have a local admin account, you're wrong to assume tha Domain admins, however, are given local admin rights on the server. That's how domain admin works. D is the only one we know fo sure has local admin rights on that server based on the information given (rather than wrongful assumptions).

upvoted 1 times

Jcbrow27 10 months, 2 weeks ago

correct user2

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application#prerequisites

upvoted 1 times

rseb 1 year ago

I believe this is B. Despite you need to local rights to install it (create the service), you also need App Admin role to complete the setup - during the connector wizard you are prompted for your App Admin creds in order to register itself in your AAD, like described in step 8 https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

upvoted 3 times

Chipper 1 year ago

The question literally says the user needs to be able to install the app proxy. User 4 is the only one who can do that on prem

upvoted 1 times

MomoLomo 1 year, 1 month ago

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application#prerequisites

it doesn't mention anything about on prem roles required so i think given answer is correct

upvoted 1 times

Azreal_75 1 year, 1 month ago

I thought it was D initially but I'm inclined to agree after reading that article, we are all assuming that best practices are being adopt such that elevated admin permissions are required for the installation - the article above just assumes the person doing the install is admin, so Imma hang my hat on B.

upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains five domain controllers.

Your company purchases Microsoft 365 and creates a Microsoft Azure Directory (Azure AD) tenant named contoso.onmicrosoft,com.

You plan to establish federation authentication between on-premises Active Directory and the Azure AD tenant by using Active Directory Federation Services (AD

FS).

You need to establish the federation.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Action to perform before establishing the federation:

- From the Azure portal, add a custom domain name.
- From the Azure portal, configure an authentication method.
- From a domain controller, install a Pass-through Authentication Agent.
- From a domain controller, install Windows Identity Foundation 3.5.

Tool to use to establish the federation:

- Active Directory Domains and Trusts
- Azure AD Connect
- The AD FS console
- The Azure portal

Correct Answer:

Answer Area

Action to perform before establishing the federation:

- From the Azure portal, add a custom domain name.
- From the Azure portal, configure an authentication method.
- From a domain controller, install a Pass-through Authentication Agent.
- From a domain controller, install Windows Identity Foundation 3.5.

Tool to use to establish the federation:

- Active Directory Domains and Trusts
- Azure AD Connect
- The AD FS console
- The Azure portal

The on-premises Active Directory domain is named contoso.com. Before you can configure federation authentication between on-premises Active Directory and the Azure AD tenant, you need to add the domain contoso.com to Microsoft 365. You do this by adding a custom domain name.

The next step is to establish the federation. You can configure AD FS by using Azure AD Connect.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom#configuring-federation-with-ad-fs

lucidgreen Highly Voted 1 year, 7 months ago

Azure AD Connect does all the magic in the console. All you need is to have the domain added to Azure. Unless you have some extra m you need to do. But that's beyond the scope of this question.

upvoted 9 times

Goofer Highly Voted 2 years, 8 months ago

there are 3 ways to create a Federation.
1. Installation Azure AD Connect --> User Sign-in --> Federation with ADFS
2. Powershell on ADFS server --> Convert-MsolDomainToFederated -DomainName <domain>
3. ADFS console --> create Relying Party Trust

3. Create

upvoted 8 times

WoneSix 2 years, 7 months ago

While the aqbove are true, what you SHOULD use to keep from having errors, is to use AAD Connect to create the federation. It's mo foolproof.

upvoted 11 times

Moderator Most Recent 2 months ago

Still a valid question (July 30th 2022), variation on it though (1st anwer).

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 1 times

mkoprivnj 1 year, 9 months ago

1 & 2 is correct. Add custom domain to AAD tenant and for federation use AAD Connect.

upvoted 5 times

Jake1 1 year, 10 months ago

Answer is correct. Azure Active Directory (Azure AD) Connect lets you configure federation with on-premises Active Directory Federation Services (AD FS) and Azure AD.

upvoted 1 times

donathon 1 year, 11 months ago

Answer is correct: https://azure.microsoft.com/en-ca/resources/videos/configuring-ad-fs-for-user-sign-in-with-azure-ad-connect/

upvoted 3 times

[Removed] 2 years, 2 months ago

double question again

upvoted 4 times

Alvaroll 2 years ago

2-22 https://www.examtopics.com/exams/microsoft/ms-100/view/36/

upvoted 1 times

STFN2019 2 years, 2 months ago

ans is correct

upvoted 2 times

juliuscsir 2 years, 6 months ago

Is a custom domain required, since the tenant will be a subdomain of 'onmicrosoft.com'?

upvoted 2 times

melki_zedek 2 years, 4 months ago

Yes a custom domain is required. for a production environment custom domain is preferred over the .onmicrosoft.com

upvoted 1 times

VP11 2 years, 6 months ago

If you plan to federate your on-premises Windows Server AD with Azure AD, then you need to select I plan to configure this domain for single sign-on with my local Active Directory when you run the Azure AD Connect tool to synchronize your directories.
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain

upvoted 1 times

Sisko 2 years, 8 months ago

Second drop down should be ADFS Console, shouldn't it?

upvoted 2 times

HOTSPOT -

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

You need to identify which users can perform the following tasks:

- View sync errors in Azure AD Connect Health.
- Configure Azure AD Connect Health settings.

Which user should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

View sync errors in Azure AD Connect Health: [▼]
- User1
- User2
- User3

Configure Azure AD Connect Health settings: [▼]
- User1
- User2
- User3

Correct Answer:

Answer Area

View sync errors in Azure AD Connect Health: [▼]
- User1
- **User2**
- User3

Configure Azure AD Connect Health settings: [▼]
- **User1**
- User2
- User3

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-diagnose-sync-errors https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

renrenren 1 week, 2 days ago

User 2 for 2nd
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations#:~:text=Contributor,AD%20Connect%20Health.

upvoted 1 times

xyz213 2 weeks, 2 days ago

User2 for both?

upvoted 3 times

HOTSPOT -

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.

The domain contains the users shown in the following table.

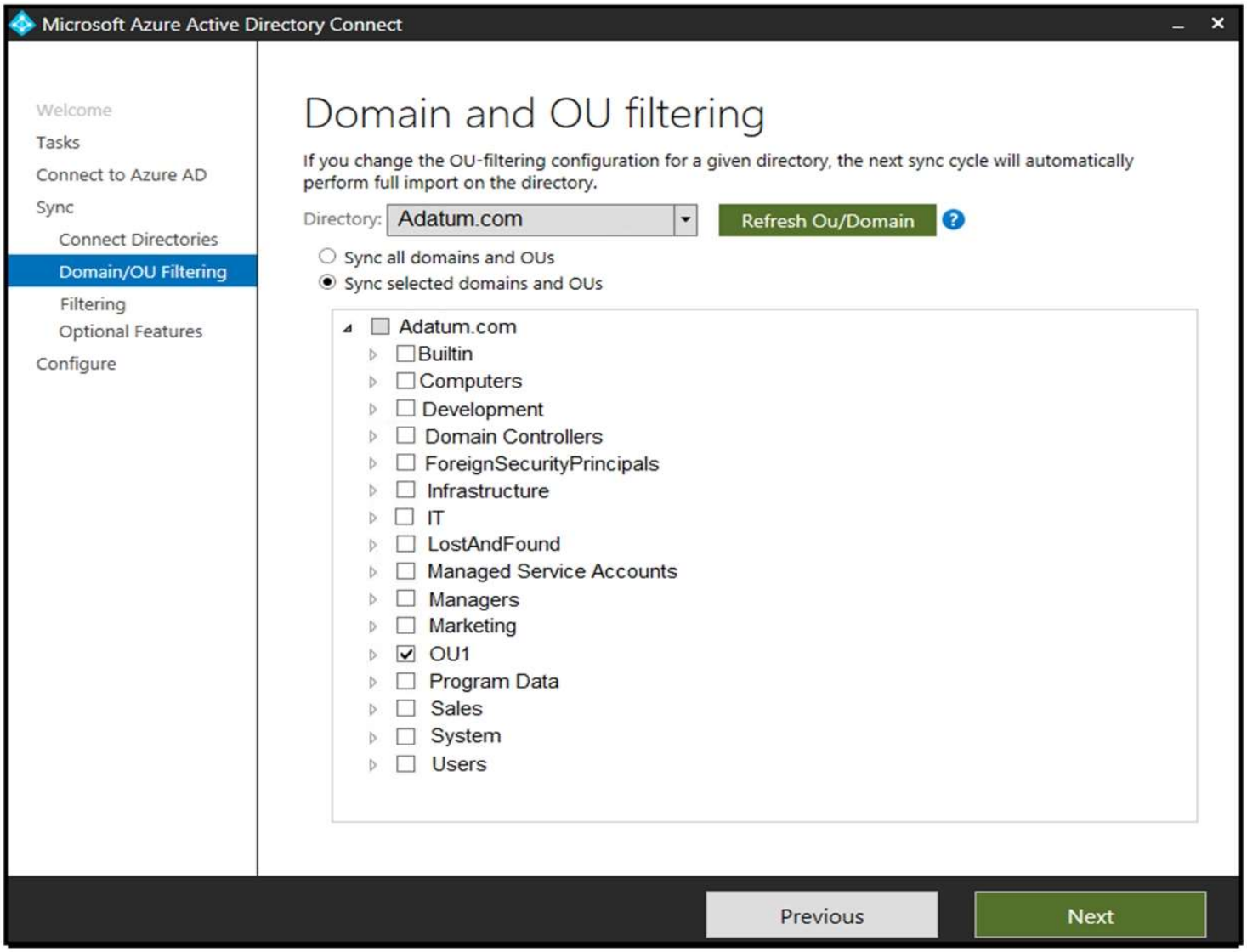
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

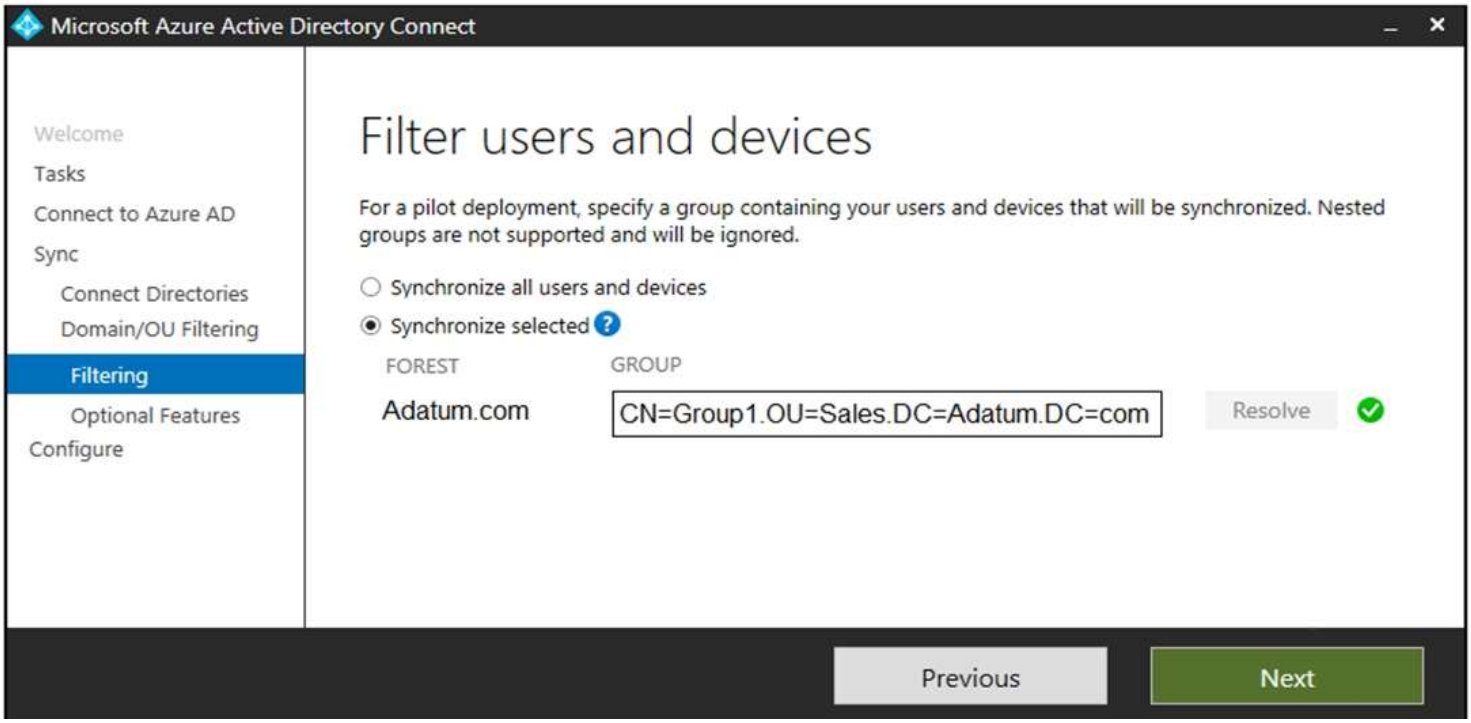
Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.

You configure Domain and OU filtering as shown in the following exhibit.



You configure Filter users and devices as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 syncs to Azure Active Directory (Azure AD).	○	○
User2 syncs to Azure Active Directory (Azure AD).	○	○
Group2 syncs to Azure Active Directory (Azure AD).	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 syncs to Azure Active Directory (Azure AD).	○	○
User2 syncs to Azure Active Directory (Azure AD).	○	○
Group2 syncs to Azure Active Directory (Azure AD).	○	○

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

Swyft 1 week ago

The questions states "You are deploying Azure AD Connect."
From MS "You can configure group-based filtering the first time that you install Azure AD Connect by using custom installation. It's

intended for a pilot deployment where you want only a small set of objects to be synchronized. When you disable group-based filtering
can't be enabled again. " https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering
So it will still work.
However Nested group membership is not resolved – objects to synchronize must be direct members of the group used for filtering.
So I would say
YNN

upvoted 1 times

Pupu2196 2 weeks, 3 days ago

Can anyone provide an answer to this?

upvoted 1 times

xyz213 2 weeks, 3 days ago

Should be N/N/N
When a Group is not in a synced OU nothing gets synced
Besides that Nested group membership is not resolved – objects to synchronize must be direct members of the group used for filtering
https://azurecloudai.blog/2019/11/07/field-notes-azure-active-directory-group-filtering-gotchas/

upvoted 1 times

chewitt 2 weeks, 1 day ago

Why wouldn't User 1 and 2 sync they are in OU1 that is synced?

upvoted 1 times

KemalM 2 weeks, 6 days ago

Wrong ... It should be No, No, No since group is Sales OU which does not synchronize

When using OU-based filtering in conjunction with group-based filtering, the OU(s) where the group and its members are located must
included. (https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-based-filteri

upvoted 1 times

Topic 4 - Question Set 4

Question #1 *Topic 4*

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.
All users use Windows 10 devices to access Microsoft Office 365 apps.
All the devices are in a workgroup.
You plan to implement passwordless sign-in to contoso.com.
You need to recommend changes to the infrastructure for the planned implementation.
What should you include in the recommendation?

A. Join all the devices to contoso.com.

B. Deploy Azure AD Application Proxy.

C. Deploy X.509.3 certificates to all the users.

D. Deploy the Microsoft Authenticator app.

Correct Answer: *D*
Reference:
https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/

PmgCosta 5 months, 1 week ago
From: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone

Prerequisites
To use passwordless phone sign-in with the Microsoft Authenticator app, the following prerequisites must be met:

Recommended: Azure AD Multi-Factor Authentication, with push notifications allowed as a verification method. Push notifications to yo
smartphone or tablet help the Authenticator app to prevent unauthorized access to accounts and stop fraudulent transactions. The
Authenticator app automatically generates codes when set up to do push notifications so a user has a backup sign-in method even if th
device doesn't have connectivity.
Latest version of Microsoft Authenticator installed on devices running iOS 8.0 or greater, or Android 6.0 or greater.
The device on which the Microsoft Authenticator app is installed must be registered within the Azure AD tenant to an individual user.
upvoted 1 times

Question #2 *Topic 4*

You have a Microsoft 365 subscription and a hybrid Microsoft Exchange Online deployment.
You plan to deploy iOS devices that will use Outlook for iOS and Hybrid Modern Authentication (HMA).
You need to ensure that HMA is configured correctly.
What should you use?

A. Apple Configurator

B. Microsoft Remote Connectivity Analyzer

C. Microsoft Diagnostics and Recovery Toolset (DaRT)

D. Microsoft Support and Recovery Assistant

Correct Answer: *B*
Reference:
https://testconnectivity.microsoft.com/tests/o365

You have a hybrid deployment of Microsoft 365 that contains the users shown the following table.

Name	Source	Last sign in
User1	Azure Active Directory (Azure AD)	Yesterday
User2	Windows Server Active Directory	Two days ago
User3	Windows Server Active Directory	Never

Azure AD Connect has the following settings:

- Password Hash Sync: Enabled
- Pass-through authentication: Enabled

You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.

Which users should you identify?

A. none

B. User1 only

C. User1 and User2 only

D. User1, User2, and User3

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

renrenren 1 month ago

Not sure, but probably go for D. User3 will be able to log in according to
"The first time you enable the password hash synchronization feature, it performs an initial synchronization of the passwords of all in-scope users."

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

upvoted 1 times

defalt1846 1 month ago

why not c? since the user 3 never signed in.

upvoted 1 times

BoxGhost 5 months, 1 week ago

Surely the answer is B? The article linked specifically mentions you would have to re-run the wizard manually to disable PTA if connectiv is lost!

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#cloud-authentication-pass-through-authentication

Considerations. You can use password hash synchronization as a backup authentication method for pass-through authentication, whe the agents can't validate a user's credentials due to a significant on-premises failure. Fail over to password hash synchronization doesn happen automatically and you must use Azure AD Connect to switch the sign-on method manually.

upvoted 2 times

PmgCosta 5 months, 1 week ago

Nop, the answer is D, because the Password Hash Syncronization is also enabled, if you are offline, AzureAD have the HASH for all th users

upvoted 3 times

xyz213 2 weeks, 3 days ago

I am with BoxGhost here. Only User1

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-faq
"Does password hash synchronization act as a fallback to Pass-through Authentication?
No. Pass-through Authentication does not automatically failover to password hash synchronization. To avoid user sign-in failures you should configure Pass-through Authentication for high availability."

upvoted 1 times

xyz213 2 weeks, 3 days ago

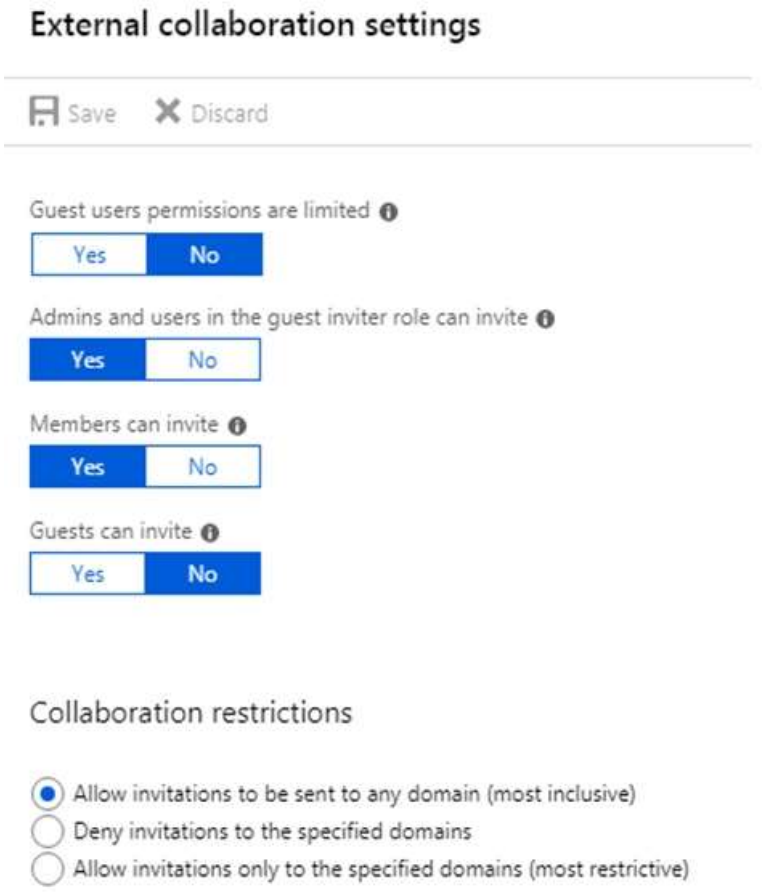
PHS with PTA is only used if you have PTA but want to use "sign-in desaster recovery or leaked credential reports - see Decision Tree:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 subscription that contains a guest user named User1. User1 is assigned the User administrator role.

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. Contoso.com is configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1 can **[answer choice]**.

- open the Azure portal only
- open the Azure portal and view users only
- open the Azure portal, view users, and create new guest users only
- open the Azure portal, view users, create new users, and create new guest users

All other guest users can **[answer choice]**.

- open the Azure portal only
- open the Azure portal and view users only
- open the Azure portal, view users, and create new guests only
- open the Azure portal, view users, create new users, and create new guest users

Correct Answer:

Answer Area

User1 can [answer choice].

- open the Azure portal only
- open the Azure portal and view users only
- open the Azure portal, view users, and create new guest users only
- **open the Azure portal, view users, create new users, and create new guest users**

All other guest users can [answer choice].

- open the Azure portal only
- **open the Azure portal and view users only**
- open the Azure portal, view users, and create new guests only
- open the Azure portal, view users, create new users, and create new guest users

Default permissions for guests are restrictive by default. Guests can be added to administrator roles, which grant them full read and write permissions contained in the role. There is one additional restriction available, the ability for guests to invite other guests. Setting Guests can invite to No prevents guests from inviting other guests.

User1 is assigned the User Administrator role. Therefore, User1 can open the Azure portal, view users, create new users, and create new guest users.

In the exhibit, the 'Guest user permissions are limited' is set to no. This means that guest users have the same permissions as members. However, the 'Guests can invite' setting is set to No. Therefore, other guest users (all guest users except User1) can open the Azure portal and view users in the same way as member users can.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/b2b/delegate-invitations https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions

Domza Highly Voted 1 year, 6 months ago

Why would you give a Guest - an Admin Role???

upvoted 5 times

gsmith9897 1 year, 5 months ago

We hired an outside contractor to work on our Sharepoint site, so he has a guest account with admin rights to Sharepoint.

upvoted 15 times

apel Most Recent 9 months ago

I don't think any guest users or non admin users can view users in azure AD portal. When they select azure AD, they will get no access error code 403.

upvoted 2 times

alex_p 6 months, 3 weeks ago

You should first try it - then make comments

upvoted 8 times

jkklim 9 months, 2 weeks ago

corrrect answers.

upvoted 1 times

JakeH 10 months, 3 weeks ago

In exam today

upvoted 2 times

junior6995 1 year ago

Don't bother discussing External Collaboration settings on this question, this section in Azure AD is renewed with better wording. Outdated question.

upvoted 2 times

TimurKazan 1 year ago

what a silly answers. create is not the same as invite! another bad question from MS. In fact user1 can invite user. not create

upvoted 1 times

Chipper 1 year ago

User1 is an admin (User Administrator). why would this user not be able to create users?

upvoted 2 times

GlenRMag16 8 months, 1 week ago

I tried it in my lab and user admin can only invite user, not create

upvoted 1 times

itmaster 6 months ago

I also tried in my lab and user administrator CAN create a guest user, so how come in your lab he cannot?! I think you need to out and log in again after assiging a new permission :)

upvoted 1 times

adaniel89 1 year, 3 months ago

1st box - D
2nd box - C - all users can create guest user accounts
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/add-users-administrator

upvoted 1 times

J0J0 1 year, 3 months ago

Guest cannot invite. read.

upvoted 6 times

Aysan 1 year, 4 months ago

when the guest can invite guest option is disabled, how the user admin (which is a guest) can invite more guest users?

upvoted 2 times

chaoscreater 1 year, 3 months ago

Read the question? Admins and users in the guest inviter role can invite. User1 is admin.

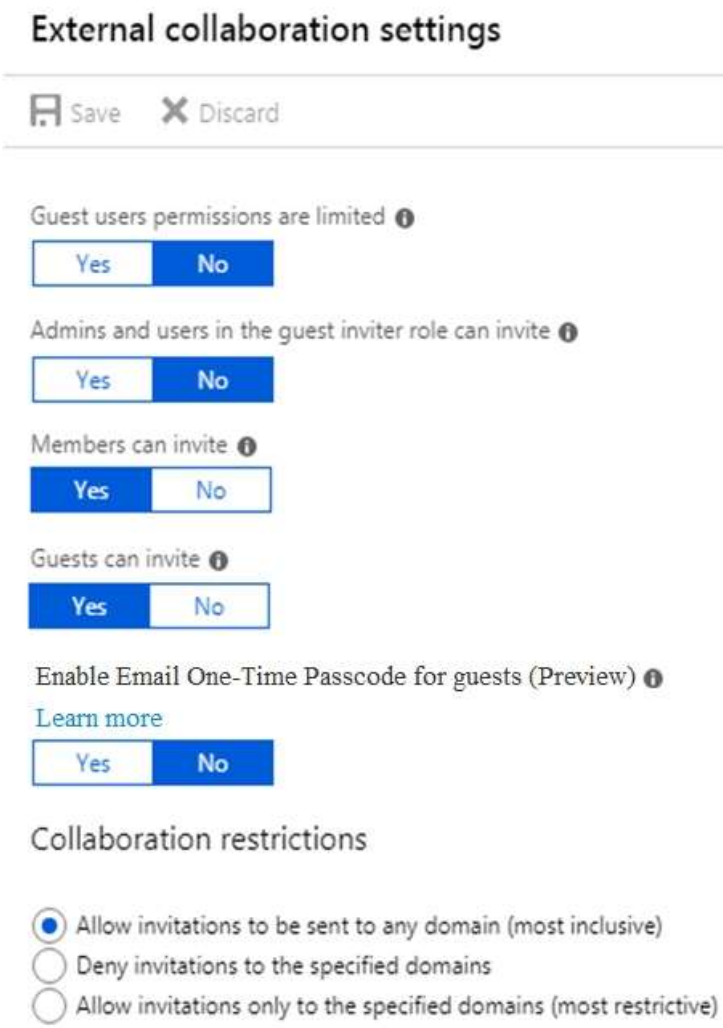
upvoted 2 times

Razuli 1 year, 4 months ago

What about: contains a guest user named User1. User1 is assigned the User administrator role but guest roles are blocked

upvoted 1 times

You have a Microsoft 365 subscription and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
Contoso.com is configured as shown in the following exhibit.



You need to ensure that guest users can be created in the tenant.
Which setting should you modify?

A. Guests can invite.

B. Guest users' permissions are limited.

C. Members can invite.

D. Admins and users in the guest inviter role can invite.

E. Deny invitations to the specified domains.

Correct Answer: *D*
The setting ג€Admins and users in the guest inviter role can inviteג€ is set to No. This means that no one can create guest accounts because they cannot 'invite' guests. This setting needs to be changed to Yes to ensure that guest users can be created in the tenant.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/delegate-invitations https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions

MartiFC 1 year, 2 months ago
D is correct
upvoted 4 times

Question #6 *Topic 4*

Your company recently purchased a Microsoft 365 subscription.
You enable Microsoft Azure Multi-Factor Authentication (MFA) for all 500 users in the Azure Active Directory (Azure AD) tenant.
You need to generate a report that lists all the users who completed the Azure MFA registration process.
What is the best approach to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. From Azure Cloud Shell, run the Get-AzureADUser cmdlet.

B. From Azure Cloud Shell, run the Get-MsolUser cmdlet.

C. From the Azure Active Directory admin center, use the Usage & insights blade.

D. From the Azure Active Directory admin center, use the Risky sign-ins blade.

Correct Answer: *B*
You can use the Get-MsolUser cmdlet to generate a report that lists all the users who completed the Azure MFA registration process. The full command would look like this:
Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0} | Select-Object -Property

UserPrincipalName -
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting

jwaegebaert Highly Voted 1 year, 5 months ago
Usage & insights blade also gives a quick overview of all the users registered with MFA. I would even say it's easier to use than the CLI
upvoted 14 times

BGM_YKA 1 year, 4 months ago
Usage & Insights, Authentication methods activity can give you a report on the registered members and who's not.
upvoted 3 times

BGM_YKA 1 year, 4 months ago
So is C. better than B.?

I think C. is better for ad-hoc check as its pretty quick and you don't have to lookup the PS attributes to build the list
upvoted 4 times

Manojch 1 year, 4 months ago
where can i fing usage & Insights?
upvoted 1 times

AlexLiourtas 10 months ago
azure ad portal.azure.com
upvoted 1 times

rfox321 1 year ago
This is correct. Not only that, that commandlet is NOT an AzureAD command. It is an MSOL command.. two completely different powershell modules. I highly suggest trying it and/or reviewing.
upvoted 2 times

BoxGhost 5 months, 1 week ago
Yep, it says select the best answer. This is much easier than messing about with CLI/PS commands

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/authentication-methods-usage-amp-insights/ba-p/745370
upvoted 1 times

amitsharma170490 Most Recent 3 weeks, 3 days ago
B & C both are correct, if I have to choose the best answer then would go for C as UI is more User friendly then running the PS, but ind
PS is more helpful in automating things and getting things faster if the script is handy
upvoted 2 times

Kainzor 2 months ago

I am not here to debate but from the article: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-report

It is specified in there the following: "Identify users who have registered for MFA using the PowerShell that follows. This set of comman excludes disabled users since these accounts cannot authenticate against Azure AD: Answer: Get-MsolUser

There are different ways to get it sure but we can't really blame others when the question is so often unclear, just 1 single extra info would've made the right answer clearer.

upvoted 1 times

Claire91 2 months, 2 weeks ago

Answer C: From the Azure Active Directory admin center, use the Usage & insights blade.

Azure Active Directory > Useage and Insights > Authentication methods Activity > You can see all users regisitered and the usage

upvoted 1 times

Rhoddy 3 months, 2 weeks ago

Selected Answer: B

Correct answer is B. Usage & Insights only reports on MFA METHOD and the question is asking for a report on USERS registered. You cannot get a list of users from Usage & Insights.

upvoted 1 times

Mug1992 6 months, 3 weeks ago

Selected Answer: C

Change my mind please - can you run Get-MsolUser in AZURE CLOUD SHELL ?
I think it works, but with Windows Powershell with the module MSOnline.
So defenitly C.

upvoted 1 times

joergsi 8 months, 1 week ago

You can use below PowerShell cmdlets to get a list of users with MFA Enabled:

Install-Module MSOnline If the module is not installed already.

Connect-MsolService Login with Global Admin account.

Get-MsolUser -All | select DisplayName,BlockCredential,UserPrincipalName,@{N="MFA Status"; E={ if($_.StrongAuthenticationRequirements.State -ne $null){ $_.StrongAuthenticationRequirements.State} else { "Disabled"}}}

To get a list of users with MFA Enabled

=> Answer B is correct

upvoted 2 times

Wojer 8 months, 2 weeks ago

For me is C, because for Azure Cloud Shell you need to create a subscription, and for usage&insight it's just there.

upvoted 1 times

kanag1 8 months, 3 weeks ago

Selected Answer: C

Usage & Insights provides the details

upvoted 1 times

Storm 9 months ago

Has anybody tried running the get-msoluser from Cloud Shell ?
You all seems so sure ;-)...

upvoted 2 times

Shadow983 9 months, 1 week ago

Selected Answer: C

C is a better answer

upvoted 1 times

jkklim 9 months, 2 weeks ago

C is correct - i use it daily to generate report of MFA

upvoted 1 times

08twitch 9 months, 2 weeks ago

Selected Answer: B

It says open Cloud Shell, not open PowerShell. I'm answering B

upvoted 1 times

AlexLiourtas 9 months, 1 week ago

where does it say that?

upvoted 2 times

allesglar 10 months, 3 weeks ago

I will go with B. Even though C is also correct and maybe even easier B is the method recommended in the documentation.

upvoted 3 times

allesglar 10 months, 3 weeks ago

I will go with B. Even though C is also correct and maybe even easier B is the method recommended in the documentation.

upvoted 1 times

TimurKazan 11 months ago

C is an easier way to achieve the goal, with many additional settings

upvoted 1 times

fko1978 1 year, 1 month ago

in my opinion c is better. For B you need to open powershell connect to msonline with account and type command. C would be easier, i guess.If you allready have powershell running and connected, b would be best

upvoted 1 times

Question #7 *Topic 4*

You have a Microsoft 365 Enterprise subscription.
You have a conditional access policy to force multi-factor authentication when accessing Microsoft SharePoint from a mobile device.
You need to view which users authenticated by using multi-factor authentication.
What should you do?

A. From the Microsoft 365 admin center, view the Security & Compliance reports.

B. From the Azure Active Directory admin center, view the user sign-ins.

C. From the Microsoft 365 admin center, view the Usage reports.

D. From the Azure Active Directory admin center, view the audit logs.

Correct Answer: *B*
With the sign-ins activity report in the Azure portal, you can get the information you need to determine how your environment is doing.
The sign-ins report can provide you with information about the usage of managed applications and user sign-in activities, which includes information about multi- factor authentication (MFA) usage. The MFA data gives you insights into how MFA is working in your organization. It enables you to answer questions like:
⇨ Was the sign-in challenged with MFA?
How did the user complete MFA?
▪
⇨ Why was the user unable to complete MFA?
⇨ How many users are challenged for MFA?
⇨ How many users are unable to complete the MFA challenge?
⇨ What are the common MFA issues end users are running into?
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting

gaem 4 months, 2 weeks ago
Selected Answer: B
COrrect Answer
upvoted 1 times

junior6995 1 year ago
Azure AD > Security > Risky Sign-Ins > Add the Filter Application: SharePoint and the other Filter Authentication Method: MFA. Done.
upvoted 3 times

zorro1 1 year ago
The questions is about normal sign-ins, not risky sign-ins
upvoted 1 times

BoxGhost 5 months, 1 week ago
I wish there was an option to downvote silly answers,
upvoted 4 times

mitsios96 1 year, 1 month ago
B , Answer is correct.
upvoted 4 times

You have a Microsoft 365 Enterprise E5 subscription.
You need to enforce multi-factor authentication on all cloud-based applications for the users in the finance department.
What should you do?

A. Create a sign-in risk policy.

B. Create a new app registration.

C. Assign an Enterprise Mobility + Security E5 license to the finance department users.

D. Configure the sign-in status for the user accounts of the finance department users.

Correct Answer: *A*
You can configure a sign-in risk policy that applies to the Finance department users. The policy can be configured to 'Allow access' but with multi-factor authentication as a requirement.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Create a sign-in risk policy.
2. Create a conditional access policy.
Other incorrect answer options you may see on the exam include the following:
1. Create an activity policy.
2. Create a session policy.
3. Create an app permission policy.
4. Configure the sign-in status for the user accounts of the finance department users.
5. Assign an Enterprise Mobility + Security E5 license to the finance department users.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

fofo1960 Highly Voted 11 months, 3 weeks ago
I guess the real answer is to Create a Conditional Access Policy for the Finance Department.
But in this question there is no such, so assuming that the risky finance user which make the answer A
upvoted 10 times

BoxGhost 5 months, 1 week ago
Yes, it must be a typo as all of the other answers are even more useless. You could argue assigning an E5 license could be helpful if t
are using Azure MFA but they could also just use per user MFA which doesn't require any licenses.
upvoted 2 times

Storm Most Recent 9 months ago
The answer should be conditional access policy. The answer does not make sense...
Sign-in risk is based on heuristic data like:
Users with leaked credentials.
Sign-ins from anonymous IP addresses.
Impossible travel to atypical locations.
Sign-ins from infected devices.
Sign-ins from IP addresses with suspicious activity.
Sign-ins from unfamiliar locations.

We can not decide that the users in the finance department are risky users, or have risky sign-in's...
upvoted 4 times

Question #9 *Topic 4*

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.
Your company purchases Microsoft 365 and creates a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
You plan to install Azure AD connect on a member server and implement pass-through authentication.
You need to prepare the environment for the planned implementation of pass-through authentication.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Modify the email address attribute for each user account.

B. From the Azure portal, add a custom domain name.

C. From Active Directory Domains and Trusts, add a UPN suffix.

D. Modify the User logon name for each user account.

E. From the Azure portal, configure an authentication method.

F. From a domain controller, install an Authentication Agent.

Correct Answer: *BCF*
The on-premise Active Directory domain is named contoso.local. Before you can configure Azure AD Connect, you need to purchase a routable domain, for example, contoso.com.
You then need to add the domain contoso.com to Microsoft as a custom domain name.
The user accounts in the Active Directory domain need to be configured to use the domain name contoso.com as a UPN suffix. You need to add contoso.com to the Active Directory first by using Active Directory Domains and Trusts to add contoso.com add a UPN suffix. You can then configure each account to use the new
UPN suffix.
An Authentication Agent is required on a domain controller to perform the authentication when pass-through authentication is used. When the custom domain and user accounts are configured, you can install and configure Azure AD Connect. An Authentication Agent is installed when you select the pass-through authentication option in the Azure AD Connect configuration or you can install the Authentication Agent manually.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

Kipperson Highly Voted 1 year, 4 months ago
BCD I would think. the Pass through agent should never be installed on a domain controller as best practice and C because the suffix needs to be updated?
upvoted 19 times

MSFrankWu Highly Voted 1 year, 4 months ago
Should this be BCD as the user's UPN suffix need to be update to contoso.com?
upvoted 12 times

joergsi Most Recent 8 months, 1 week ago
Selected Answer: BCD
I would go with the answer provided by Storm!
upvoted 1 times

LillyLiver 8 months, 1 week ago
Selected Answer: BCD
An auth agent on a DC? No, thank you.
upvoted 1 times

ExamTraining24 8 months, 2 weeks ago
Selected Answer: BCD
As explained by others.. PTA agent should not be installed on Domain controllers.
upvoted 1 times

Wojer 8 months, 2 weeks ago

there is nothing about contoso.com so in my opinion, it should be CDF
upvoted 1 times

Storm 9 months ago
BCD
Allthough one could argue that it should be CDF...

B - Because Microsoft never want's us to use onmicrosoft.com
C - Because We need to have a routable domain-name
D - Because All synced users need the routeable domain name as UPN

NOT F - Because
1. Authentication Agents should not be installed on a domain controller
2. Authentication Agents is installed after AD Connect is installed and configured, we are only asked to prepare...
upvoted 4 times

tcmaggio 9 months, 2 weeks ago
Selected Answer: BCD
BCD imho... Question states: prepare! And also, theres no point in installing PTA Agent prior to getting users fully prepared to be synch and that includes configure them with new upn suffix
upvoted 2 times

Jcbrow27 10 months, 2 weeks ago
Selected Answer: BCD
are the correct
upvoted 2 times

thomasimmer 10 months, 2 weeks ago
Selected Answer: CDF
Contoso.local can not be added
upvoted 2 times

fko1978 1 year, 1 month ago
C,D,F. you can try to add contoso.local, but it wouldn't work
upvoted 3 times

Test63126536256316 1 year, 1 month ago
bcd i think
upvoted 1 times

nicoidinfo 1 year, 1 month ago
BCD should be better. Auth agent will be installed with AD Connect. UPN of the users must be changed before install AD Connect
upvoted 1 times

Ash473 1 year, 1 month ago
In Exam today
upvoted 2 times

Ash473 1 year, 1 month ago
in exam today
upvoted 1 times

stromnessian 1 year, 2 months ago
CDF would be right in this case.
upvoted 2 times

Storm 9 months ago
1. Authentication agents should not be installed on domain controllers...
2. Aditional Authentication Agents is added after Passthrough is enabled, we are asked to prepare...
upvoted 1 times

fko1978 1 year, 3 months ago
you cant add contoso.local in 365. nothing in the question is about any other domain. So B wouldnt be right in my opinion.
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company plans to deploy several Microsoft Office 365 services.
You need to design an authentication strategy for the planned deployment. The solution must meet the following requirements:
⇨ Users must be able to authenticate during business hours only.
⇨ Authentication requests must be processed successfully if a single server fails.
⇨ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
⇨ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
Solution: You design an authentication strategy that contains a pass-through authentication model. The solution contains two servers that have an Authentication
Agent installed and password hash synchronization configured.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This solution meets the following goals:
⇨ Users must be able to authenticate during business hours only.
⇨ Authentication requests must be processed successfully if a single server fails.
⇨ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
However, the following goal is not met:
Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
▪
You would need to configure Single-sign on (SSO) to meet the last requirement.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

kanag1 8 months, 3 weeks ago
Doesn't it work with ADFS configuration? Anyways the answer is NO
upvoted 1 times

kanag1 8 months, 3 weeks ago
Passthru with SSO is the answer. Please read the next question.
upvoted 1 times

JEricThomas610 10 months ago
The part about preventing users from logging in was not covered in this solution.
upvoted 1 times

Eric_ 10 months, 3 weeks ago
Question: how does this configuration prevent logons outside business-hours?
upvoted 3 times

sliix 7 months, 3 weeks ago
As PTA uses on-prem AD, you can limit the logins outside business hour by opening the user profile settings in ADUC.
upvoted 2 times

maxustermann 11 months, 1 week ago
Correct, SSO is missing
upvoted 3 times

Luthercrop 1 year, 5 months ago

I agree with the answer

upvoted 2 times

Question #11 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company plans to deploy several Microsoft Office 365 services.
You need to design an authentication strategy for the planned deployment. The solution must meet the following requirements:
☞ Users must be able to authenticate during business hours only.
☞ Authentication requests must be processed successfully if a single server fails.
☞ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
☞ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
Solution: You design an authentication strategy that contains a pass-through authentication model. You install an Authentication Agent on three servers and configure seamless SSO.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
This solution meets all the requirements:
☞ Users must be able to authenticate during business hours only. (This can be configured by using Logon Hours in Active Directory. Pass-through authentication passes authentication to the on-premise Active Directory)
☞ Authentication requests must be processed successfully if a single server fails. (We have Authentication Agents running on three servers)
When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in. (This can be configured in
▪
Active Directory. Pass-through authentication passes authentication to the on-premise Active Directory)
☞ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically. (This goal is met by seamless SSO)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company plans to deploy several Microsoft Office 365 services.
You need to design an authentication strategy for the planned deployment. The solution must meet the following requirements:
⇨ Users must be able to authenticate during business hours only.
⇨ Authentication requests must be processed successfully if a single server fails.
⇨ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
⇨ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
Solution: You design an authentication strategy that uses password hash synchronization and seamless SSO. The solution contains two servers that have an
Authentication Agent installed.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This solution meets the following requirements:
⇨ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
Authentication requests must be processed successfully if a single server fails.
▪
The following requirements are not met:
⇨ Users must be able to authenticate during business hours only.
⇨ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
To meet these two requirements, you would have to configure pass-through authentication.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

joergsi 8 months ago

Selected Answer: B

My checklist would be the following:
=> Two or more AD Connects are needed, 1 active, at least one in staging mode
=> No
=> Passthrough authentication
=> No
=> Seamless SSO
=> Yes

=> (B)

upvoted 1 times

Eric_ 10 months, 3 weeks ago

How strange, here we suddenly do not have logon-times configured, in other questions it was just assumed it was. Inconsistent questioning...

upvoted 2 times

melatocaroca 1 year, 3 months ago

Answer: NO

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Seamless SSO is an opportunistic feature. If it fails for any reason, the user sign-in experience goes back to its regular behavior - i.e, the user needs to enter their password on the sign-in page.

The solution contains two servers that have an Authentication Agent installed is not part of this equation, because are not required in t scenario, SSO for joined domain devices that will sign in Office 365 in an automatic way

Reference:
• https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso
• https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-how-it-works

upvoted 1 times

melatocaroca 1 year, 3 months ago

Forgot, than Users must be able to authenticate during business hours only. no any reference about Group policy configured, so double NO

upvoted 2 times

joergsi 8 months ago

Requirements:
☞ Users must be able to authenticate during business hours only.
☞ Authentication requests must be processed successfully if a single server fails.
=> Two or more AD Connects are needed, 1 active, at least one in staging mode
☞ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in
=> Passthrough authentication
☞ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed automatically.
=> Seamless SSO

My checklist would be the following:
=> Two or more AD Connects are needed, 1 active, at least one in staging mode
=> No
=> Passthrough authentication
=> No
=> Seamless SSO

=> (B)

upvoted 1 times

arai002 1 year, 6 months ago

ANS:No
Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

upvoted 1 times

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location 1	131.107.20.0/24	Yes
Location 2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:

- Users and groups assignment: All users
- Cloud apps assignment: App1
- Conditions: Include all trusted locations
- Grant access: Require multi-factor authentication

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	○	○

Box 1: Yes -

131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.

Box 2: Yes.

131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.
Box 3: Yes.
131.107.5.5 is an MFA Trusted IP so that counts as a Trusted Location in the conditional access policy. The ز€All Trusted Locationsز€ setting includes MFA Trusted
IPs. Therefore, the conditional access policy applies so User2 must use MFA.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Gus01 Highly Voted 1 year, 5 months ago
3rd Box should be no as IP not from Trusted Location so Policy does not apply
Subnet 131.107.5.5 is not in the range of 131.107.50.0/24
upvoted 15 times

dminerva94 1 year, 1 month ago
False, the question states

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.
upvoted 3 times

mitsios96 1 year ago
He is enforced to do so as a user, though
upvoted 2 times

J0J0 1 year, 4 months ago
Regardless, whether that's a typo or what. User2 is enforced to use MFA
upvoted 4 times

rfox321 1 year ago
Wrong - When MFA is enforced PER user, it will enforce MFA regardless.
upvoted 2 times

Storm 9 months ago
You are so wrong ;-)
MFA is enforced exept if user has an IP in a MFA trusted location, in this case 131.107.5.0/24
upvoted 2 times

BoxGhost 5 months, 1 week ago
https://www.petervanderwoude.nl/post/conditional-access-and-named-locations/#:~:text=The%20biggest%20difference%20is%20the,feature%20configuration%20of%20conditional%20access.

Trusted IPs is a feature configuration of multi-factor authentication, while named locations is a feature configuration of conditional access.
upvoted 1 times

morito 3 months, 1 week ago
I dont think thats correct. Per this article from microsoft: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition. Specifically this section: Sign-ins from trusted named locations improve the accuracy of Azure AD Identity Protection's risk calculation, lowering a user's sign-in risk when they authenticate from a location marked as trusted. Additionally, trusted named locations can be targeted in Conditional Access policies.
upvoted 1 times

prepre Highly Voted 1 year, 5 months ago
User 2 has MFA 'ENFORCED' they will always be required to enter it, even if their location doesn't apply to the policy.
upvoted 5 times

bill1982 Most Recent 2 months, 2 weeks ago
Answer is N,Y,Y
All trusted locations are included (not Excluded)- meaning any one from those location and only from those locations will be granted access with condition of Require MFA.
if you have IP other than 131.107.5.0/24 rage then this policy will not apply.
As for User2, MFA is enabled per user basis so will prompt for MFA regardless of condtional Access policy.
upvoted 1 times

Stiobhan 4 months, 1 week ago
Even though User 1 has MFA disabled, the conditional access policy will still apply and require MFA be used. User 1 will need to sort out the disabled status before accessing App1 (raise a ticket with IT 🤣)
upvoted 1 times

Nilz76 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 1 times

lamrandom 8 months, 2 weeks ago

from the documentation:
If needed, you can instead enable each account for per-user Azure AD Multi-Factor Authentication. When users are enabled individually they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remember MFA on trusted devices feature is turned on).
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

so answer 3 is NO.

Also, "Enforced" means that the user has completed the MFA Registration process.:
from the same link:
All users start out Disabled. When you enroll users in per-user Azure AD Multi-Factor Authentication, their state changes to Enabled. W enabled users sign in and complete the registration process, their state changes to Enforced. Administrators may move users between states, including from Enforced to Enabled or Disabled.

upvoted 1 times

kanag1 8 months, 3 weeks ago

The given answer is correct !

upvoted 1 times

fko1978 1 year, 1 month ago

If user 2 wasnt enforced to use MFA the 3rd box should say no, but in this case all boxes are yes

upvoted 3 times

Storm 9 months ago

Wrong - Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.

upvoted 1 times

Nico95 1 year, 1 month ago

key word on the exhibit is: Conditions: "INCLUDE" all trusted locations
That is why answer is YES.
Agreed that in general we do configure trusted location to EXCLUDE from being forced to use MFA, but this was not the Q

upvoted 4 times

itmaster 6 months ago

trusted locations are only 2. This has nothing to do with trusted IPs in MFA settings

upvoted 1 times

spg987 1 year, 1 month ago

In exam today

upvoted 5 times

Nasser 1 year, 1 month ago

The first box should be NO because the MFA feature is disabled for the user1, even if the conditional policy force him to use MFA, but h couldn't because the MFA is not enabled at the first place

upvoted 3 times

Storm 9 months ago

Why comment, when you are just guessing ?

upvoted 2 times

melatocaroca 1 year, 4 months ago

They do tell use that Named locations have been configured to block not included IP ranges, but to create location you need to include one IP range

1 Open the Azure portal and navigate to Azure Active Directory > Conditional access > Named locations;
2 On the Named locations blade, click New location to open the New blade;
3 On the New blade, provide a Name and IP range, and click Create;

https://www.petervanderwoude.nl/post/conditional-access-and-named-locations/

Locations are designated in the Azure portal under Azure Active Directory > Security > Conditional Access > Named locations. These named network locations may include locations like an organization's headquarters network ranges, VPN network ranges, or ranges th you wish to block. Named locations can be defined by IPv4/IPv6 address ranges or by countries.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
https://docs.microsoft.com/en-us/answers/questions/31819/trusted-locations-mfa-conditional-access-not-apply.html

answer should be YES | YES | YES.

upvoted 4 times

F_M 1 year, 4 months ago

Microsoft documentation reports both named locations marked as trusted and MFA Trusted IPs (configured in the MFA external setting page) as "trusted locations". So here the correct answer should be YES | YES | YES.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#all-trusted-locations

upvoted 2 times

cloudboys 1 year, 5 months ago

As mentioned to the questions already stated here " Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IP so that this range is match for statement 3 as well, so the answer will be YES
so finally, YES, YES, YES for all 3 statements

upvoted 3 times

balajim212 1 year, 5 months ago

Multi-factor authentication (MFA) trusted IPs are used to bypass MFA, even if it is using Conditional Access. Unless this IP range is part the Trusted locations, it will not be applied by the CA policy which says "Include trusted locations".

upvoted 2 times

balajim212 1 year, 5 months ago

Hence the answer should be NO here.

upvoted 2 times

Razuli 1 year, 5 months ago

Seems to me the answer is correct: yes, yes, yes. Only because of: Conditionss: Include all trusted locations
⇨ Grant access: Require multi-factor
Please correct me if wrong

upvoted 4 times

TheWallPTA 1 year, 6 months ago

131.107.5.5 is not part of the trusted location...Should be NO.
Correct me if I'm wrong but 131.107.50.0/24 translates to 131.107.50.1 -> 131.107.50.255

upvoted 4 times

Eltooth 1 year, 5 months ago

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.
Note the 3rd octet on this subnet and compare to your statement.

Answer is Yes - MFA enforced.

upvoted 3 times

gladi 1 year, 5 months ago

It's wrong. Subnet 131.107.5.5 is not in the range of 131.107.50.0/24 then should be NO.

upvoted 3 times

PandaTuga 1 year, 3 months ago

read the statements gladi:
- 2nd line (after the first table) "Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs."
- but even if it did not match, the 1st table enforces the user2 to use MFA in any case

upvoted 3 times

itmaster 6 months ago

Enforce means the user has completed the MFA registeration, but it doesn't mean in any case the user will get the MFA eve logged in from trusted IP. Check below reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#:~:text=When%20users%20are%20in%20one%20of%20these%20locations%2C%20there%27s%20no%20Azure 0AD%20Multi%2DFactor%20Authentication%20prompt

upvoted 1 times

joergsi 8 months, 1 week ago

You are wrong, you missed:
Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.
The tenant contains the named locations shown in the following table.

upvoted 1 times

Question #14 *Topic 4*

You have a Microsoft 365 Enterprise E5 subscription.
You need to enforce multi-factor authentication on all cloud-based applications for the users in the finance department.
What should you do?

A. Create an activity policy.

B. Create a new app registration.

C. Create a conditional access policy.

D. Create a session policy.

Correct Answer: *C*
You can configure a conditional access policy that applies to the Finance department users. The policy can be configured to 'Allow access' but with multi-factor authentication as a requirement.
The reference below explains how to create a conditional access policy that requires MFA for all users. To apply the policy to finance users only, you would select
Users and Group in the Include section instead of All Users and then specify the finance department group.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Create a sign-in risk policy.
2. Create a conditional access policy.
Other incorrect answer options you may see on the exam include the following:
1. Create an activity policy.
2. Create a session policy.
3. Create an app permission policy.
4. Configure the sign-in status for the user accounts of the finance department users.
5. Assign an Enterprise Mobility + Security E5 license to the finance department users.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

mitsios96 1 year, 1 month ago
C , is the right answer.
upvoted 3 times

Question #15 *Topic 4*

You have a Microsoft 365 subscription.
Your company deploys an Active Directory Federation Services (AD FS) solution.
You need to configure the environment to audit AD FS user authentication.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From all the AD FS servers, run auditpol.exe.

B. From all the domain controllers, run the Set-AdminAuditLogConfig cmdlet and specify the λ€"LogLevel parameter.

C. On a domain controller, install Azure AD Connect Health for AD DS.

D. From the Azure AD Connect server, run the Register-AzureADConnectHealthSyncAgent cmdlet.

E. On an AD FS server, install Azure AD Connect Health for AD FS.

Correct Answer: *DE*
To audit AD FS user authentication, you need to install Azure AD Connect Health for AD FS. The agent should be installed on an AD FS server. After the installation, you need to register the agent by running the Register-AzureADConnectHealthSyncAgent cmdlet.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-adfs

Player1 Highly Voted 2 years, 6 months ago
+1, should be A, E. See: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#enable-auditing-for-ad-fs

"Register-AzureADConnectHealthSyncAgent" is only necessary if agent registration fails after installing Azure AD Connect.
upvoted 35 times

DenisRossi 3 months ago
You're right!
upvoted 1 times

F_M 1 year, 4 months ago
In addition, "Register-AzureADConnectHealthSyncAgent" is only for the sync service, not for the ADFS one.
upvoted 4 times

ctfalci Highly Voted 2 years, 1 month ago
Answer: D E
Explanation
To audit AD FS user authentication, you need to install Azure AD Connect Health for AD FS. The agent should be installed on an AD FS server. After the installation, you need to register the agent by running theRegister-AzureADConnectHealthSyncAgentcmdlet.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-instal
l
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-adfs
upvoted 8 times

donathon 2 years ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#installing-the-azure-ad-connec
health-agent-for-ad-fs >> E is correct because this is AD FS, the agent should be installed on the ADFS server.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#to-enable-auditing-for-ad-fs-on
windows-server-2008-r2 >> You will then have to enable auditing using auditpol.
D is wrong because this is for Sync not ADFS.
B is wrong because this is not done at the DCs.
C is wrong because the article states ADFS server not DCs.
AD FS server should be different from your Sync server. Do not install AD FS agent to your Sync server.
upvoted 12 times

OneplusOne 1 year, 9 months ago
Donathon is right!

upvoted 2 times

Claire91 Most Recent 2 months, 2 weeks ago

Selected Answer: AE

Explained in this Microsoft Doc

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#enable-auditing-for-ad-fs

upvoted 1 times

LillyLiver 8 months, 1 week ago

Selected Answer: AE

You need to install the audit agent on the ADFS box and enable auditing for it to work.

upvoted 2 times

AlexLiourtas 10 months, 1 week ago

Selected Answer: AE

AE

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-logging

upvoted 2 times

Mulder71 6 months, 2 weeks ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#to-enable-auditing-for-ad-fs-on-windows-server-2012-r2
To enable auditing for AD FS on Windows Server 2012 R2
On the Start screen, open Server Manager, and then open Local Security Policy. Or on the taskbar, open Server Manager, and then select Tools/Local Security Policy.

Go to the Security Settings\Local Policies\User Rights Assignment folder. Then double-click Generate security audits.

On the Local Security Setting tab, verify that the AD FS service account is listed. If it's not listed, then select Add User or Group, and a it to the list. Then select OK.

To enable auditing, open a Command Prompt window with elevated privileges. Then run the following command:

auditpol.exe /set /subcategory:{0CCE9222-69AE-11D9-BED3-505054503030} /failure:enable /success:enable

upvoted 1 times

allesglar 10 months, 3 weeks ago

Selected Answer: AE

Register-AzureADConnectHealthADFSAgent will be executed automatically on the AD FS after installing the agent. Afterwards, audipol needed to activate the logging.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

upvoted 3 times

fofo1960 11 months, 3 weeks ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#to-enable-auditing-for-ad-fs-on-windows-server-2012-r2

To enable auditing for AD FS on Windows Server 2012 R2:
auditpol.exe /set /subcategory:{0CCE9222-69AE-11D9-BED3-505054503030} /failure:enable /success:enable

So Yes, its A and E

upvoted 1 times

zul_n 1 year ago

i'd say the answers are A and E

A. From all the AD FS servers, run auditpol.exe

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#to-enable-auditing-for-ad-fs-on-windows-server-2012-r2

E. On an AD FS server, install Azure AD Connect Health for AD FS.

upvoted 2 times

gonick 1 year ago

A & E. You only need to register if the service failed to do so after installing AAD Connect, as this is part of the process
upvoted 1 times

melatocaroca 1 year, 3 months ago
Correct Answers: A,E

Set-AdfsProperties -AuditLevel None
Auditing is disabled and no events will be logged.
Basic (Default) Set-AdfsProperties -AuditLevel Basic
No more than 5 events will be logged for a single request
Verbose Set-AdfsProperties -AuditLevel Verbose
All events will be logged. This will log a significant amount of information per request.
auditpol.exe.
Open a command prompt with elevated privileges and run the following command to enable auditing auditpol.exe /set /subcategory:"Application Generated" /failure:enable /success:enable

Reference
https://dirteam.com/sander/2019/08/15/howto-enable-auditing-and-logging-for-ad-fs-servers-and-the-ad-fs-farm/
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-logging
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-adfs
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#enable-auditing-for-ad-fs
upvoted 2 times

init2winit 1 year, 5 months ago
+1 for A,E as the valid answer
upvoted 3 times

Davood 1 year, 6 months ago
Correct answer is D,E.
upvoted 2 times

[Removed] 1 year, 8 months ago
Agreed - A and E
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#enable-auditing-for-ad-fs
upvoted 4 times

Rstilekar 1 year, 8 months ago
Correct ones A & E.
D is only required if agent registration fails. Clearly mentioned here - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/h
to-connect-health-agent-install#to-enable-auditing-for-ad-fs-on-windows-server-2016
So D is absolutely out of Question.
upvoted 3 times

mkoprivnj 1 year, 9 months ago
D & E for sure!
upvoted 1 times

VTHAR 1 year, 11 months ago
Answer is A & E. Here below is the exact section in the same link for reference.

A) https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#to-enable-auditing-for-ad-fs-or
windows-server-2016

E) https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#installing-the-azure-ad-connect
health-agent-for-ad-fs
upvoted 4 times

jhawkins28 1 year, 10 months ago
In order for the Usage Analytics feature to gather and analyze data, the Azure AD Connect Health agent needs the information in th
AD FS Audit Logs. These logs are not enabled by default. Use the following procedures to enable AD FS auditing and to locate the AD
audit logs, on your AD FS servers.
A+E for sure!
upvoted 5 times

Jake1 1 year, 10 months ago
Agreed. A & E for sure. You need to install the Health Agent and then to enable auditing, you run auditpol.exe.
upvoted 2 times

shark1 2 years, 3 months ago
A, E https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#installing-the-azure-ad-conne
health-agent-for-ad-fs
upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
⇨ User passwords must be 10 characters or more.
Solution: Implement password hash synchronization and configure password protection in the Azure AD tenant.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This solution meets the following requirement:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable. (this is because the authentication is performed by Azure Active Directory).
This solution does not meet the following requirement:
⇨ Users passwords must be 10 characters or more.
To meet this requirement, you would need to configure the Default Domain Policy in the on-premise Active Directory.
Azure Password Protection can prevent users from using passwords from a 'banned password' list but it cannot be configured to require that passwords must be
10 characters or more.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

grumpypants Highly Voted 3 years, 1 month ago
i think the answer is correct. the password policy from on-premises takes over.
see microsoft: When password hash synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users.
upvoted 19 times

jdean 2 years, 9 months ago
agree, in fact AzureAD doesnt even store the password rather just a sync of the hash. Any password request change requires writeb (if enabled)
upvoted 2 times

moh15 2 years, 1 month ago
then ans is B
upvoted 1 times

DJHASH786 Highly Voted 2 years, 9 months ago
B is the answer as you configure password protection policy in AD not Azure
upvoted 10 times

Cheekypoo Most Recent 2 months ago
Was in my exam today 05/08/22 - along with the other variations of the question.
upvoted 1 times

spg987 1 year, 1 month ago
In exam today
upvoted 3 times

mkoprivnj 1 year, 9 months ago

No for sure!
upvoted 3 times

emil568 2 years, 1 month ago
Password could be applied to AD but is not about length of password it is about complexity of password. So it is B
upvoted 2 times

Fala_Fel 2 years, 8 months ago
Yep correct Answer is B: No
From Microsoft "Password complexity policy - When password hash synchronization is enabled, the password complexity policies in yo
on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use all of the valid
passwords from your on-premises Active Directory instance to access Azure AD services." https://docs.microsoft.com/en-us/azure/activ
directory/hybrid/how-to-connect-password-hash-synchronization
Therefore password protection in Azure will not enforce 10 characters or more.
upvoted 7 times

Goofer 2 years, 8 months ago
It is password policy of on-premise active directory (that will be synced by azure ad connect)
Answer B is correct
upvoted 2 times

Goofer 2 years, 8 months ago
wrong reply
upvoted 1 times

Marz 2 years, 9 months ago
I think the answer is B. To use Azure Password Protection you need to install an agent on the DC. This is not done. So this is wrong. You
would need to configure local GPO to set the minimum PW length to 10 in this case. And it is not mentioned.
upvoted 1 times

Marz 2 years, 9 months ago
See also question 10 of this topic. It supports my idea that the password policy should be set in local AD. Not Azure.
upvoted 4 times

dad032 3 years, 1 month ago
Password hash synchronization and configure password protection is correct, so for me the correct answer is YES.
upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
⇨ User passwords must be 10 characters or more.
Solution: Implement pass-through authentication and modify the password settings from the Default Domain Policy in Active Directory.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This solution does not meet the following requirement:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
This is because with pass-through authentication, the authentication is performed by the on-premise Active Directory.
This solution does meet the following requirement:
⇨ User passwords must be 10 characters or more.
Configuring the Default Domain Policy in the on-premise Active Directory meets the requirement.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

melatocaroca 1 year, 3 months ago
Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable, NO
• Check to ensure that Active Directory is available and is responding to requests from the agents.
User passwords must be 10 characters or more
• Configuring the Default Domain Policy in the on-premise Active Directory meets the requirement. YES

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-pass-through-authentication
upvoted 2 times

wonap 1 year, 5 months ago
should be yes?
upvoted 2 times

lucidgreen 1 year, 5 months ago
PTA requires on-prem AD to be available. So no.
upvoted 6 times

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
A temporary employee at your company uses an email address of user1@outlook.com.
You need to ensure that the temporary employee can sign in to contoso.com by using the user1@outlook.com account.
What should you do?

A. From the Azure Active Directory admin center, create a new user.

B. From the Microsoft 365 admin center, create a new contact.

C. From the Azure Active Directory admin center, create a new guest user.

D. From the Microsoft 365 admin center, create a new user.

Correct Answer: *C*
You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user's account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest user must then redeem their invitation to access resources. An invitation of a user does not expire.
The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question, the external vendor already has a Microsoft account (user1@outlook.com) so he can authenticate using that.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator

jcgonzalez1978 Highly Voted 1 year, 8 months ago
Answer is correct! You can create a Guest user in Azure AD
upvoted 7 times

k9_bern_001 Most Recent 1 month, 1 week ago
correct
upvoted 1 times

Question #19 *Topic 4*

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com that contains 10,000 users.
The company has a Microsoft 365 subscription.
You enable Azure Multi-Factor Authentication (MFA) for all the users in contoso.com.
You run the following query.
search "SigninLogs" | where ResultDescription == "User did not pass the MFA challenge."
The query returns blank results.
You need to ensure that the query returns the expected results.
What should you do?

A. From the Azure Active Directory admin center, configure the diagnostics settings to archive logs to an Azure Storage account.

B. From the Security & Compliance admin center, turn on auditing.

C. From the Security & Compliance admin center, enable Office 365 Analytics.

D. From the Azure Active Directory admin center, configure the diagnostics settings to send logs to an Azure Log Analytics workspace.

Correct Answer: *D*
You can now send audit logs to Azure Log Analytics. This gives you much easier reporting on audit events and the ability to perform queries such as the one in this question.
References:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

PattiD Highly Voted 1 year, 9 months ago
DDDDDDDDDDDDDDDD
upvoted 7 times

melatocaroca Highly Voted 1 year, 3 months ago
Answer D

Integrate Azure AD logs with Log Analytics using Azure Monitor: http://aka.ms/AzureADLogAnalytics
Analyze Azure AD activity logs with Log Analytics, sample queries: https://aka.ms/AzureADLogAnalyticsqueries
Install and use the Log Analytics views for Azure Active Directory: https://aka.ms/AADLogAnalyticsviews
upvoted 5 times

Claire91 Most Recent 2 months, 2 weeks ago
Selected Answer: D
Answer is D:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
upvoted 2 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 3 times

gsmith9897 1 year, 4 months ago
Perhaps all users passed their MFA challenges?
upvoted 4 times

Razuli 1 year, 4 months ago
Doubt it lol
upvoted 7 times

bog23 1 year, 6 months ago
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
upvoted 2 times

mkoprivnj 1 year, 9 months ago
D?? but not sure!

upvoted 2 times

Turak64 1 year, 1 month ago

If you're not sure, either find out or don't comment. It just adds to the confusion

upvoted 18 times

Question #20 *Topic 4*

Your company has a Microsoft 365 subscription that has multi-factor authentication configured for all users.
Users that connect to Microsoft 365 services report that they are prompted for multi-factor authentication multiple times a day.
You need to reduce the number of times the users are prompted for multi-factor authentication on their company-owned devices. Your solution must ensure that users are still prompted for MFA.
What should you do?

A. Enable the multi-factor authentication trusted IPs setting, and then verify each device as a trusted device.

B. Enable the remember multi-factor authentication setting, and then verify each device as a trusted device.

C. Enable the multi-factor authentication trusted IPs setting, and then join all client computers to Microsoft Azure Active Directory (Azure AD).

D. Enable the remember multi-factor authentication setting, and then join all client computers to Microsoft Azure Active Directory (Azure AD).

Correct Answer: *B*
The remember Multi-Factor Authentication feature for devices and browsers that are trusted by the user is a free feature for all Multi-Factor Authentication users.
Users can bypass subsequent verifications for a specified number of days, after they've successfully signed-in to a device by using Multi-Factor Authentication.
The feature enhances usability by minimizing the number of times a user has to perform two-step verification on the same device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

jkklim 9 months, 2 weeks ago
B
https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e
50a0-93b4585e7eb4

https://support.microsoft.com/en-us/account-billing/add-a-trusted-device-to-your-microsoft-account-fe3860c8-bc04-9770-e218-b4fd6b767f4b
upvoted 1 times

jkklim 9 months, 2 weeks ago
B
https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e
50a0-93b4585e7eb4

https://support.microsoft.com/en-us/account-billing/add-a-trusted-device-to-your-microsoft-account-fe3860c8-bc04-9770-e218-b4fd6b767f4b
upvoted 1 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 2 times

Kipperson 1 year, 4 months ago
I would think D. B just verify but what does it actually accomplish? If you select D then you can configure your conditional access to byp
any domain joined devices or mark them as compliant to bypass.
upvoted 2 times

lucidgreen 1 year, 5 months ago
According to the answer description given, both B and D satisfy the requirement of enabling the remember login for x number of days
upvoted 4 times

lucidgreen 1 year, 5 months ago
The difference being that D won't really make a difference.
upvoted 2 times

lucidgreen 1 year, 5 months ago
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication

upvoted 3 times

Tweezle 1 year ago

Correct Answer Should be B. The Link you gave is very clear

upvoted 2 times

chaoscreater 1 year, 3 months ago

If D won't really make a difference, then why did you say both B and D satisfy the requirement? Be consistent.

upvoted 2 times

Turak64 1 year, 1 month ago

It just says company own devices, doesn't say what devices these are

upvoted 1 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You plan to allow the users in your organization to invite external users as guest users to your Microsoft 365 tenant.
You need to prevent the organization's users from inviting guests who have an email address that uses a suffix of @gmail.com.

Correct Answer: *See explanation below.*
You need to add gmail.com as a denied domain in the 'External collaboration settings'.
1. Go to the Azure Active Directory admin center.
2. Select Users then select 'User settings'.
3. Under External Users, select the 'Manage external collaboration settings'.
4. Under 'Collaboration restrictions', select the 'Deny invitations to the specified domains' option.
5. Under, Target Domains, type in the domain name 'gmail.com'
6. Click the Save button at the top of the screen to save your changes.
References:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/allow-deny-list

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You hire a new global administrator named Irvin Sayers to manage your Microsoft 365 tenant.
You need to modify Irvin Sayers to meet the following requirements:
⇨ Uses at least two methods of user authentication
⇨ Has the highest Microsoft Office 365 administrative privileges

Correct Answer: *See explanation below.*
You need to assign the Global Admin role to Irvin Sayers. You then need to configure the account to require Multi-Factor Authentication (MFA).
1. In the Microsoft 365 admin center, select Users then select Active Users.
2. Select the Irvin Sayers account to open the account properties blade.
3. In the Roles section, click on the 'Manage roles' link.
4. Select the 'Admin center access' option.
5. Select Global Administrator then click the 'Save changes' button.
The next step is to enable the account for Multi-Factor Authentication (MFA).
1. If the Irvin Sayers account is selected in the user accounts list, deselect it (click on the tick icon next to the account name). Selecting a user account changes the menu options at the top of the page; deselecting the accounts changes the menu options back.
2. Click on the 'Multi-factor authentication' link at the top of the page.
3. In the 'Multi-factor authentication' page, select the Irvin Sayers account.
4. Click the 'Enable' link on the right side of the page.
5. In the pop-up window, click the 'enable multi-factor auth' button.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
Your company has a web application named App1.
The company plans to publish App1 by using a URL of https://app1.contoso.com.
You need to register App1 to your Microsoft Office 365 tenant.

Correct Answer: *See explanation below.*
You need to register App1 in Azure Active Directory.
1. Go to the Azure Active Directory admin center.
2. Select Azure Active Directory.
3. Select 'App registrations'.
4. Click the 'New registration' link.
5. Enter the name App1.
6. Click the Register button.
7. To add the URL to App1, select App1 in the list of registered apps.
8. In the properties page of App1, select Branding.
9. Enter the URL https://app1.contoso.com in the 'Home page URL' box.
10. Click Save to save the changes.
References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You plan to provide an external user named fabrikamuser@fabrikam.com with access to several resources in your Microsoft 365 tenant.
You need to ensure that the external user can be added to Office 365 groups.

Correct Answer: *See explanation below.*
You need to create a guest account for the external user.
1. Go to the Azure Active Directory admin center.
2. Select Users.
3. Click the 'New guest user' link.
4. Select the 'Invite user' option.
5. Give the account a name and enter fabrikamuser@fabrikam.com in the email address field.
6. Click the 'Invite' button.
References:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/b2b-quickstart-add-guest-users-portal

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You need to ensure that all mobile devices that connect to Microsoft Exchange Online meet the following requirements:
- A password must be used to access the devices.
- Data on the devices must be encrypted.

Correct Answer: *See explanation below.*
You need to modify the default mobile device mailbox policy.
1. Go to the Exchange Admin Center.
2. Select 'mobile' then select 'mobile device mailbox policies'.
3. Click the 'Create a policy' button.
4. Select the Default policy and click the edit icon (pencil icon).
5. Select the 'Security' link to open the security settings.
6. Tick the 'Require a password' checkbox.
7. Tick the 'Require encryption on device' checkbox.
8. Click the Save button to save the changes.

References:
https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You plan to invite several guest users to access the resources in your organization.
You need to ensure that only guests who have an email address that uses the @contoso.com suffix can connect to the resources in your Microsoft 365 tenant.

Correct Answer: *See explanation below.*
You need to add contoso.com as an allowed domain in the 'External collaboration settings'.
1. Go to the Azure Active Directory admin center.
2. Select Users then select 'User settings'.
3. Under External Users, select the 'Manage external collaboration settings'.
4. Under 'Collaboration restrictions', select the 'Allow invitations only to the specified domains (most restrictive)' option.
5. Under, Target Domains, type in the domain name 'contoso.com'
6. Click the Save button at the top of the screen to save your changes.
References:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/allow-deny-list

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You need to prevent non-administrators in your organization from registering applications.

Correct Answer: *See explanation below.*
You need to configure the App Registrations setting in Azure Active Directory.
1. Go to the Azure Active Directory admin center.
2. Select Azure Active Directory.
3. Select 'User settings'
4. In the 'App registrations' section, toggle the 'Users can register applications' setting to No.
5. Click Save to save the changes.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
Your organization recently partnered with another organization named Fabrikam, Inc.
You plan to provide a Microsoft 365 license to an external user named user1@fabrikam.com, and then to share documents with the user.
You need to invite user1@fabrikam.com to access your organization.

Correct Answer: *See explanation below.*
You need to create a guest account for user1.
1. Go to the Azure Active Directory admin center.
2. Select Users.
3. Click the 'New guest user' link.
4. Select the 'Invite user' option.
5. Give the account a name (User1) and enter user1@fabrikam.com in the email address field.
6. Click the 'Invite' button.
References:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/b2b-quickstart-add-guest-users-portal

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You plan to provide several users in your organization with the ability to join their Windows 10 device to Microsoft Azure Active Directory (Azure AD).
You need to ensure that all the users who join a device use multi-factor authentication.

Correct Answer: *See explanation below.*
You need to configure the device settings in Azure Active Directory.
1. Go to the Azure Active Directory admin center.
2. Select Azure Active Directory.
3. Select Devices.
4. Select Device Settings.
5. Toggle the 'Require Multi-Factor Auth to join devices' setting to Yes.
6. Click Save to save the changes.
References:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
You need to prevent the users in your organization from establishing voice calls from Microsoft Skype for Business to external Skype users.

Correct Answer: *See explanation below.*
You need to configure the External Communications settings in the Skype for Business admin center.
1. You need to go to the Skype for Business admin center. If you see a Skype for Business admin center in the admin center list in the Microsoft portal, open it and skip to step 4.
2. If you don't see a Skype for Business admin center in the admin center list in the Microsoft portal, open the Teams admin center.
3. In the Teams admin center, choose Skype > Legacy Portal.
4. In the Skype for Business admin center, select Organization.
5. Select External communications.
6. Untick the 'Let people use Skype for Business to communicate with Skype users outside your organization' checkbox.
7. Click Save to save the changes.

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
⇨ User passwords must be 10 characters or more.
Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This solution does not meet the following requirement:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
This is because with pass-through authentication, the authentication is performed by the on-premise Active Directory.
This solution does not meet the following requirement:
⇨ Users passwords must be 10 characters or more.
To meet this requirement, you would need to configure the Default Domain Policy in the on-premise Active Directory.
Azure Password Protection can prevent users from using passwords from a 'banned password' list but it cannot be configured to require that passwords must be
10 characters or more.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

Goofer Highly Voted 2 years, 8 months ago
PTA checks Active Directory
upvoted 8 times

WoneSix 2 years, 6 months ago
Yes, so the first goal is not achieved.
upvoted 4 times

Jake1 1 year, 10 months ago
Exactly, since the hashed PW is not stored in AAD, it has to talk to AD and if it's not available, you can't auth.
upvoted 2 times

mkoprivnj Most Recent 1 year, 9 months ago
No for sure!
upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory forest.
You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
⇨ User passwords must be 10 characters or more.
Solution: Implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
This solution meets the requirements:
⇨ Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable. (this is because the authentication is performed by Azure Active Directory).
Users passwords must be 10 characters or more. (the Default Domain Policy in the on-premise Active Directory can be configured to require the password
▪ length)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

Your company has three main offices and one branch office. The branch office is used for research.
The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.
You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.
What should you include in the recommendation?

A. Microsoft Azure Active Directory (Azure AD) conditional access.

B. Microsoft Azure Active Directory (Azure AD) password protection.

C. A Microsoft Endpoint Manager device compliance policy.

D. A Microsoft Endpoint Manager device configuration profile.

Correct Answer: *A*
With Azure Active Directory (Azure AD) Conditional Access, you can control how authorized users can access your cloud apps. The location condition of a
Conditional Access policy enables you to tie access controls settings to the network locations of your users.
For this question, we need to configure a location condition in a conditional access policy and apply the policy to users in that location (the branch office). The conditional access policy can be required to 'Allow Access' but 'Required MFA'.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

stoneface 9 months, 1 week ago
Repeated question
upvoted 2 times

venwaik 1 year, 2 months ago
Agree with the answer.
Azure AD>Conditional Access > Policies > open policy > under access controls click "* controls selected" and tick the require multi-facto
authentication box.
upvoted 2 times

Your network contains an Active Directory domain named contoso.com.
All users authenticate by using a third-party authentication solution.
You purchase Microsoft 365 and plan to implement several Microsoft 365 services.
You need to recommend an identity strategy that meets the following requirements:
- Provides seamless SSO
- Minimizes the number of additional servers required to support the solution
- Stores the passwords of all the users in Microsoft Azure Active Directory (Azure AD)
- Ensures that all the users authenticate to Microsoft 365 by using their on-premises user account

You are evaluating the implementation of federation.
Which two requirements are met by using federation? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. minimizes the number of additional servers required to support the solution

B. provides seamless SSO

C. stores the passwords of all the users in Azure AD

D. ensures that all the users authenticate to Microsoft 365 by using their on-premises user account

Correct Answer: *BD*
When you choose this federation as the authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password. AD FS can use on-premise Active Directory as an authentication provider. AD FS can also provide SSO when using Active Directory as an authentication provider.
Incorrect Answers:
A: Additional servers are required to support the AD FS infrastructure.
C: The passwords are not synchronised to Azure AD.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

ctfalci Highly Voted 2 years, 1 month ago
Answer: B D
Explanation
When you choose this federation as the authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password. AD FS can use on-premises Active Directory as an authentication provider. AD FS can also provide SSO when using Active Directory as an authentication provider.
upvoted 20 times

Fegoseen Highly Voted 1 year, 11 months ago
The only possible answer is B and D. A is obviously wrong as with federation you need more infrastructure compared to other authentication methods. C is another very wrong option as with federation authentication Azure AD hands off everything to the authentication agent installed on-premise.

Answer is correct: B D
upvoted 7 times

haazybanj Most Recent 11 months, 3 weeks ago
I don't understand the question and answer options
upvoted 2 times

melatocaroca 1 year, 3 months ago
Correct Answer: B, D

When you choose this federation as the authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password. AD FS can use on-premise Active Directory as an authentication provider. AD FS can also provide SSO when using Active Directory as an authentication provider.

Incorrect Answers:
A: Additional servers are required to support the AD FS infrastructure.
C: The passwords are not synchronized to Azure AD. (Require agents on-premise DC) Password synchronization – Utilizes the password change notification service (PCNS) to capture password changes from Active Directory and propagate them to other connected data sources.

Reference:
https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn
https://samilamppu.com/2019/01/04/from-adfs-to-password-hash-sync-and-seamless-sso/
https://docs.microsoft.com/en-us/microsoft-identity-manager/infrastructure/mim2016-password-management
upvoted 3 times

lucidgreen 1 year, 7 months ago
Two answers required. A&C are out.
upvoted 2 times

lucidgreen 1 year, 6 months ago
Don't be fooled by the imaginary misuse of the term "seamless". "Seamless SSO" is more of a branding/feature offering that uses a couple variations of an authentication technology, depending on the version of Windows. Different types of SSO can be "seamless" i their own ways.
upvoted 5 times

mkoprivnj 1 year, 9 months ago
B & D for sure!
upvoted 3 times

us3r 1 year, 10 months ago
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/set-up-adfs-for-single-sign-on

B is correct
upvoted 2 times

PersonT 2 years ago
Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.
Seamless SSO is not applicable to Active Directory Federation Services (ADFS).
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso
upvoted 2 times

VTHAR 1 year, 11 months ago
Yes, that's right. B is incorrect. It must be C since ADFS requires additional server (recommended) which cross A out.
upvoted 2 times

HAdjerHY 1 year, 5 months ago
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/overview/whats-new-active-directory-federation-services-windows-server
upvoted 1 times

TimurKazan 1 year, 1 month ago
thanks,mate, now AD FS can provide us with Seamless SSO
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company plans to deploy several Microsoft Office 365 services.
You need to design an authentication strategy for the planned deployment. The solution must meet the following requirements:
⇨ Users must be able to authenticate during business hours only.
⇨ Authentication requests must be processed successfully if a single server fails.
⇨ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
⇨ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
Solution: You design an authentication strategy that uses federation authentication by using Active Directory Federation Services (AD FS). The solution contains two AD FS servers and two Web Application Proxies.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This solution meets the following requirements:
⇨ Users must be able to authenticate during business hours only.
⇨ Authentication requests must be processed successfully if a single server fails.
⇨ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
The following requirement is not met:
⇨ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
To meet this requirement, you would need to configure seamless Single Sign-on (SSO)
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

tejb Highly Voted 1 year, 1 month ago
I believe the answer is YES
upvoted 6 times

joergsi Most Recent 8 months ago
Selected Answer: B
Task:
⇨ Users must be able to authenticate during business hours only.
⇨ Authentication requests must be processed successfully if a single server fails.
=> More than 1 connected server required (
⇨ When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in.
=> Passthrough
⇨ Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
=> Seamless SSO

Solution: You design an authentication strategy that uses federation authentication by using Active Directory Federation Services (AD F
The solution contains two AD FS servers and two Web Application Proxies.

Review:
Passthrough with Seamless SSO is missing => FAILED!

(B)
upvoted 3 times

LillyLiver 8 months, 1 week ago
Selected Answer: B

I guessed Yes. After thinking about it, and considering how MS writes their questions, I think the answer is No after all. Nowhere in the question did it say that SSO was enabled. Only that ADFS was deployed as HA. I think the answer is No.

upvoted 3 times

alex_p 5 months, 3 weeks ago

ADFS provides SSO

upvoted 2 times

Jkayx94 8 months, 2 weeks ago

Selected Answer: B

To enable SSO you need to configure Directory Sync to enable SSO to M365. Solution doesn't report this, purely sets up AD FS and connects it to M365.

upvoted 1 times

dumpmaster 8 months, 2 weeks ago

Selected Answer: A

I believe the answer is YES.

upvoted 3 times

melatocaroca 1 year, 3 months ago

Correct Answer: B

This solution meets the following requirements:
Users must be able to authenticate during business hours only. AD on premise policy
OK

Authentication requests must be processed successfully if a single server fails. ADFS farm
OK

When the password for an on-premises user account expires, the new password must be enforced the next time the user signs in. ADF
sync with Azure AD password change notification service (PCNS) (agent installed of on-premise DC), to capture password changes from
Active Directory and propagate them to other connected data sources

The following requirement is not met or yes, but more detailed are required than provides:
Users who connect to Office 365 services from domain-joined devices that are connected to the internal network must be signed in automatically.
Can be if Azure AD password change notification service (PCNS) (agent installed of on-premise DC),

Reference:
https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn
https://docs.microsoft.com/en-us/microsoft-identity-manager/infrastructure/mim2016-password-management

upvoted 1 times

LoremanReturns 1 year, 4 months ago

I believe the right answer is YES. Federation provide the ability to login to Microsoft 365 using SSO from domain-joined devices: https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/set-up-adfs-for-single-sign-on#step-8-configure-the-client-computer-for-single-sign-on. "After you add the Federation server name to the local Intranet zone in Internet Explorer, the NTLM authentication is used when users try to authenticate on the ADFS server. Therefore, they are not prompted to enter their credentials. Administrators can implement Group Policy settings to configure a Single Sign-On solution on client computers that are joined to the domain."

upvoted 4 times

melatocaroca 1 year, 3 months ago

Can be if Azure AD password change notification service (PCNS) (agent installed of on-premise DC), but they do not provide any information about this in the question, so IMHO should YES, with more question info, and NO with the provided question as is, with additional info, no Case study, just plane question

upvoted 1 times

gethisfake 1 year, 4 months ago

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods. Seamless SSO is not applicable to Active Directory Federation Services (ADFS).

upvoted 2 times

TimurKazan 1 year, 1 month ago

that is not correct. please read about what's new in AD FS

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

You create a conditional access policy that has the following configurations:

- Users and groups:
- Include: Group1
- Exclude: Group2
- Cloud apps: Include all cloud apps
- Conditions:
- Include: Any location
- Exclude: Montreal
- Access control: Grant access, Require multi-factor authentication

User1 is on the multi-factor authentication (MFA) blocked users list.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

The Blocked User list is used to block specific users from being able to receive Multi-Factor Authentication requests. Any authentication attempts for blocked users are automatically denied. Users remain blocked for 90 days from the time that they are blocked.

Box 1: Yes -
133.107.10.20 is in the Montreal named location. The conditional access policy excludes Montreal so the policy does not apply. Therefore, User1 can access
Microsoft Office 365.

Box 2: No -
193.77.10.15 is in the Toronto named location. The conditional access policy applies to Group1 which User1 is a member of and all locations except for Montreal.
Therefore, the conditional access policy applies in this case. The policy requires MFA but User1 is on the MFA blocked list so he is unable to use MFA.
Therefore, User1 cannot access Microsoft 365.

Box 3: Yes -
User2 is in Group1 and Group2. The conditional access policy applies to Group1 but excludes Group2. Therefore, the conditional access policy does not apply in this case so User2 can access Microsoft Office 365.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

TimurKazan Highly Voted 1 year, 1 month ago
N-N-Y
User1 is in the blocked list, hence he can not authenticate to any resources
User2 is member of included and excluded group, since exclusion wins over inclusion the policy does not work for him
upvoted 14 times

fko1978 1 year ago
i was thinking that too. User1 (mfa enabled) is in the block list, so no access to anything.
upvoted 2 times

allesglar 11 months, 1 week ago
I also agree. The fact that mfa is enabled for the user means that he will prompted to use mfa next time he sign in. This is but not possible because he is in the block list and therefore wont be able to access any resources. The policy does not play a role.
upvoted 1 times

Sweethaven 2 months, 3 weeks ago
Wrong, User 1 is excluded as its within the Montreal location.
upvoted 1 times

stromnessian Highly Voted 1 year, 2 months ago
Y, N, Y
For 1., User1 does not have MFA enforced but is on the MFA block list, but as Montreal is excluded from the CA policy, MFA is not requir
so an MFA challenge will not have to be sent to User1.
upvoted 9 times

allesglar 11 months, 1 week ago
If needed, you can instead enable each account for per-user Azure AD Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remember MFA on trusted devices feature is turned on).
So 1) is N. He has to use mfa but he cannot because he is in the block list.
upvoted 1 times

Nilz76 Most Recent 6 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 1 times

Durden871 7 months, 1 week ago
I had said YNY, but my reasoning for Y on box 3 seems to contradict the answer provided. I thought most restrictive policy would win? I
this case, both groups are applied. The location is on the grant access and user 2 has MFA enforced. Which is it? Did the policy allow us
because of the group exclusion or did it allow user 2 because they met the criteria of the CA?
upvoted 1 times

joergsi 8 months ago
A confusing resolution was provided:
The Blocked User list is used to block specific users from being able to receive Multi-Factor Authentication requests. Any authentication
attempts for blocked users are automatically denied. Users remain blocked for 90 days from the time that they are blocked.

In the scenario:
User1 is on the multi-factor authentication (MFA) blocked users list.
=> This would mean, that User1 can't use MFA for 90 days.

In this case, why is question 1 Yes?

Shouldn't it be N/N/Y?
upvoted 1 times

melatocaroca 1 year, 3 months ago
iMHO

Answer: N, Y,Y

Conditional Access policy to work. User based mfa vs Conditional access mfa
If user-based MFA is enabled, it will override the Conditional Access policies
extremely important to note, is that if you enable MFA via the MFA portal,
you completely rub out the ability to utilize Conditional Access Policies.
You must have the Azure MFA user state set to disabled,
and a Conditional Access policy configured to require multi factor authentication for Conditional Access policy-based settings to apply

https://messageops.com/user-based-mfa-vs-conditional-access-mfa/
https://jkindon.com/2018/08/12/azure-mfa-vs-conditional-access/
upvoted 2 times

melatocaroca 1 year, 3 months ago
Sorry typo error

Answer: N, N, Y
upvoted 4 times

melatocaroca 1 year, 3 months ago
Box 1: No
User 1 133.107.10.20 Montreal location. Montreal, policy does not apply. User1 can access, because per user setting is set to requ
MFA, and user policy have priority, over policy

Box 2: No
193.77.10.15 Toronto location. The conditional access policy applies to Group1 which User1 is a member of and all locations exce
for Montreal, requires MFA, User1 is on the MFA blocked list, per user setting is MFA enabled. User1 cannot access Microsoft 365

Box 3: Yes -
User2 is in Group1 and Group2. The conditional access policy applies to Group1 but excludes Group2. Therefore, the conditional
access policy does not apply in this case and because User2 per user setting is enforced to use MFA can access Microsoft Office 3

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings
https://messageops.com/user-based-mfa-vs-conditional-access-mfa/
https://jkindon.com/2018/08/12/azure-mfa-vs-conditional-access/
upvoted 3 times

chaoscreater 1 year, 3 months ago
What are you on about? The policy doesn't apply to Montreal and so user 1 CAN access. Box 1 is YES.
upvoted 2 times

michszym 1 year, 2 months ago
I test it - when I've enabled MFA for User1 and added him to "block list" I cannot log on - cannot send text message during
logon.
As melatocaroca wrote, user-based MFA has a priority over conditional access policy
upvoted 3 times

Azreal_75 1 year, 1 month ago
I stand to be corrected but.....

MFA is not enforced for User 1 - just Enabled so he doesn't need to use MFA, furthermore as chaoscreater says the
Condiitional Access Policy does not apply to logins from Montreal - the answer is therfore yes for box 1.

For box 2 User 1 is now logging in from a location that Conditional Access does apply and MFA is required hence No.

I find the answer to Box 3 perplexing, in so many other areas of O365 the most restrictive policy applies but in Condition
Access that doesn't seem to be the case since being in Group 2 excludes the user from CA despite being in Group 1 as w
upvoted 1 times

michszym 1 year, 3 months ago

Box 1: No? you wrote:"User 1 can access" - I think he can acces but require MFA (so should be YES)

upvoted 1 times

michszym 1 year, 3 months ago

sorry, it's No because User1 is on Blocked User List and he can't receive MFA request

upvoted 2 times

Question #37 *Topic 4*

Your network contains an Active Directory domain named contoso.com. The domain contains five domain controllers.
You purchase Microsoft 365 and plan to implement several Microsoft 365 services.
You need to identify an authentication strategy for the planned Microsoft 365 deployment. The solution must meet the following requirements:
- Ensure that users can access Microsoft 365 by using their on-premises credentials.
- Use the existing server infrastructure only.
- Store all user passwords on-premises only.
- Be highly available.

Which authentication strategy should you identify?

A. pass-through authentication and seamless SSO

B. pass-through authentication and seamless SSO with password hash synchronization

C. password hash synchronization and seamless SSO

D. federation

Correct Answer: *A*
Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.
Incorrect Answers:
B: Password hash synchronization replicates passwords to Azure Active Directory. This does not meet the following requirement: Store all user passwords on- premises only
C: Password hash synchronization replicates passwords to Azure Active Directory. This does not meet the following requirement: Store all user passwords on- premises only
D: Federation requires additional servers running Active Directory Federation Services. This does not meet the following requirement: Use the existing server infrastructure only.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/choose-ad-authn

ctfalci Highly Voted 2 years, 1 month ago
Answer: A
Explanation
Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, wh ensures that the password validation doesn't happen in the cloud.
upvoted 15 times

Beowulf Highly Voted 2 years, 4 months ago
"A" is correct answer.
Reason: This solution is appropriate when your organization is constrained from allowing any form of password synchronization to the cloud. This may include being restricted from allowing cryptographic hashes of passwords to be stored in the cloud
upvoted 6 times

haazybanj Most Recent 1 year ago
Having 5 Domain controllers makes it highly available. I will go for A.
upvoted 1 times

tejb 1 year, 1 month ago
The correct answer is B.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

As a DR mode, Microsoft recommends Pass through Authentication + Password Sync...in case PTA Agents are not available, Password h sync kicks in! I had a discussion with Microsoft guys and this is what they recommended
upvoted 3 times

MomoLomo 1 year, 1 month ago

https://docs.microsoft.com/en-us/microsoft-365/enterprise/plan-for-directory-synchronization?view=o365-worldwide

When passwords are changed or reset on-premises, the new password hashes are synchronized to Azure AD so that your users can always use the same password for cloud resources and on-premises resources. The user passwords are never sent to Azure AD or stored in Azure AD in clear text. Some premium features of Azure AD, such as Identity Protection, require PHS regardless of which authentication method is selected.

So technically speaking passwords are not saved in the cloud and with PTA sure thing it's highly available

I agree with you

upvoted 1 times

lucidgreen 1 year, 7 months ago

Disregard everything I've said. PtH w/ SSO is the way to go. All the others require some form of additional infrastructure.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 2 times

lucidgreen 1 year, 6 months ago

Passthrough Authentication can be implemented using existing servers, which would satisfy all the requirements when the agent is installed on multiple servers, all with access to domain controllers and outbound access. The advantage over PtH is that it doesn't require you to store the hash of your hashed AD password on other servers. So A is a possiblity.

upvoted 2 times

shaan6810 1 year, 9 months ago

the word "highly available" is tripping me up.
Technically, answer should be C because PHS is the only one that is referenced as "highly available" in MS docs:
Use or enable password hash synchronization for whichever authentication method you choose, for the following reasons: High availability and disaster recovery. Pass-through Authentication and federation rely on on-premises infrastructure. For pass-through authentication, the on-premises footprint includes the server hardware and networking the Pass-through Authentication agents requir
For federation, the on-premises footprint is even larger. It requires servers in your perimeter network to proxy authentication requests and the internal federation servers.

PTA is more available than Federated, and PHS is more available than PTA - but at the same time, if this question is poorly worded and storing the hash in the cloud is considered as storing the password in the cloud, then PTA with SSSO would be the answer.

upvoted 5 times

jodtzz 11 months, 3 weeks ago

I agree. Question is just unfair.

upvoted 1 times

mkoprivnj 1 year, 9 months ago

A for sure!

upvoted 2 times

techtest848 1 year, 10 months ago

Ensure that users can access Microsoft 365 by using their on-premises credentials > Requires password hash sync
Use the existing server infrastructure only > PTA (with installing authentication agent on DCs)
Store all user passwords on-premises only > This is satisfied by password hash sync anyway as the passwords synced from on-prem AD Azure AD are only hashes
Be highly available > with password hash, you can login to Microsoft services even if the DC/PTA is not accessible and also PTA agent ca be installed on multiple DCs to provide redundancy

I think the answer is B

upvoted 1 times

melatocaroca 1 year, 3 months ago

Not asking for additional or HBA authentication, so I feel B can be discarded

upvoted 1 times

Faheem2020 1 year, 10 months ago

Option A- "pass-through authentication and seamless SSO" ticks all the boxes as per below link and there is no need to consider other solutions

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

upvoted 2 times

melatocaroca 1 year, 3 months ago

C: Password hash synchronization Active Directory password hash from Active Directory is synchronized into Azure AD. This does no meet the following requirement: Store all user passwords on- premises only, store password hash not the password

upvoted 1 times

jhawkins28 1 year, 10 months ago

I believe it's a tricky question, however the answer is B.
It states 5 domain controllers and MS, says 3 or more servers with AD Connect is the best option for Pass-through, which is using their existing server configuration. Password Hash gives the High Availability, which doesn't store on Azure, it needs to be decrypted once more, but still only sees the hash which cannot be reverted.

upvoted 2 times

Jayatheerthan 1 year, 11 months ago

Password Hash Sync. This was the recommendation from Microsoft for High availability or On-premises outage survival or Identity protection. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 2 times

scottims 1 year, 11 months ago

Agree with Kazaki that C should be correct. From the link provided

"Avoid outages by using password hash synchronization because the Microsoft Azure AD cloud authentication service scales globally a is always available."

upvoted 1 times

kazaki 2 years, 3 months ago

i just passed the test today if high availability is mentioned then we need pass Hash sync
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 3 times

lucidgreen 1 year, 7 months ago

Pass the hash stores the hash of the credentials off prem. It can be highly available but if you want your credentials to only be acces locally, PtH wouldn't be the answer.

upvoted 2 times

kmjunk 2 years, 3 months ago

How does answer A meet the 'highly available' requirement? If O365 cannot forward authentication requests to the ADDS. For me the answers do not meet the requirements. In my opinion the answer should be PHS and SSO. Passwords are stored on-premise and the h is syn'd which meets the requirements. Have I got this wrong?

upvoted 4 times

Myko 2 years, 3 months ago

You have 5 domain controllers where you can run additional standalone Authentication Agents, to achieve high availability.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start
PHS does not meet the requirement of using on-premises credentials.

upvoted 4 times

[Removed] 1 year, 9 months ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta#key-benefits-of-using-azure-ad-pass-throug authentication

upvoted 1 times

Fcnet 2 years, 4 months ago

with Adfs you can install ADFS server on DC so the solution for me is
Federation
https://docs.microsoft.com/en-us/previous-versions/azure/azure-services/dn151324(v=azure.100)?redirectedfrom=MSDN

upvoted 1 times

Fcnet 2 years, 4 months ago

oups i forgot ! sorry users should use their credential to connect to O365 that's not possible with Adfs ! so A is the right answer in th case :)

upvoted 2 times

Fcnet 2 years, 4 months ago

"Ensure that users can access Microsoft 365 by using their on-premises credentials."
and store their password on premise,
again with Adfs you can do that so right answer should be Federation

upvoted 2 times

gummby8 2 years, 3 months ago

Federation needs a proxy, which can't be a DC. so it does not meet the "existing infrastructure only" requirement. Not sure I would call ADFS high availability either, but that is my personal beef with ADFS

upvoted 2 times

lucidgreen 1 year, 7 months ago

In order for ADFS to be highly available, you would need to install multiple ADFS servers in a farm. I wouldn't recommend t on a Domain Controller. The idea is that you have a main federation server that acts as the master where all configuration i

done. The rest just replicate the configuration.
So it can be done, but if you need to use the existing hardware only, then no. Unless you already have an AD FS farm.

upvoted 1 times

Fcnet 2 years, 4 months ago

Federation
would be more highly avalailable than adconnect ...
you can have Afds proxy + Adfs serverS you can have only ONE adconnect server, Adconnect is not a solution highly available

upvoted 2 times

Fcnet 2 years, 4 months ago

oups i forgot ! sorry users should use their credential to connect to O365 that's not possible with Adfs ! so A is the right answer in th case :)

upvoted 2 times

Fcnet 2 years, 4 months ago

"Ensure that users can access Microsoft 365 by using their on-premises credentials."
and store their password on premise,
again with Adfs you can do that so right answer should be Federation

upvoted 2 times

donathon 2 years ago

This will require additional infrastructure which is ADFS.

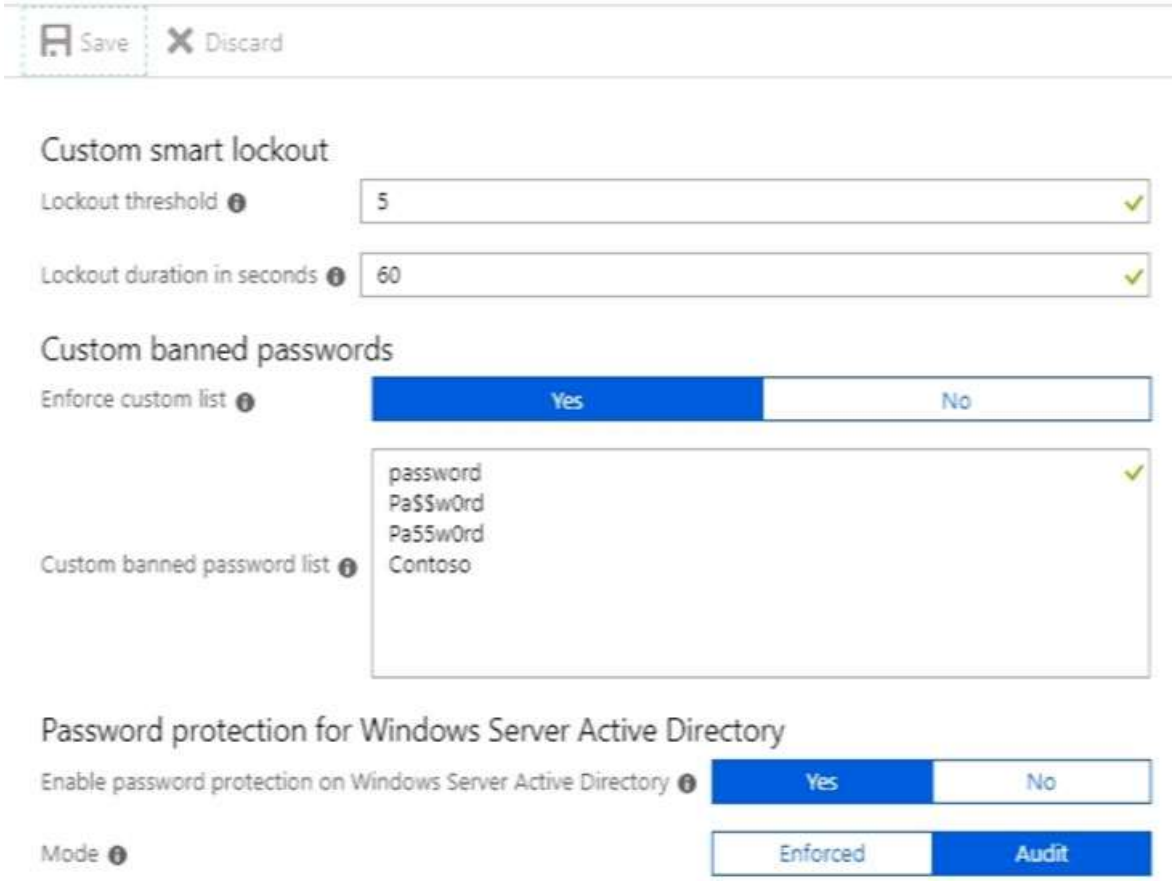
upvoted 1 times

Davidf 2 years, 4 months ago

The real question here is, are MS counting a hash of the password the same as the password? I'd be inclined to say and go with A

upvoted 5 times

Your network contains an on-premises Active Directory domain.
You have a Microsoft 365 subscription.
You implement a directory synchronization solution that uses pass-through authentication.
You configure Microsoft Azure Active Directory (Azure AD) smart lockout as shown in the following exhibit.



You discover that Active Directory users can use the passwords in the custom banned passwords list.
You need to ensure that banned passwords are effective for all users.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From a domain controller, install the Azure AD Password Protection Proxy.

B. From a domain controller, install the Microsoft AAD Application Proxy connector.

C. From Custom banned passwords, modify the Enforce custom list setting.

D. From Password protection for Windows Server Active Directory, modify the Mode setting.

E. From all the domain controllers, install the Azure AD Password Protection DC Agent.

F. From Active Directory, modify the Default Domain Policy.

Correct Answer: *ADE*
Azure AD password protection is a feature that enhances password policies in an organization. On-premises deployment of password protection uses both the global and custom banned-password lists that are stored in Azure AD. It does the same checks on-premises as Azure AD does for cloud-based changes. These checks are performed during password changes and password reset scenarios.
You need to install the Azure AD Password Protection Proxy on a domain controller and install the Azure AD Password Protection DC Agent on all domain controllers. When the proxy and agent are installed and configured, Azure AD password protection will work.
In the exhibit, the password protection is configured in Audit mode. This is used for testing. To enforce the configured policy, you need to set the password protection setting to Enforced.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Goofer Highly Voted 2 years, 7 months ago

The answers are: ADE

upvoted 25 times

PumbaMunich Highly Voted 3 years, 1 month ago

The right answer should include D and exclude C. There was no request of adding any password to the banned list, but rather to make sure that those existing in the banned list do not get used. Therefore the list should be enforced, making one of the right actions D rat than C.

upvoted 24 times

charat 4 months, 1 week ago

I'm afraid that's incorrect. ADE are correct. The setting for banned list is already enforced according to the screenshot

upvoted 1 times

Cheekypoo Most Recent 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Stiobhan 4 months, 1 week ago

Defo A&D, just not sure E is neccessary! But there you go!

upvoted 1 times

charat 4 months, 1 week ago

On exam 05/22/22. Great question!

upvoted 2 times

joergsi 8 months, 1 week ago

Of Topic Question to the other user, have you tried the following, copy the text of a question in google, and you will find out that there several other providers in the internet with exactly the same question and answer combinations.
Based on this, my suspicion was, that every "provider" is using the same source.
If you check out the watermark of the image, you will see, that the source is Prepaway :)!

upvoted 1 times

jjong 1 year ago

in exam today

upvoted 4 times

Ash473 1 year, 1 month ago

In exam today

upvoted 3 times

Mbewu 1 year, 1 month ago

how was it?

upvoted 1 times

mkoprivnj 1 year, 9 months ago

ADE is correct!

upvoted 3 times

Alvaroll 2 years ago

3-14 https://www.examtopics.com/exams/microsoft/ms-100/view/19/

upvoted 2 times

STFN2019 2 years, 2 months ago

ade it is

upvoted 3 times

JaBe 2 years, 3 months ago

A D E although the AD Password Protection Proxy is installed on a member server, not a DC (see diagram in answer link).

upvoted 8 times

ilRobi 1 year, 1 month ago

I agree, MS even recommends at least 2 Proxies per forest on member servers, not on a DC "because it would need internet connectivity and that may be a security concern".

upvoted 3 times

shark1 2 years, 3 months ago

A, D, E

This is duplicated question.

upvoted 7 times

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that includes a user named User1.

You enable multi-factor authentication for contoso.com and configure the following two fraud alert settings:

- Set Allow users to submit fraud alerts: On
- Automatically block users who report fraud: On

You need to instruct the users in your organization to use the fraud reporting features correctly.

What should you tell the users to do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

A user can report fraud on her account by: [▼]
- Typing a special code after receiving an alert call
- Sending an email message to an administrator
- Using the Microsoft Authenticator app

If User1 reports fraud on his account, the account will be blocked automatically for: [▼]
- 6 hours
- 1 day
- 7 days
- 90 days

Correct Answer:

Answer Area

A user can report fraud on her account by: [▼]
- Typing a special code after receiving an alert call
- Sending an email message to an administrator
- Using the Microsoft Authenticator app

If User1 reports fraud on his account, the account will be blocked automatically for: [▼]
- 6 hours
- 1 day
- 7 days
- 90 days

Code to report fraud during initial greeting: When users receive a phone call to perform two-step verification, they normally press # to confirm their sign-in. To report fraud, the user enters a code before pressing #. This code is 0 by default, but you can customize it.

Block user when fraud is reported: If a user reports fraud, their account is blocked for 90 days or until an administrator unblocks their account. An administrator can review sign-ins by using the sign-in report, and take appropriate action to prevent future fraud. An administrator can then unblock the user's account.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert

itworxx Highly Voted 2 years, 3 months ago

Using the authenticator app
90 days

upvoted 15 times

TonySuccess Highly Voted 2 years, 3 months ago

Yeah, pretty sure if this question appeared in a more current version of this exam, it would be:

Using the Authenticator App
90 Days

upvoted 10 times

TonySuccess 2 years, 3 months ago

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#:~:text=The%20fraud%20alert%20feature%20lets,app%20or%20through%20their%20phone.&text=An%20administrator%20can%20then%20unblock%20the%20user's%20account.

upvoted 2 times

Nico95 Most Recent 1 year, 1 month ago

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.

From :
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

upvoted 1 times

joergsi 8 months, 1 week ago

In this case, two of the provided answers are correct! But which one does MSFT want to see?

upvoted 1 times

densyo 1 year, 3 months ago

users can report the fraud attempt using the Microsoft Authenticator app or through their phone.

upvoted 5 times

Nico95 1 year, 1 month ago

Exact
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

upvoted 2 times

mkoprivnj 1 year, 9 months ago

MS auth app + 90 days.

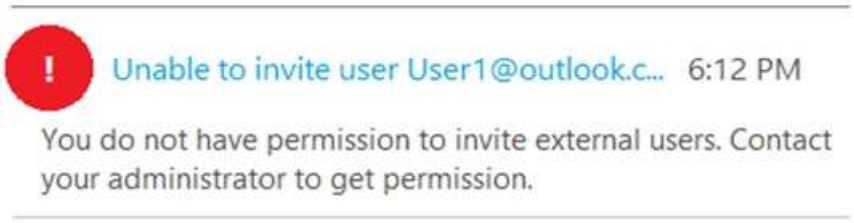
upvoted 4 times

Alvaroll 2 years ago

3-15 https://www.examtopics.com/exams/microsoft/ms-100/view/19/

upvoted 2 times

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
An external user has a Microsoft account that uses an email address of user1@outlook.com.
An administrator named Admin1 attempts to create a user account for the external user and receives the error message shown in the following exhibit.



You need to ensure that Admin1 can add the user.
What should you do from the Azure Active Directory admin center?

A. Add a custom domain name named outlook.com.

B. Modify the Authentication methods.

C. Modify the External collaboration settings.

D. Assign Admin1 the Security administrator role.

Correct Answer: *C*
In the External Collaboration settings, you can set the following invitation policies:
- Turn off invitations
- Only admins and users in the Guest Inviter role can invite
- Admins, the Guest Inviter role, and members can invite
- All users, including guests, can invite

In this question, an Admin user is unable to invite the guest user. This suggests that invitations are turned off altogether.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/delegate-invitations

mkoprivnj Highly Voted 1 year, 9 months ago
C for sure!
upvoted 6 times

samjohnjohn Most Recent 1 year, 2 months ago
https://docs.microsoft.com/en-us/azure/active-directory/b2b/delegate-invitations
upvoted 1 times

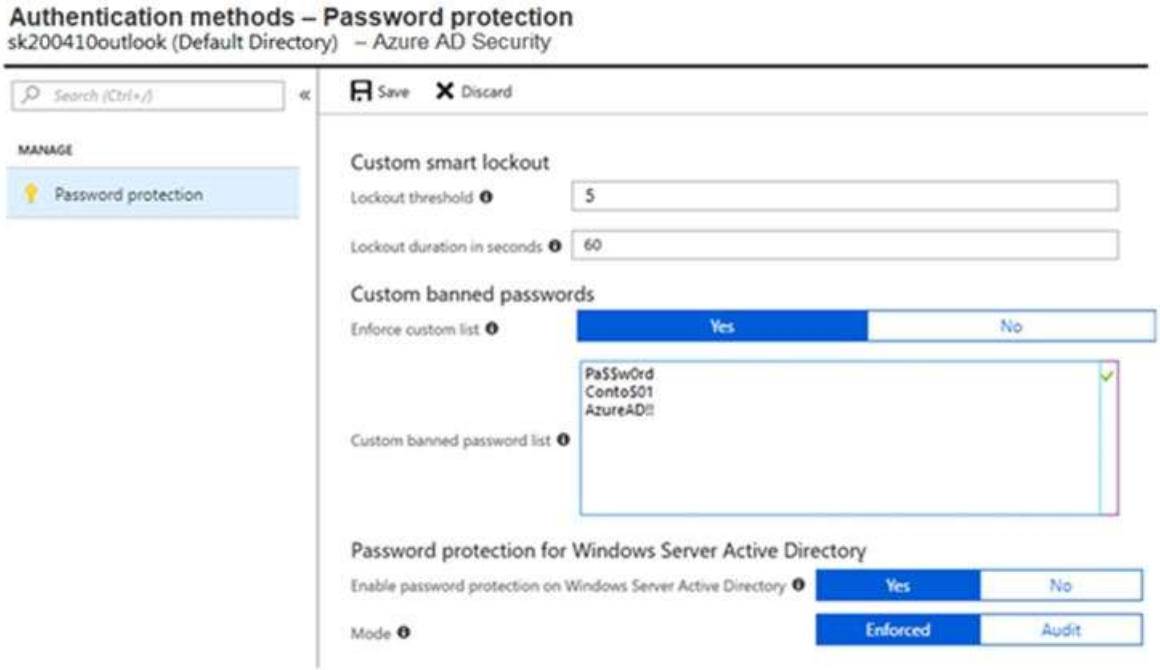
Alvaroll 2 years ago
3-16 https://www.examtopics.com/exams/microsoft/ms-100/view/19/
upvoted 2 times

Dimonchik 2 years, 1 month ago
Ref: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-external-users#chec
guest-collaboration-settings
upvoted 1 times

HOTSPOT -

You have a Microsoft 365 Enterprise E5 subscription.

You create a password policy as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If users are locked out of their account, they have [**answer choice**].

- five sign-in attempts each subsequent minute
- one sign-in attempt each subsequent minute
- five sign-in attempts every five minutes
- one sign-in attempt every five minutes

Users can create a password of [**answer choice**].

- PasswordPa55w.rd
- Conto$01Pa$$word
- AzureAD!!111
- pa$$w0rd

Correct Answer:

Answer Area

If users are locked out of their account, they have [**answer choice**].

- five sign-in attempts each subsequent minute
- **one sign-in attempt each subsequent minute**
- five sign-in attempts every five minutes
- one sign-in attempt every five minutes

Users can create a password of [**answer choice**].

- **PasswordPa55w.rd**
- Conto$01Pa$$word
- AzureAD!!111
- pa$$w0rd

By default, smart lockout locks the account from sign-in attempts for one minute after 10 failed attempts. In this question, the lockout threshold if 5 failed attempts.

The account locks again after each subsequent failed sign-in attempt, for one minute at first and longer in subsequent attempts.

Password evaluation goes through several steps including normalization and Substring matching which is used on the normalized password to

check for the user's first and last name as well as the tenant name.
The next step is to identify all instances of banned passwords in the user's normalized new password. Then:
1. Each banned password that is found in a user's password is given one point.
2. Each remaining unique character is given one point.
3. A password must be at least five (5) points for it to be accepted.
Conto$01Pa$$word contains two banned passwords and no remaining unique characters so is given a score of 2 points. This is less than the required 5 points so will be rejected.
Pa$$w0rd contains a banned password and no remaining unique characters so is given a score of 1 point. This is less than the required 5 points so will be rejected.
AzureAD!!111 contains a banned password (AzureAD!!) and has three remaining characters. However, the remaining characters are all the same (they're all 1s) so that is only one unique character. So that password will be given a score of 2. One for the banned password and 1 for the unique character. This is less than the required 5 points so will be rejected.
PasswordPa55w.rd does not contain a banned password. PasswordPa55w.rd contains 16 characters. However, there are two 'P', two 'a', two 's', two 'w', two 'r', two 'd', and two '5' so there are 9 unique characters. Therefore, the password will be given a score of 9 points. This is more than the required 5 points so the password will be accepted.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

Moderator 2 months ago
Still a valid question (July 30th 2022).
upvoted 1 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 2 times

Eggsamine 11 months, 2 weeks ago
Agree with the answer, just thought I would add that the custom banned passwords list is case-insensitive, so Pa$$w0rd is the same as pa$$w0rd:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection#:~:text=The%20custom%20banned%20password%20list%20is%20case-insensitive
upvoted 3 times

TimurKazan 1 year, 1 month ago
correct
upvoted 2 times

Azreal_75 1 year, 1 month ago
I have a query, in the given answer it says: "PasswordPa55w.rd does not contain a banned password."

Am I being thick or is that incorrect?

The first part of the p/w is Password - in the banned passwords list is Pa$$w0rd. After normalisation would that not equate to Passwor
Or is normalisation only done on the entered passwords and not the ones in the banned password list?
upvoted 2 times

MigrationEndpoint 1 year, 5 months ago
"If the first sign-in after a lockout also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases."
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout
upvoted 2 times

Gus01 1 year, 5 months ago
Yes 5 Sign in Attempts after every minute is the correct answer
upvoted 2 times

dsiisus 1 year, 3 months ago
vikingSWE is correct
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout
upvoted 1 times

VikingSWE 1 year, 4 months ago
No it is not. After the first lockout, the user gets only one try per lockout duration.

upvoted 5 times

joergsi 8 months, 1 week ago

one sign-in attempt every minute, after 5 fails the account will be blocked! In your case, the user can sign in 5 times within 1 Minute

upvoted 1 times

TheWallPTA 1 year, 5 months ago

Lockout Threshold =
How many failed sign-ins are allowed on an account before its first lockout. If the first sign-in after a lockout also fails, the account lock out again.
Lockout duration in seconds =
The minimum length in seconds of each lockout. If an account locks repeatedly, this duration increases.
So I think it should be: 5 Signin Attempts each Minute.

upvoted 1 times

VikingSWE 1 year, 4 months ago

No. After the first lockout, the user gets only one try per lockout duration.

upvoted 5 times

subbuhotmail 1 year, 2 months ago

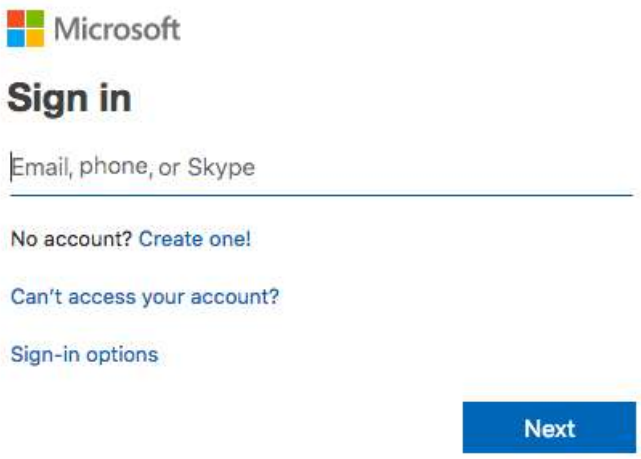
S0 basically,
1. If users attempts 5 wrong password then it will lock. --> Locked
2. After 60 seconds, lock released.
3. If user enter wrong password , then in the 1st attempt after lockout ---> it will lock again.
4. If user enter correct password then all reset to normal again.

upvoted 6 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



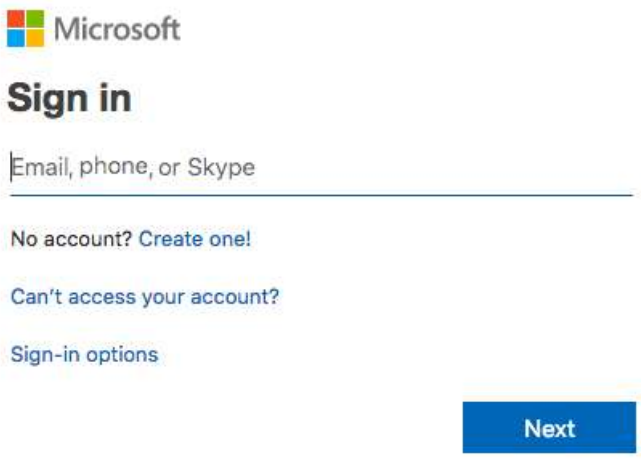
You need to ensure that when Lynne Robbins attempts to sign in to the Microsoft Office 365 portal, Lynne Robbins is prompted to authenticate by using multiple methods.
To answer, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*
You need to enable Multi-Factor Authentication for Lynne Robbins.
1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Users section and select Active Users.
3. Click the 'Multi-factor authentication' link.
4. Select Lynne Robbins.
5. In the right navigation pane, select the 'Enable' link to enable MFA for the account.
6. Confirm the setting by clicking the 'Enable multi-factor authentication' button.
7. Click the Close button to close the confirmation window.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to create a SharePoint site named Project1. Users from your organization must be able to share content from the site to external users.
To answer, sign in to the Microsoft 365 portal.

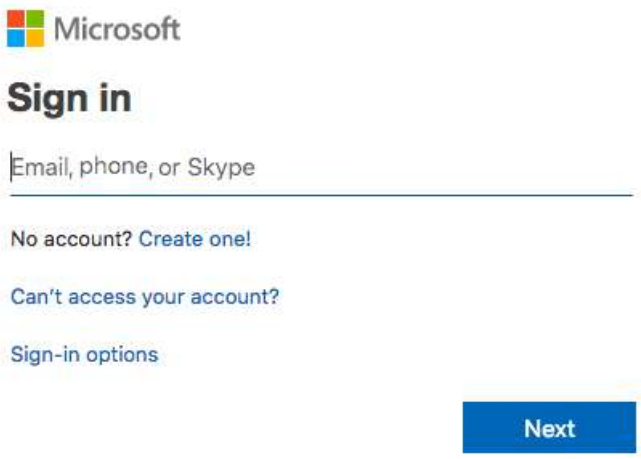
Correct Answer: *See explanation below.*
You need to create a SharePoint site and configure the sharing settings.
1. Go to the SharePoint Admin Center.
2. In the left navigation pane, expand Sites then select 'Active Sites'.
3. Click on the '+ Create' link to add a new site.
4. Select 'Other Options' then 'Team Site' for the template.
5. Give the site the name 'Project1'.
6. In the 'Primary Administrator' field, start typing 'admin' then select the admin@LODSe878763.onmicrosoft.com account when it appears.
7. Click Finish to create the site.
8. In the Active Sites list, select the Project1 site.

9. Click the Sharing link at the top of the sites list.
10. Under 'External Sharing', select 'Anyone'.
11. Click Save to save the changes.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



You need to ensure that an external user named dev@fabrikam.com can register an application in your Microsoft 365 tenant. The solution must use the principle of least privilege.
To answer, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*
You need to create a guest account for the external user and assign the Application Developer role. As the user's domain is an external domain, you will need to
'invite' the user. The external user will need to accept the invitation to create the account.
1. Go to the Azure Active Directory Admin Center.
2. In the left navigation pane, select Users.
3. Click on the '+ New Guest User' link.
4. Ensure that the 'Invite user' option is selected.
5. Enter dev@fabrikam.com in the email address field.

6. In the Roles section, 'user' will be selected by default. Click on 'user' to open a list of roles.
7. Select Application Developer in the list and click the 'Select' button to assign the role.
8. Click the 'Invite' button to send the invitation.

Question #45 *Topic 4*

Your company has a Microsoft 365 subscription and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
An external vendor has a Microsoft account that has a username of user1@outlook.com.
You plan to provide user1@outlook.com with access to several resources in the subscription.
You need to add the external user account to contoso.onmicrosoft.com. The solution must ensure that the external vendor can authenticate by using user1@outlook.com.
What should you do?

A. From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify ג€"UserPrincipalName user1@outlook.com.

B. From the Microsoft 365 admin center, add a contact, and then specify user1@outlook.com as the email address.

C. From the Azure portal, add a new guest user, and then specify user1@outlook.com as the email address.

D. From the Azure portal, add a custom domain name, and then create a new Azure AD user and use user1@outlook.com as the username.

Correct Answer: *C*
You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user's account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest user must then redeem their invitation to access resources. An invitation of a user does not expire.
The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question, the external vendor already has a Microsoft account (user1@outlook.com) so he can authenticate using that.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator

mkoprivnj Highly Voted 1 year, 9 months ago
C for sure!
upvoted 6 times

Razuli Highly Voted 1 year, 5 months ago
C, tested this on my tenant
upvoted 5 times

Hani_Ajaj Most Recent 1 year, 7 months ago
You need to configure the environment to audit AD FS user authentication.
upvoted 1 times

Question #46 *Topic 4*

You have a Microsoft 365 subscription that contains several Microsoft SharePoint Online sites.
You discover that users from your company can invite external users to access files on the SharePoint sites.
You need to ensure that the company users can invite only authenticated guest users to the sites.
What should you do?

A. From the Microsoft 365 admin center, configure a partner relationship.

B. From SharePoint Online Management Shell, run the Set-SPOSite cmdlet.

C. From the Azure Active Directory admin center, configure a conditional access policy.

D. From the SharePoint admin center, configure the sharing settings.

Correct Answer: *D*
You need to set the Sharing settings to 'Existing Guests'. This setting allows sharing only with guests who are already in your directory. These guests may exist in your directory because they previously accepted sharing invitations or because they were manually added.
Reference:
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

mkoprivnj Highly Voted 1 year, 9 months ago
D for sure! SPO admin center, config sharing.
upvoted 7 times

Jokke71 Highly Voted 2 years, 7 months ago
Reference: https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off#change-the-organization-level-external-sharing setting
upvoted 6 times

andylop04 Most Recent 4 months ago
Selected Answer: D
D 100%
upvoted 1 times

adaniel89 1 year, 3 months ago
External Sharing is for the entire Sharepoint and Onedrive enviroment, however, to only cover an individual Sharepoint site you should use Set-SPOsite
https://docs.microsoft.com/en-us/powershell/module/sharepoint-online/set-sposite?view=sharepoint-ps
B should be the correct answer!
upvoted 1 times

michszym 1 year, 2 months ago
Read the question: "You need to ensure that the company users can invite only authenticated guest users to the sites." --> so you ne to change it for all sites, not for individual Sharepoint site!!!
upvoted 2 times

donathon 2 years ago
A: This configures external sharing for the whole MS365 stacks like OneDrive or Teams etc. The question states “to the sites”.
B: Should be Set-SPOTenant.
C: Does not help.
upvoted 5 times

jpcapone 1 year, 8 months ago
How can you create a partner federation with "only authenticated guest users"?
upvoted 1 times

McAlec 1 year, 4 months ago
Set the content sharing level from Anyone to New and existing guests on the External sharing page.
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off
upvoted 1 times

Question #47 *Topic 4*

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.
You purchase a Microsoft 365 subscription.
You implement password hash synchronization and Azure Active Directory (Azure AD) Seamless Single Sign-On (Seamless SSO).
You need to ensure that users can use Seamless SSO from the Windows 10 computers.
What should you do?

A. Create a conditional access policy in Azure AD.

B. Deploy an Azure AD Connect staging server.

C. Join the computers to Azure AD.

D. Modify the Intranet zone settings by using Group Policy

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

banditben86 Highly Voted 1 year, 8 months ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

D is correct
upvoted 7 times

L33D Most Recent 10 months, 2 weeks ago
Selected Answer: D
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start#why-do-you-need-to-modify-users-intranet-zone-settings

Why do you need to modify users' Intranet zone settings?

By default, the browser automatically calculates the correct zone, either Internet or Intranet, from a specific URL. For example, http://contoso/ maps to the Intranet zone, whereas http://intranet.contoso.com/ maps to the Internet zone (because the URL contains period). Browsers will not send Kerberos tickets to a cloud endpoint, like the Azure AD URL, unless you explicitly add the URL to the browser's Intranet zone.
upvoted 3 times

TimurKazan 1 year, 1 month ago
it clearly states that device doesn't need to be Azure AD joined, but should be AD joined, so I would go with D
upvoted 3 times

samjohnjohn 1 year, 2 months ago
C also seems feasible.
upvoted 2 times

tochno 1 year, 2 months ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start
It says that "The device doesn't need to be Azure AD Joined"

D is correct.
upvoted 1 times

melatocaroca 1 year, 3 months ago
Answer Can be C or D, IMHO, Better answer C

SSO via PRT works once devices are registered with Azure AD for hybrid Azure AD joined, Azure AD joined or personal registered device via Add Work or School Account. For more information on how SSO works with Windows 10 using PRT

https://blog.matrixpost.net/azure-active-directory-seamless-single-sign-on-and-primary-refresh-token-prt/
upvoted 3 times

ErikNLH 1 year, 8 months ago

This might be true. but C is also right.

For Windows 10, the recommendation is to use Azure AD Join for the optimal single sign-on experience with Azure AD.
upvoted 3 times

exaja 1 year, 4 months ago

The device has to be joined to your Active Directory domain, but it doesn't need to be Azure AD Joined.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start#step-4-test-the-feature
upvoted 1 times

Fcnet 1 year, 2 months ago

this is wrong the device need to be azure ad joined otherwise Sso won't work, tested and validated with a support case too so the answer is C & D both are needed
without SCP and without azure ad joined Sso won't work
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains#prerequisites
upvoted 1 times

Eggsamine 11 months, 2 weeks ago

Wrong
The device is joined to your Active Directory domain. The device doesn't need to be Azure AD Joined.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start#:~:text=The%20device%20is%20joined%20to%20your%20Active%20Directory%20domain.%20The%20device%20doesn%20need%20to%20be%20Azure%20AD%20Joined.
upvoted 1 times

HOTSPOT -

You work at a company named Contoso, Ltd.

Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.

Name	Can enroll devices
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

Contoso purchases a company named Fabrikam, Inc.

Contoso plans to add the following domains to the Microsoft 365 subscription:

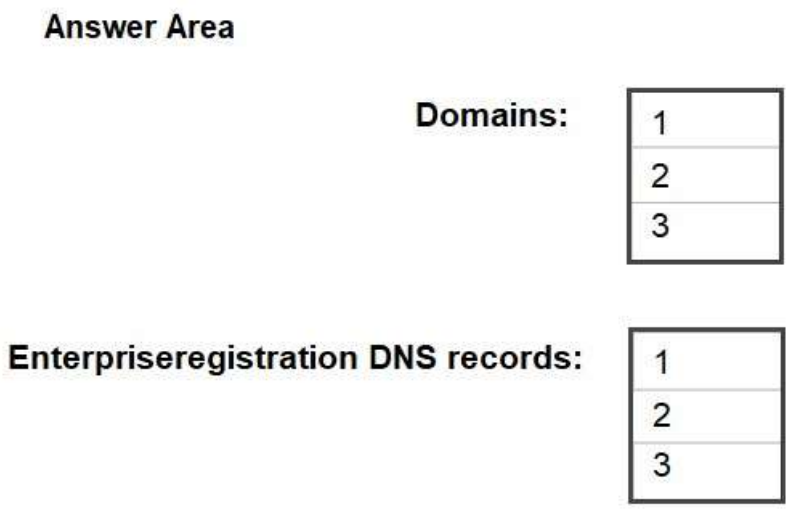
- fabrikam.com
- east.fabrikam.com
- west.contoso.com

You need to ensure that the devices in the new domains can register by using Autodiscover.

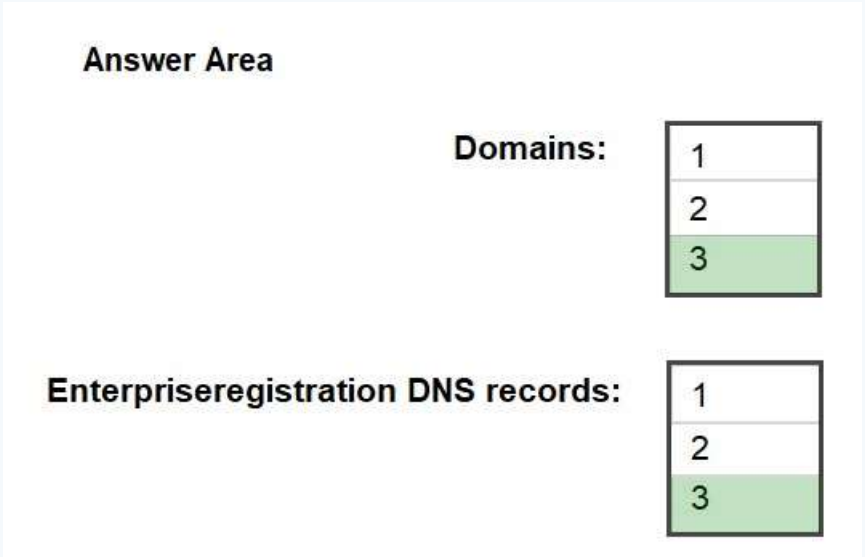
How many domains should you verify, and what is the minimum number of enterpriseregistration DNS records you should add? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

TimNov Highly Voted 1 year, 4 months ago

The first question should be 1. Contoso is already verified and added, subdomains do not need verifying and adding so only fabrikam.c needs verifying. 3 CNAMEs are needed though for each domain.

upvoted 27 times

afbnfz Highly Voted 1 year, 4 months ago

The answer to the first part of the question is 1, not 3.

"When you add a subdomain, it is automatically verified based on the parent domain that is being verified." - https://docs.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide

upvoted 14 times

Cheekypoo Most Recent 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Mug1992 6 months, 3 weeks ago

In the first box should be 3 (the answer is correct).
The domain needs to be always verified ! The verification is a simple DNS record to MSFT know that you are owner of the domain. The subdomains are automatically verified, but that not mean you bypass the domain verfication!
Seconde box is 3 also. All domains need a DNS record for registration device, even if its a sub domain.

upvoted 1 times

LillyLiver 8 months, 1 week ago

Answer: 1, 3.

If the company uses more than one UPN suffix, you need to create one CNAME for each domain name and point each one to EnterpriseEnrollment-s.manage.microsoft.com. For example, users at Contoso use the following formats as their email/UPN:

name@contoso.com
name@us.contoso.com
name@eu.contoso.com

upvoted 1 times

Muizzbell 11 months ago

The Answer should be 1 domain - Fabrikam and 3 Enterprise Registration DNS which are CNames:
You need to ensure that the devices in the new domains can register by using Autodiscover.
Type Host name Points to TTL
CNAME EnterpriseEnrollment.fabrikam.com EnterpriseEnrollment-s.manage.microsoft.com 1 hour
CNAME EnterpriseEnrollment.east.fabrikam.com EnterpriseEnrollment-s.manage.microsoft.com 1 hour
CNAME EnterpriseEnrollment.west.contoso.com EnterpriseEnrollment-s.manage.microsoft.com 1 hour

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#step-1-create-cname-optional

upvoted 1 times

Eggsamine 11 months, 2 weeks ago

The number of domains should be 1

"If you want to add a subdomain name such as 'europe.contoso.com' to your organization, you should first add and verify the root domain, such as contoso.com. The subdomain is automatically verified by Azure AD. To see that the subdomain you added is verified, refresh the domain list in the browser."

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-manage#:~:text=If%20you%20want%20to%20add%20a%20subdomain%20name%20such%20as%20%E2%80%98europe.contoso.com%%80%99%20to%20your%20organization%2C%20you%20should%20first%20add%20and%20verify%20the%20root%20domain%2C%20sh%20as%20contoso.com.%20The%20subdomain%20is%20automatically%20verified%20by%20Azure%20AD.%20To%20see%20that%20%20subdomain%20you%20added%20is%20verified%2C%20refresh%20the%20domain%20list%20in%20the%20browser.

upvoted 1 times

mitsios96 1 year, 1 month ago

Guys,

It's 1 domain: fabrikam.com (contoso.com already verified, and any sub-domain doesn't require verification)

Regarding the DNS Records the answer is 2: The autodiscover mentioned here is for enterprise registration , not Outlook Autodiscover.
These are DNS records for mobile device management, which are 2 CNAME Records
enterpriseregistration.domain.xxx point to enterpriseregistration.windows.net
and
enterpriseenrollment.domain.xx point to enterpriseenrollment.manage.microsoft.com

upvoted 5 times

RML_Wyvern 1 year, 1 month ago

The second answer specifies EnterpriseRegistration DNS records not Autodiscover. So should answer bse 1 and 0? EnterpriseRegistrati is used to redirect to intune so not for email.

upvoted 1 times

MomoLomo 1 year, 2 months ago

1 domain
3 cnames

upvoted 4 times

melatocaroca 1 year, 3 months ago

IMHO Answer 2 domains, 3 DNS records

Already in place an verified
• contoso.com
• contoso.onmicrosoft.com
New domains
• west.contoso.com verified from contoso.com
New adquisition Fabrikam
Need to be verified
• fabrikam.com
no needed to verify
east.fabrikam.com
west.contoso.com

When you add a subdomain, it is automatically verified based on the parent domain that is being verified.

We recommend that you create an Autodiscover CNAME record for every domain on your account,
including domain aliases and accepted domains.
You need to create either a CNAME or SRV record where your domain is hosted.
Only then you can synchronize your offline address book, show free/busy information and enable the Out of office feature in Outlook.

• autodiscover.fabrikam.com
• autodiscover.east.fabrikam.com
• autodiscover.west.contoso.com

upvoted 1 times

Bennett008 1 year, 4 months ago

I agree with afbnfz. It states "Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the followi
table" and therefore contoso.com has already been registered/configured.

Therefore only root domain of fabrikam.com needs to be verified. The answer the first part of the question is 1 and 3 x CNAMEs

upvoted 2 times

prepre 1 year, 5 months ago

You do not need to verify sub-domain and so you'll only need to verify fabrikam.com, for autodiscover though, each will need a CNAME

upvoted 1 times

japhar 1 year, 5 months ago

Exactly my thought! you just need to verify contoso.com and fabrikam.com, but you'll need DNS for each subdomain.

upvoted 1 times

Question #49 *Topic 4*

Your company has a hybrid deployment of Microsoft 365.

Users authenticate by using pass-through authentication. Several Microsoft Azure AD Connect Authentication Agents are deployed.

You need to verify whether all the Authentication Agents are used for authentication.

What should you do?

A. From the Azure portal, use the Troubleshoot option on the Pass-through authentication page.

B. From Performance Monitor, use the #PTA authentications counter.

C. From the Azure portal, use the Diagnostics settings on the Monitor blade.

D. From Performance Monitor, use the Kerberos authentications counter.

Correct Answer: *A*

On the Troubleshoot page, you can view how many agents are configured. If you click on the agents link, you can view the status of each agent.

Each agent will have a status of Active or Inactive.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-pass-through-authentication

d3an Highly Voted 2 years, 8 months ago

This should be B - the #PTA counter in Performance Monitor. Troubleshooting in Azure AD will only help if there is an active issue, the question states that you just wish to check that all agents are handling authentication requests.

Ref - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-pass-through-authentication#performance-monit counters

upvoted 31 times

lucidgreen 1 year, 6 months ago

B requires you to check each server individually.
A allows you to check all at once. Azure Portal > Azure Active Directory > Azure AD Connect > click on Pass-through authentication. It will take you to the agents and give you their health.

upvoted 6 times

PandaTuga 1 year, 3 months ago

you can use a single server to collect the #PTA performance counters from several servers

upvoted 1 times

lucidgreen 1 year, 6 months ago

And by A, I mean it's wrong because you're looking in the wrong place. You can check it in Azure Portal, is what I meant.

upvoted 1 times

KornienkoBoris 1 year, 1 month ago

In the Azure portal you only check the status of Agent: active or not, but not traffic. For this you need the performance counte

"Pass-through Authentication provides high availability using multiple Authentication Agents, and not load balancing. Depenc on your configuration, not all your Authentication Agents receive roughly equal number of requests. It is possible that a speci Authentication Agent receives no traffic at all."

upvoted 2 times

Fcnet Highly Voted 2 years, 4 months ago

A is right
It is asked to verifiy to "whether all the Authentication Agents are used for authentication"
so if the agent works fine and is seen with ACTIVE Status from the Azure portal then it can't be used for anything else : authentication.
so the answer is A

upvoted 7 times

T_B 2 years, 3 months ago

A is right, see: https://docs.microsoft.com/nl-nl/azure/active-directory/hybrid/tshoot-connect-pass-through-authentication

upvoted 4 times

jage01 Most Recent 6 months, 2 weeks ago

Selected Answer: A

Ensure that the Pass-through Authentication feature is still Enabled on your tenant and the status of Authentication Agents shows Activ and not Inactive.

A - MS WAY

upvoted 1 times

AlexLiourtas 8 months, 1 week ago

Selected Answer: B

answer b PTA

upvoted 2 times

melatocaroca 1 year, 3 months ago

IMHO
Answer B not right

Performance Monitor counters
Another way to monitor Authentication Agents is to track specific Performance Monitor counters on each server where the Authenticat Agent is installed. Use the following Global counters (# PTA authentications, #PTA failed authentications and #PTA successful authentications) and Error counters (# PTA authentication errors):

Answer A Right
Check status of the feature and Authentication Agents
Ensure that the Pass-through Authentication feature is still Enabled on your tenant and the status of Authentication Agents shows Activ and not Inactive. You can check status by going to the Azure AD Connect blade on the Azure Active Directory admin center.

Reference
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-pass-through-authentication

upvoted 2 times

LoremanReturns 1 year, 3 months ago

Answer A is the right answer: https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/hybrid/tshoot-conne pass-through-authentication.md

upvoted 2 times

Domza 1 year, 4 months ago

I think, this question could be rephrased in a different way.

upvoted 2 times

estarisbourne 1 year, 8 months ago

I am hoping they give credit to either answer as technically both are correct. A and B but I think B is more correct because it goes into t whole being able to see which host is not being used as much reality as load balancing is not exactly a thing and/or if one host experiences issues that the others do not. A bit out of the scope for the question tho

upvoted 1 times

Storm 1 year, 7 months ago

No - A is definately not right....
There is absolutely nothing to see on the "Troubleshoot option" exept some links to help with different sync remidiations...
The place people here are referencing "seeing status etc" for each agent, is not in the "Troubleshoot" option.

Only correct answer is B...

upvoted 6 times

[Removed] 1 year, 8 months ago

Agreed with B.
You were asked to verify whether Authentication Agents are USED.
Use #PTA counter
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-pass-through-authentication#performance-monitor-counters

upvoted 4 times

bingomutant 1 year, 8 months ago

also note the ALL in the question

upvoted 1 times

MichaelJS 1 year, 9 months ago

Probably B is right.
They probably look for this answer with this question:
"Another way to monitor Authentication Agents is to track specific Performance Monitor counters on each server where the Authentication Agent is installed. Use the following Global counters (# PTA authentications, #PTA failed authentications and #PTA successful authentications) and Error counters (# PTA authentication errors)"

Ref - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-pass-through-authentication#performance-monit
counters

upvoted 1 times

mkoprivnj 1 year, 9 months ago

B for sure!

upvoted 2 times

Jake1 1 year, 10 months ago

Answer is definitely B ad d2an said. To monitor Authentication Agents is to track specific Performance Monitor counters on each server
where the Authentication Agent is installed. Use the following Global counters (# PTA authentications, #PTA failed authentications and
#PTA successful authentications) and Error counters (# PTA authentication errors):

upvoted 1 times

itmp 2 years, 5 months ago

Answer is wrong - (this answer is listed as correct on other websites too...)
On Azure Active Directory -> Azure AD Connect -> Pass-through authentication you can view the number of agents, authentication ager
IP and status (e.g. Active)

This indicates that a PTA Agent is authenticated and connected to Azure Service. It does not mean that it is actually capable of
authenticating users.

The question asks to verify whether Authentication Agents are USED for authentication.
That is done with #PTA authentications counter.

upvoted 4 times

VTHAR 1 year, 11 months ago

Agreed! If the question is asking to ensure "all the authentication agents are active" then it would have been A. But since the questio
is asking "all the authentication agents are used for authentication", you can ONLY verify this with #PTA counter.

upvoted 2 times

VTHAR 1 year, 11 months ago

Correct answer should be "B. From Performance Monitor, use the #PTA authentications counter."

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Report reader
User2	User administrator
User3	Security administrator
User4	Global administrator

From the Sign-ins blade of the Azure Active Directory admin center, for which users can User1 and User2 view the sign-ins? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1 can view the sign-ins for the following users: ▼
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

User2 can view the sign-ins for the following users: ▼
- User2 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Correct Answer:

Answer Area

User1 can view the sign-ins for the following users: ▼
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4 ✓

User2 can view the sign-ins for the following users: ▼
- User2 only ✓
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Who can access the activity reports data?

➪ Users in the Security Administrator, Security Reader, Global Reader, and Report Reader roles

➪ Global Administrators

Any user (non-admins) can access their own sign-ins

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Davidchercm Highly Voted 1 year, 1 month ago

answer is correct :

Who can access it?
You can always access your own sign-ins history using this link: https://mysignins.microsoft.com

To access the sign-ins log, you need to be:

A global administrator

A user in one of the following roles:

Security administrator

Security reader

Global reader

Report reader

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

upvoted 7 times

BDuff Most Recent 8 months, 3 weeks ago

Tested this and the answer is correct.

upvoted 3 times

HOTSPOT -

Your network contains an on-premises Active Directory domain. The domain contains a server named Server1. Server1 has a share named Share1 that contains the files shown in the following table.

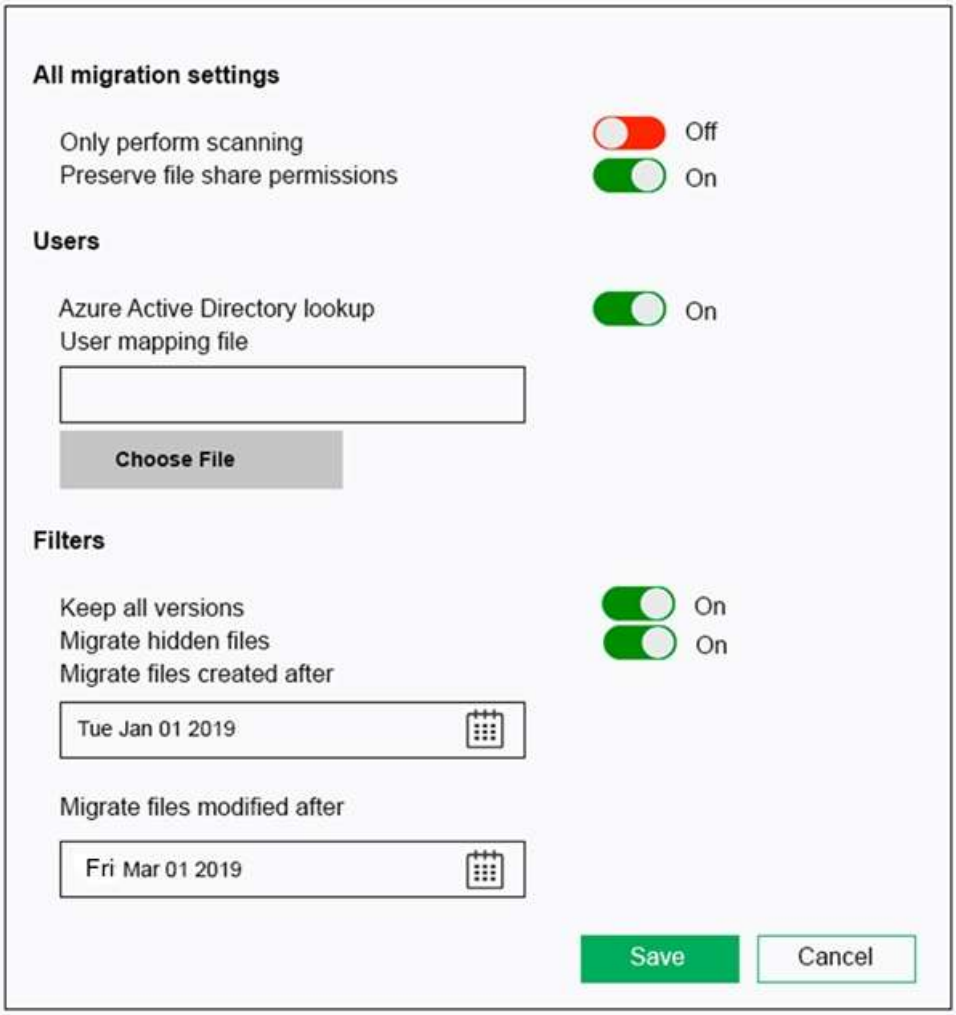
Name	Created	Modified	Permission
File1.txt	12/15/2018	03/15/2019	Domain Users: Allow Read
File2.txt	01/15/2019	03/15/2019	User1: Allow Read
File3.txt	03/05/2019	03/15/2019	Domain Users: Allow Read User1: Deny Read

You have a hybrid deployment of Microsoft 365.

You create a Microsoft SharePoint site collection named Collection1.

You plan to migrate Share1 to a document library in Collection1.

You configure the SharePoint Migration Tool as shown in the exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
File1.txt will be migrated to SharePoint.	○	○
File2.txt will be migrated to SharePoint.	○	○
User1 will be denied access to read File3.txt in SharePoint when the migration is complete.	○	○

Correct Answer:

Statements	Yes	No
File1.txt will be migrated to SharePoint.	○	●
File2.txt will be migrated to SharePoint.	●	○
User1 will be denied access to read File3.txt in SharePoint when the migration is complete.	○	●

VikingSWE Highly Voted 1 year, 4 months ago

N, Y, N
1. No, because the file was created before 2019-03-01. Both conditions must be fulfilled.
2. Yes, both Created and Modified dates are OK.
3. No special permissions are preserved. "Deny" counts as a special permission.

upvoted 24 times

VikingSWE 1 year, 4 months ago

And by 2019-03-01, I mean 2019-01-01.

upvoted 1 times

arunjana 1 year, 3 months ago

Note: At this time, the special permissions, such as Deny, will not be saved.
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating

upvoted 1 times

AnoniMouse Highly Voted 1 year, 5 months ago

The question is: How does the migration logic works? Does that mean that:

1: Files Create After some date AND Files Modified After other dates, or
2: Files Create After some date OR Files Modified After other dates?

If option 1 is true, then answer 1 is NO as the AND statement will exclude it
If option 2 is true, then answer 1 is YES as the OR statement would be more inclusive

upvoted 9 times

Nilz76 Most Recent 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 1 times

kanag1 8 months, 2 weeks ago

The Answer is : N, Y, N
Please refer the link that says :
There are three types of permissions that will be migrated: Read, Write, and Full control.
Note: At this time, the special permissions, such as Deny, will not be saved.
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating

upvoted 8 times

joergsi 8 months, 1 week ago

Thank you for providing the link and explanation, but I'm confused by your conclusion for file3.
Domain users = read, User1=deny => special permission for user1 will not be migrated => user1 is domain user which means user1 read the file!
So it must be Y

upvoted 1 times

DK_edu 7 months, 3 weeks ago

The statement is:
"User1 will be denied access to read File3.txt in SharePoint when the migration is complete."

The answer is N because User1 will not be denied access. They will be able to access it.

upvoted 2 times

LillyLiver 8 months, 1 week ago

I can confirm as I just ran through everything in this question with my own tenant. Both conditions need to be met, and the Deny fo
User1 will be seen as a special permission and will ALLOW User1 to open the file in SPO.

Nice work, Kanag1!
upvoted 4 times

fofo1960 9 months ago
I think and based on the test that the answer is correct
The relation is AND, so
1 - No
2- Yes
3- Yes, as the Domain users are granted access and will be migrated, but the deny wont be migrated. so the final result on the cloud wi
be that domain users can read and Domain users include User3
Correct me if I was wrong.
upvoted 3 times

JakeH 10 months, 3 weeks ago
In exam today
upvoted 2 times

smudo1965 11 months, 3 weeks ago
deny is excluded from migration therefore 3. answer is yes
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating
1. answer from my side is yes too because it was modified inside the time frame... if it was not modified it would be no
upvoted 1 times

Linux09 1 year ago
Read the question again. We are talking about a "share". If you look at the exhibit, the "Preserve file share permissions" is set to on. Th
makes the answer YES.

NYY
upvoted 2 times

lengySK 1 year, 1 month ago
I think N Y N...3rd answer Note: At this time, the special permissions, such as Deny, will not be saved.
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating
upvoted 3 times

emilianogalati 1 year, 1 month ago
YYY

On the first answer:
I could still need a 20yo file, that would not be migrated if the implemented logic is AND.
Moreover, if the creation date field and the modify one use the logic operator AND only the file after March 2019 wil be migrated.

So what's the point to set a creation date filter?
upvoted 1 times

Madball 1 year, 2 months ago
I think the answer is NYY

1. No, because the file was created before 2019-03-01.
2. Yes, both modified and created dates are OK.
3. Yes, the question says the user will be denied access, if the permissions are migrated over then they will be blocked from accessing t
file.
upvoted 1 times

chaoscreater 1 year, 3 months ago
People need to start using their heads. If all you need to do is modify a file to make it recent, then what's the point of the filters? Any su
old file created 20 years ago can bypass this limitation, if all you need to do is make them have a new modified date. There's a reason f
the filters and so both the created and modified date need to fulfill the condition.
upvoted 5 times

bwl 1 year, 3 months ago
i think should be y y y
there is no logic in it if the files must be created AND modified after a certain date.
If a file has been created in 1999 it does not mean it is no longer in use, that's what the modified after filter is for, to catch those files
which are older already but still in use and therefor have to be migrated.

I think the file rights will be transfered as well:

Preserve user permissions for file share migration:- By default, this is set to On. If set to Off, no permissions will be preserved.
https://mundrisoft.com/tech-bytes/how-to-use-the-sharepoint-migration-tool/
upvoted 4 times

maikelb 1 year, 4 months ago

VikingSWE you have it all right !!!
N, Y, N
1. No, because the file was created before 2019-03-01. Both conditions must be fulfilled.
2. Yes, both Created and Modified dates are OK.
3. No special permissions are preserved. "Deny" counts as a special permission.
https://docs.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating
Thanks for ;-)

upvoted 5 times

melatocaroca 1 year, 3 months ago

When preparing for your file share migration, it's important to know what's being migrated when you use the SharePoint Migration Tool and what's not.

User level file and folder permissions Explicit deny permission will not be migrated

https://docs.microsoft.com/en-us/sharepointmigration/fileshare-to-odsp-migration-guide

so 3 must be N

upvoted 1 times

lokylook 1 year, 6 months ago

First answer should be yes because its modified after 1st march 19
There is no such Deny function on SharePoint online so third answer is no

upvoted 3 times

000zest 1 year, 5 months ago

First answer is NO. File was created before 1st Jan 2019, and therefore doesn't meet the policy to be migrated to SharePoint Online.

upvoted 1 times

AlexLiourtas 9 months, 4 weeks ago

but there are two filtering rules.
1. when the file was created
2. when the file was modified.

file1 does not meet the first rule, but does the second. it should be migrated.

upvoted 1 times

japhar 1 year, 5 months ago

But it was modified after 1st march 19, so it should be a YES?

upvoted 7 times

Razuli 1 year, 5 months ago

My thoughts exactly japhar

upvoted 3 times

lucidgreen 1 year, 6 months ago

The answer is correct, however, the 3rd answer is correct because user rights will be preserved, not because it will be migrated.

upvoted 5 times

HOTSPOT -

You have a Microsoft 365 Enterprise E5 subscription.

You add a cloud-based app named App1 to the Microsoft Azure Active Directory (Azure AD) enterprise applications list.

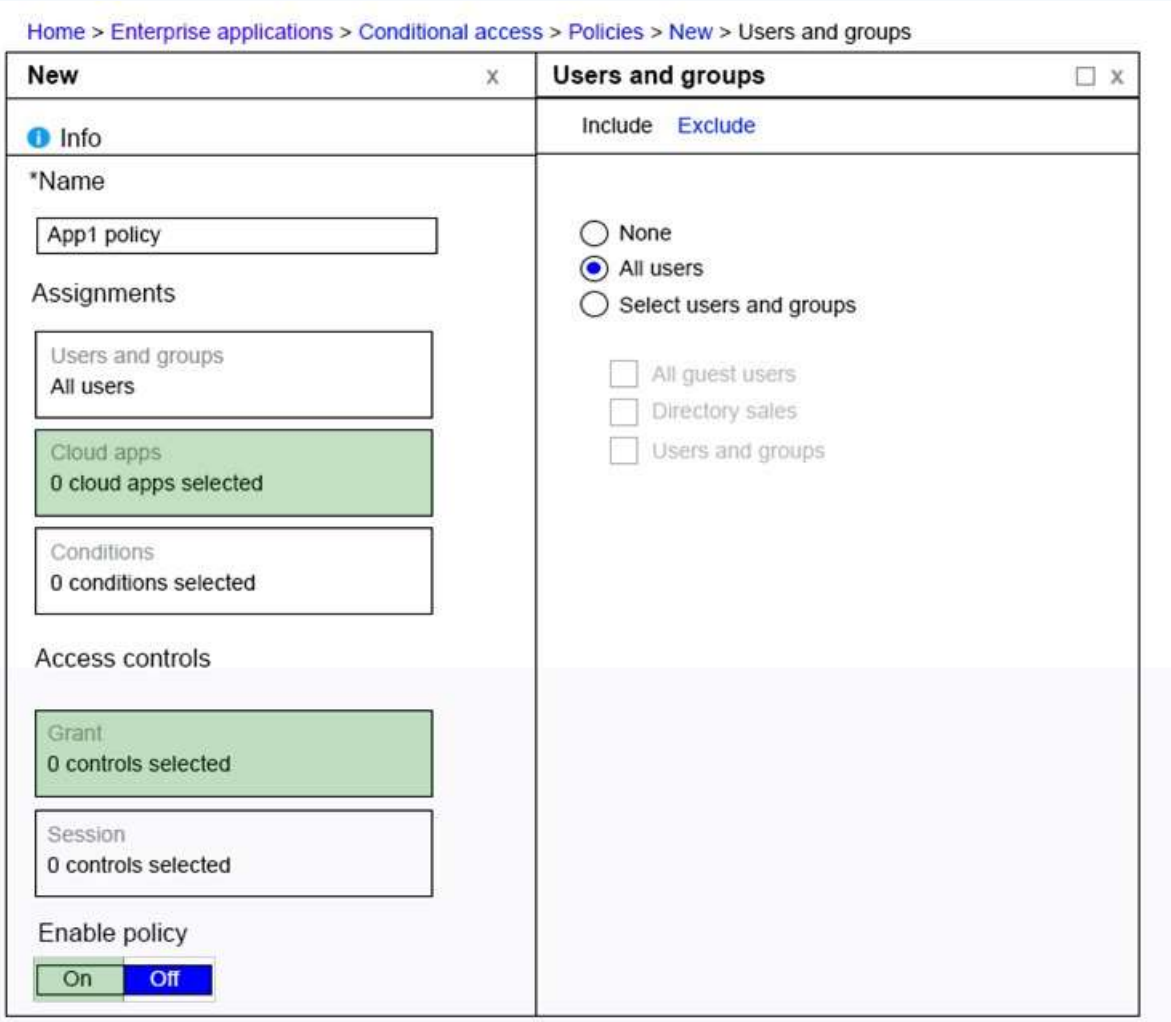
You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.

Which three settings should you configure from the policy? To answer, select the appropriate settings in the answer area.

Hot Area:



Correct Answer:



In the Cloud Apps section, you need to select the name of the app (App1) that the policy will apply to.

In the Grant section under Access Controls, there is a checkbox named ג€Require Multi-factor Authenticationג€. That checkbox needs to be ticked.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/best-practices

https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Conditional-Access-now-in-the-new-Azure-portal/ba-p/250060

itmp Highly Voted 2 years, 4 months ago

1. Cloud Apps
2. Grant
3. Enable policy

upvoted 21 times

Dimonchik 2 years, 1 month ago

How about exclude all users settings enabled?

upvoted 3 times

Joshing 1 year, 11 months ago

I believe it's not excluding users and is still on the including tab. Looking on the left hand side it just says all users as well. If it we excluding all users you would need 4 steps to complete the task.

upvoted 3 times

Mr01z0 Most Recent 1 year, 4 months ago

This policy will still not work, you still need a condition, a condition determines when the conditional access policy will apply, so for instance you could set any location. Since the condition is 0 there are none set.

upvoted 1 times

cowpoo 1 year, 8 months ago

Pretty sure you have to set Condition (such as location) otherwise MFA wont trigger

upvoted 1 times

PD1885 1 year, 8 months ago

Locations appear to be optional and the question doesn't state any requirement around location base:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

upvoted 2 times

mkoprivnj 1 year, 9 months ago

1. Cloud Apps
2. Grant
3. Enable policy

upvoted 2 times

Jhill777 2 years, 4 months ago

This seems correct. Require MFA is in Access Controls.

upvoted 2 times

HOTSPOT -

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.

Contoso.com contains the users shown in the following table.

Name	Group
User1	Group1
User2	*None*

You add an enterprise application named App1 to contoso.com.

You configure the following self-service settings for App1:

- Allow users to request access to this application is set to Yes.
- To which group should assigned users be added is set to Group1.
- Who is allowed to approve access to this application is set to User2.
- Require approval before granting access to this application is set to Yes.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can request access to App1.	○	○
When User2 requests access to App1, the user is added to Group1automatically.	○	○
User2 can approve requests for App1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can request access to App1.	○	○
When User2 requests access to App1, the user is added to Group1automatically.	○	○
User2 can approve requests for App1.	○	○

Box 1: Yes.

User1 can request access to App1 because ג€Allow users to request access to this applicationג€ is set to Yes.

Box 2: No.

User2 is an approver. If User2 requests access to App1, he will still need to approve the request before he is added to Group1.

Box 3: Yes.

User2 can approve requests for App1 because ג€Who is allowed to approve access to this applicationג€ is set to User2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

Sprinqfield Highly Voted 1 year, 4 months ago

I guess, its N, N, Y.

User1 already member with Group1

upvoted 10 times

michszym 1 year, 3 months ago

User1 won't see "Request Access" button if he is already in Group1?

upvoted 1 times

michszym 1 year, 2 months ago

I've made test - Answers will be: NYY
Box1 - user already in Group1 can see App1 in MyApps and cannot see on list to requested App so he cannot request them once again
Box2 - user2 is automatically added to Group1 when he request App1
Box3 obviously Y

upvoted 13 times

Chipper 1 year, 2 months ago

This is my thinking as well. If user2 is an approver and user2 asks for the app, wouldn't it be auto approved? Is there another approver that needs to approve these types of requests?

upvoted 1 times

Durden871 7 months, 1 week ago

- To which group should assigned users be added is set to Group1.
- Require approval before granting access to this application is set to Yes.

Even though User 2 is an approver, it isn't a member of Group 1 and to join you need to accept the approval.

I would say box one should be no. Why would you be able to request access to an app you already have access to?

upvoted 1 times

joergsi Most Recent 8 months ago

The answer is YYY
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list?view=o365-worldwide#url-syntax-f
the-tenant-allowblock-list

- Wildcards (*) are allowed in the following scenarios:
A left wildcard must be followed by a period to specify a subdomain.
For example, *.contoso.com is allowed; *contoso.com is not allowed.

=> fabrikam*.com is not allowed!

- The tilde (~) character is available in the following scenarios:
A left tilde implies a domain and all subdomains.
For example ~contoso.com includes contoso.com and *.contoso.com.

because the ~ is not been used:
=> contoso.com would be blocked
=> us.contoso.com would NOT be blocked

upvoted 1 times

alex_p 5 months, 3 weeks ago

dude, you are commenting something different!

upvoted 8 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid deployment of Microsoft 365 that contains the objects shown in the following table.

Name	Type	Source
User1	User	Azure Active Directory (Azure AD)
User2	User	Windows Server Active Directory
Group1	Group	Cloud
Group2	Group	Windows Server Active Directory

Azure AD Connect has the following settings:

- Password Hash Sync: Enabled
- Password writeback: Enabled
- Group writeback: Enabled

You need to add User2 to Group 2.
Solution: From Azure PowerShell, you run the Set-AzureADGroup cmdlet.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The Set-AzureADGroup cmdlet updates a group in Azure Active Directory (AD) but User2 and Group2 are objects in Windows Server AD.

lucidgreen Highly Voted 1 year, 5 months ago
The correct commandlet would be Add-AzureADGroupMember.
upvoted 8 times

J0J0 1 year, 4 months ago
Should be done in on-premise AD
upvoted 9 times

melatocaroca 1 year, 3 months ago
Add-AzureADGroupMember
-ObjectId <String>
-RefObjectId <String>
[-InformationAction <ActionPreference>]
[-InformationVariable <String>]
[<CommonParameters>]

Reference
https://docs.microsoft.com/en-us/powershell/module/azuread/add-azureadgroupmember?view=azureadps-2.0
upvoted 1 times

venwaik Most Recent 1 year, 2 months ago
Since group2 is located on-prem, you should add user2 in the on-prem AD.
Command would be:
Add-AdGroupMember -identity "Groupname" -member "username"
upvoted 4 times

venwaik 1 year, 2 months ago
BUT: since group writeback is enabled, you should use "Add-AzureADGroupMember -ObjectId (Groupname) -RefObjectID (Usernam
in this case as Lucidgreen commented.
upvoted 1 times

Redrock2063 1 year, 1 month ago
Group writeback only applies to Microsoft 365 groups, not AD security groups
upvoted 10 times

m43s 1 year, 1 month ago

Brilliant my friend 🤌

upvoted 2 times

haazybanj 11 months, 1 week ago

The type of group is not specified

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid deployment of Microsoft 365 that contains the objects shown in the following table.

Name	Type	Source
User1	User	Azure Active Directory (Azure AD)
User2	User	Windows Server Active Directory
Group1	Group	Cloud
Group2	Group	Windows Server Active Directory

Azure AD Connect has the following settings:

- Password Hash Sync: Enabled
- Password writeback: Enabled
- Group writeback: Enabled

You need to add User2 to Group 2.
Solution: You use the Azure Active Directory admin center.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
User2 and Group2 are objects in Windows Server Active Directory (AD)

kkkeji Highly Voted 1 year, 6 months ago
B.
because User2 and Group2 are objects in Windows Server Active Directory (AD).
upvoted 15 times

Arlecchino 1 month ago
True man lol, the question above literally says the same
upvoted 1 times

lucidgreen Highly Voted 1 year, 5 months ago
B.
Group writeback leverages only M365 Groups and requires hybrid Exchange because of that.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback
upvoted 12 times

AnoniMouse 1 year, 5 months ago
I guess the answer is NO (i.e., B). According to the article lucidgreen posted, here is a quote

Groups writeback enables customers to leverage cloud groups for their hybrid needs. If you use the Microsoft 365 Groups feature, t
you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange pres
in your on-premises Active Directory.

The key here is "This option is only available if you have Exchange present in your on-premises Active Directory", and there is no mention of any Exchange in the question
upvoted 2 times

Kainzor Most Recent 2 months ago
Selected Answer: B
Should be B, AD-onprem is always the leader in hybrid environment
upvoted 1 times

fofo1960 9 months ago
Selected Answer: B

Even if you try to add the user to a NON-Microsoft365 group, you will get the following error
Mail-enabled security groups are not allowed
upvoted 1 times

MatthiasGraber 9 months, 1 week ago

Selected Answer: B

Right explanation, wrong answer. Should be B!
upvoted 2 times

tf444 9 months, 3 weeks ago

NO:
Groups writeback enables customers to leverage cloud groups for their hybrid needs. If you use the Microsoft 365 Groups feature, ther
you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange presen
your on-premises Active Directory.
upvoted 3 times

tcmaggio 10 months ago

Selected Answer: B

Right explanation, wrong answer. Should be B!
upvoted 2 times

fofo1960 11 months, 2 weeks ago

Answer is B, even if you try to add User2 to Group2 via Azure AD, you will get the following message
Directory synced objects are not allowed.
upvoted 3 times

ariperdis 1 year ago

This answer has to be B. So A is wrong. You cant add User 2 to Group2 in Security and Compliance.
upvoted 2 times

F_M 1 year, 4 months ago

Group 2 is an on prem created group so it's not an M365 group. Group writeback works only on M365 groups (and only with Exchange
prem enabled)! So B
upvoted 1 times

Flacky_Penguin32 1 year, 4 months ago

A. If you have Azure AD P2 you can write back, then if you buy P2 after the fact you just gotta redo the ADC setup wizard to enable the
setting.
upvoted 1 times

BrianGold 1 year, 5 months ago

A.
Group writeback is enabled...so, changes in Azure AD would sync back.
upvoted 3 times

Razuli 1 year, 5 months ago

I didn't think you could writeback from cloud to on prem, only on prem to cloud, maybe I'm wrong?
upvoted 1 times

chaoscreater 1 year, 3 months ago

your basic foundation is poor. Write "back" literally writes the data from cloud to onprem.
upvoted 2 times

MomoLomo 1 year, 2 months ago

when you had poor foundation did people respond to you this when you made questions !
upvoted 5 times

jh999 1 year, 2 months ago

Agreed, we can be civil right?
upvoted 4 times

AlexLiourtas 9 months, 4 weeks ago

well his name is "chaoscreator" so...that's some edgy guy right over there.
upvoted 2 times

Kipperson 1 year, 4 months ago

With group writeback you can sync M365 groups in the cloud back to on premise - not azure groups or dynamic groups either.
upvoted 2 times

chaoscreater 1 year, 3 months ago

God some of these comments on here are absolutely low level. Worst thing that can happen to a discussion on any website or any forum is EVERYONE contributing their own opinion and ideas and none of them are actual facts that have been validated. The quest is very simple. It's talking about an AD user and an AD group. Why are you talking about Azure AD?

upvoted 6 times

Question #56 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a hybrid deployment of Microsoft 365 that contains the objects shown in the following table.

Name	Type	Source
User1	User	Azure Active Directory (Azure AD)
User2	User	Windows Server Active Directory
Group1	Group	Cloud
Group2	Group	Windows Server Active Directory

Azure AD Connect has the following settings:

- Password Hash Sync: Enabled
- Password writeback: Enabled
- Group writeback: Enabled

You need to add User2 to Group 2.

Solution: You use the Security & Compliance admin center.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Security & Compliance admin center is not used to manage users.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center

tejb 1 year, 1 month ago

Correct! Should be done on-prem

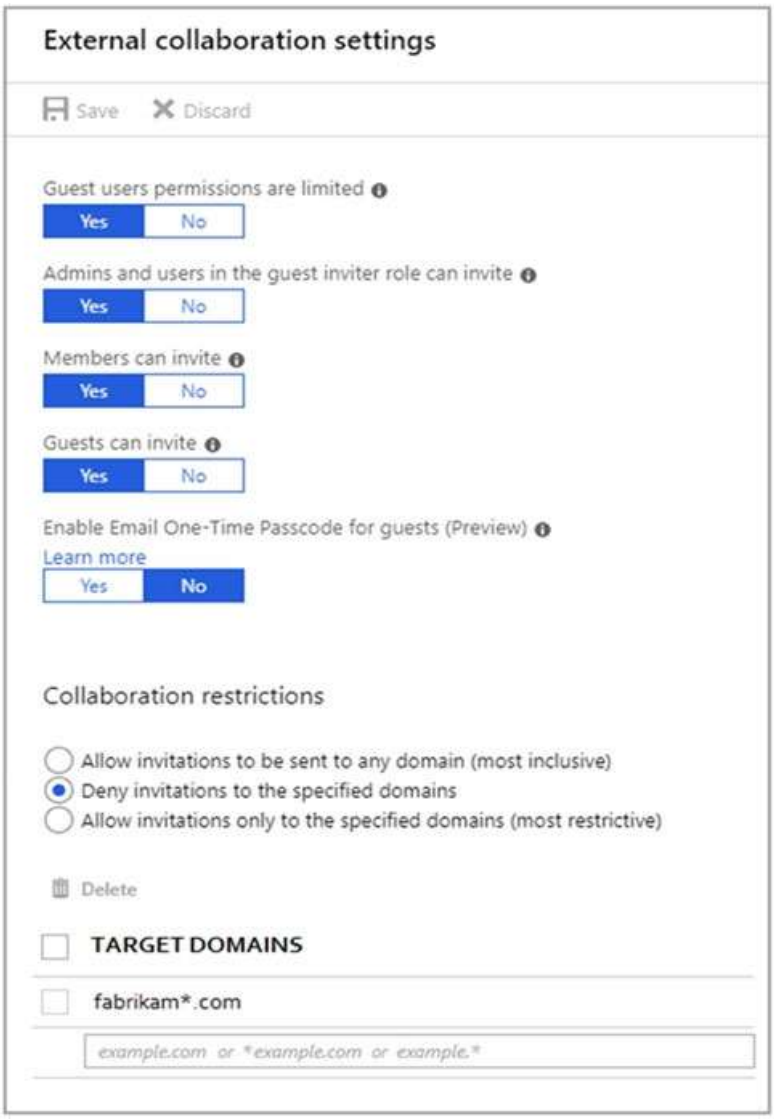
upvoted 2 times

HOTSPOT -

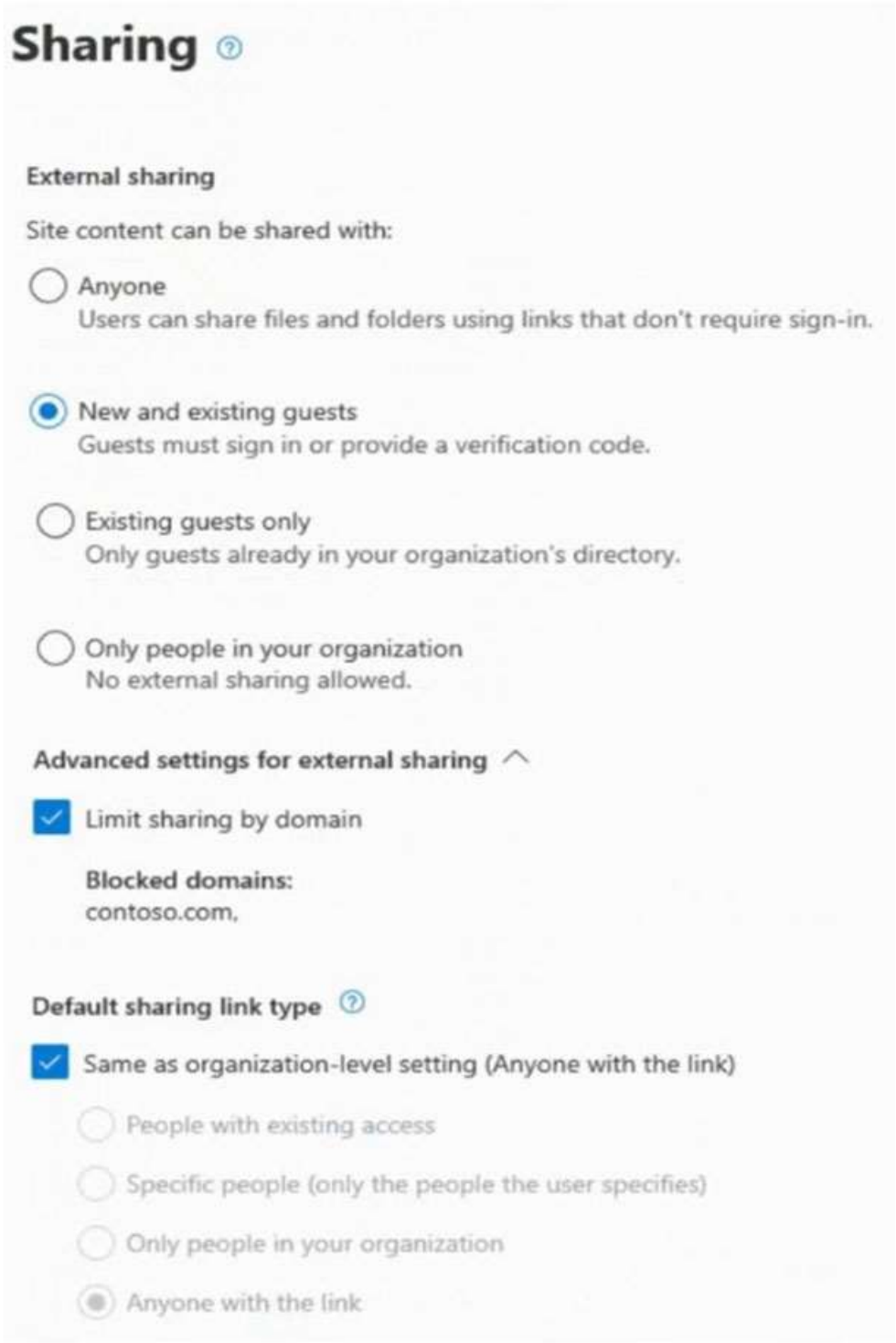
You have a Microsoft 365 subscription that uses a default domain named litwareinc.com. The subscription has a Microsoft SharePoint site collection named

Collection1.

From the Azure Active Directory admin center, you configure the External collaboration settings as shown in the External Collaboration Settings exhibit.



From the SharePoint admin center, you configure the sharing settings as shown in the SharePoint Sharing exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

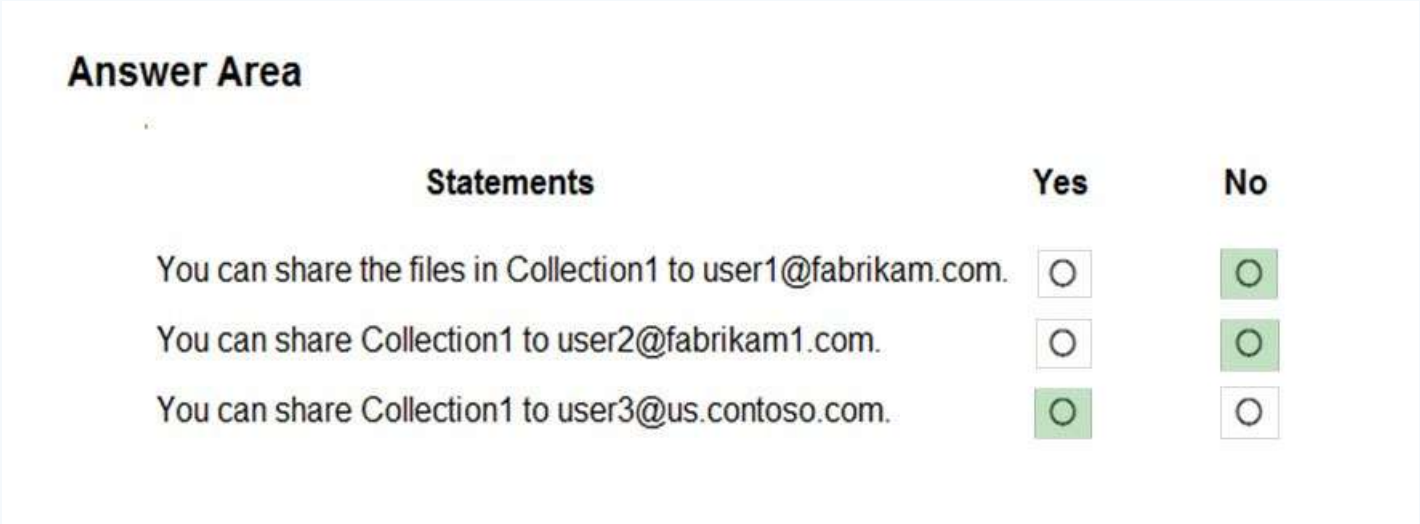
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can share the files in Collection1 to user1@fabrikam.com.	○	○
You can share Collection1 to user2@fabrikam1.com.	○	○
You can share Collection1 to user3@us.contoso.com.	○	○

Correct Answer:



Box 1: No -
In the first exhibit, ג€Deny invitations to the specified domainsג€ is selected and fabrikam.com is listed. This means that no one can send an invitation to fabrikam.com. Therefore, you cannot share the files in Collection1 to user1@fabrikam.com.

Box 2: No -
As noted above, ג€Deny invitations to the specified domainsג€ is selected and fabrikam.com is listed. This means that no one can send an invitation to fabrikam.com.
Therefore, you cannot share Collection1 to user2@fabrikam.com.

Box 3: Yes -
External sharing is enabled for any domain except contoso.com (and fabrikam.com due to the 'deny invitations' setting).
Blocking sharing to contoso.com does not block sharing to us.contoso.com. Therefore, you can share Collection1 to user3@us.contoso.com.
Reference:
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

melatocaroca Highly Voted 1 year, 3 months ago
Wildcard for fabrikan*.com will not work,

Wildcards are not supported for domain entries.

So Answer IMHO, must be YYY

References
https://docs.microsoft.com/en-us/sharepoint/restricted-domains-sharing
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-wildcard-domain#:~:text=Azure%20DNS%20supports%20wildcard%20records,(from%20the%20wildcard%20domain).
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list?view=o365-worldwide
upvoted 12 times

michszym 1 year, 2 months ago
Agree, I've tested it in my tenant, when used wildcard I'm still able to share to that domain.
upvoted 4 times

Azreal_75 1 year, 1 month ago
Meaning the wildcard didn't work in so much that adding a blocked domain of domain*.com didn;t prevent invites being sent to domain1.com?

Surely the fact that wildcards are not supported should be sufficient justification in itself for us to assume that the configuration the 1st exhibit is invalid and wouldn't do anything?

I hate the way microsoft does this sort of thing! :D
upvoted 4 times

Fegoseen Highly Voted 1 year, 6 months ago
The answer is not correct. It should be N-Y-N.
Fabrikam1.com is not the same domain as Fabrikam.com. Only Fabrikam.com is blocked. So user2@fabrikam1.com is allowed and can invited and share collection1.

Lastly, us.contoso.com is a subdomain of contoso.com. When you block a top-level domain, it will automatically block the subdomains. However, you can block a subdomain and it would not affect the top-level domain. You could see a reference below

https://github.com/MicrosoftDocs/office-docs-powershell/issues/2413

upvoted 10 times

jkklim 9 months, 2 weeks ago

please go and test before putting up answers here. domain*.com will block invite. Therefore it is NNY

upvoted 11 times

stoneface 9 months, 1 week ago

tested on my tenant, NNY seems the correct answer, correct me if am wrong

upvoted 6 times

Razuli 1 year, 5 months ago

see the wildcard "*" inside of fabrikam*.com, answer is n, n, y as far as I am aware

upvoted 7 times

nzboy123 1 year, 6 months ago

The answer is correct.
In the picture, the blocked domain is Fabrikam*.com meaning anything after Fabrikam is blocked, therefore Fabrikam1 is blocked a the user is not able to share.

upvoted 14 times

wonap 1 year, 5 months ago

shouldn't the third be on NO if you can't share with contoso.com?

upvoted 2 times

gladi 1 year, 5 months ago

External sharing is enabled for any domain except contoso.com.
Blocking sharing to contoso.com does not block sharing to us.contoso.com. Therefore, you can share Collection1 to user3@us.contoso.com.

upvoted 4 times

Azreal_75 1 year, 1 month ago

The syntax is incorrect though, wildcards can be used but only to the left of a domain name if separated by a "." to denote a subdomain, or to the right of a domain name of separated by a "/" to denote a path. Either way the syntax in the exhibit is wrong and *should* not work.

upvoted 2 times

Kainzor Most Recent 2 months ago

Answer is: YYY

Wildcards are not supported for domain entries, therefore it would work

upvoted 1 times

Stiobhan 4 months ago

Think we need to pay attention to the link from MallonoX - https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list?view=o365-worldwide#url-syntax-for-the-tenant-allowblock-list Hard to argue with that.

upvoted 1 times

Nilz76 6 months ago

A similar question to this was in my exam on 06/April/2022. I passed.

upvoted 1 times

joergsi 8 months, 1 week ago

The answer is YYY
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list?view=o365-worldwide#url-syntax-f the-tenant-allowblock-list

- Wildcards (*) are allowed in the following scenarios:
A left wildcard must be followed by a period to specify a subdomain.
For example, *.contoso.com is allowed; *contoso.com is not allowed.

=> fabrikam*.com is not allowed!

- The tilde (~) character is available in the following scenarios:
A left tilde implies a domain and all subdomains.
For example ~contoso.com includes contoso.com and *.contoso.com.

because the ~ is not been used:

=> contoso.com would be blocked
=> us.contoso.com would NOT be blocked!
upvoted 1 times

Davidchercm 8 months, 2 weeks ago
i thought contoso.com is under blocked domain . why is it a yes ?
upvoted 1 times

shifaneesa 8 months, 3 weeks ago
the answer is correct!
upvoted 1 times

TashaGirl 8 months, 3 weeks ago
100% Y N Y
In my tenant:
gimai*.com is blocked
contoso.com is blocked
Guest invite sent to:
gmail.com IS BLOCKED
gimai.com IS ALLOWED (INVITE SENT, USER CREATED)
us.contoso.com IS ALLOWED (INVITE SENT, USER CREATED)
upvoted 1 times

TashaGirl 8 months, 3 weeks ago
Wrong, sorry! Moderator please remove altogether
upvoted 2 times

FreddyLao 9 months, 3 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list?view=o365-worldwide#url-syntax-f
the-tenant-allowblock-list
Actually the answer should be Y-Y-N

fabrikam*.com is not a valid syntax
so 1 & 2 is YES.
us.contoso.com is blcoked by contoso.com
read the URL entry scenarios carefully
upvoted 1 times

davem90 10 months ago
N-N-Y is correct, blocking fabrikam*.com means that fabrikam.com and fabrikam1.com are both not allowed. Just test it, easy peasy le
squeezy!
upvoted 2 times

MallonoX 10 months, 3 weeks ago
the fabrikam*.com entry is invalid and would be ignored

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list?view=o365-worldwide#url-syntax-f
the-tenant-allowblock-list
upvoted 3 times

TimurKazan 11 months ago
I would go with Y-Y-Y
upvoted 2 times

AlexLiourtas 9 months, 4 weeks ago
??? how can you share with fabricam domain, when the domain is banned from invites.
upvoted 1 times

AlexLiourtas 9 months, 1 week ago
i ll correct my answer, it should be YYY. There is no wildcard domain at the end of the domain (e.g. wildcard*.com)
upvoted 1 times

haazybanj 1 year ago
The answer is correct. I tested it. NNY
upvoted 2 times

Lakes_Puma 1 year, 1 month ago
On the following link;
https://docs.microsoft.com/en-us/sharepoint/restricted-domains-sharing
Document dated 04/28/2021
There is the following text;

"
List the domains (maximum of 3000) in the box provided, using the format domain.com. If listing more than one domain, enter each domain on a new line.

Note
Wildcards are not supported for domain entries.
"
But I haven't tested this in any environment.
upvoted 1 times

Ash473 1 year, 1 month ago
In Exam today
upvoted 1 times

Noie 1 year, 2 months ago
Wildcard for fabrikan*.com will work. I tested it with the guest users
upvoted 2 times

You have a hybrid deployment of Microsoft 365 and an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

Password protection in Azure AD is configured as shown in the following exhibit.



Which users will be prevented from using the word `Contoso` as part of their password?

A. User1 only

B. User1 and User2 only

C. User1 and User3 only

D. User1, User2, and User3

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

Stiobhan Highly Voted 4 months ago

Defo just user 1 as the rule is enforced in Azure. User 2 is an on-prem account, rule is in audit mode so not enforced. Outlook account i irrelevant.
Answer is defo A
Can't believe I am paying for this stuff 😞

upvoted 8 times

biglittle323 3 months, 2 weeks ago

I think since the questions are accurate they can't have all the right answers or Microsoft would come crashing down on them hard.

upvoted 4 times

gaem Highly Voted 4 months, 2 weeks ago

Selected Answer: A

Wrong answer.
It should be A

upvoted 5 times

Kalzonee3611 4 months, 1 week ago

Audit mode is turned on, meaning this does not apply to on prem.

upvoted 2 times

Lekso Most Recent 1 month, 2 weeks ago

Password Protection for Window server Active Directory is also enabled so B is the answer.

upvoted 1 times

Chris7910 5 months, 1 week ago

Selected Answer: A

User 2 can use the password because it is in audit mode.
User 3 is a guest user, so answer a has to be correct

upvoted 4 times

ARYMBS 5 months, 1 week ago

Don't understand answers....
It is in audit mode??

upvoted 2 times

Question #59 *Topic 4*

You have a Microsoft 365 E5 subscription.

You need to ensure that users are prompted for multi-factor authentication (MFA) when they attempt to access Microsoft SharePoint Online resources. Users must NOT be prompted for MFA when they attempt to access other Microsoft 365 services.

What should you do?

A. From the Microsoft Endpoint Manager admin center, create an app protection policy.

B. From the multi-factor authentication page, configure the users settings.

C. From the Azure Active Directory admin center, create a conditional access policy.

D. From the Cloud App Security admin center, create an app access policy.

Correct Answer: *C*

Multi-factor authentication (MFA) is configured through conditional access policies.

Reference:

https://docs.microsoft.com/en-us/appcenter/general/configuring-aad-conditional-access

mkoprivnj Highly Voted 1 year, 9 months ago

C for sure!

upvoted 9 times

stoneface Most Recent 9 months ago

C is the chosen one!

upvoted 2 times

cloudboys 1 year, 3 months ago

correct !

upvoted 2 times

HOTSPOT -

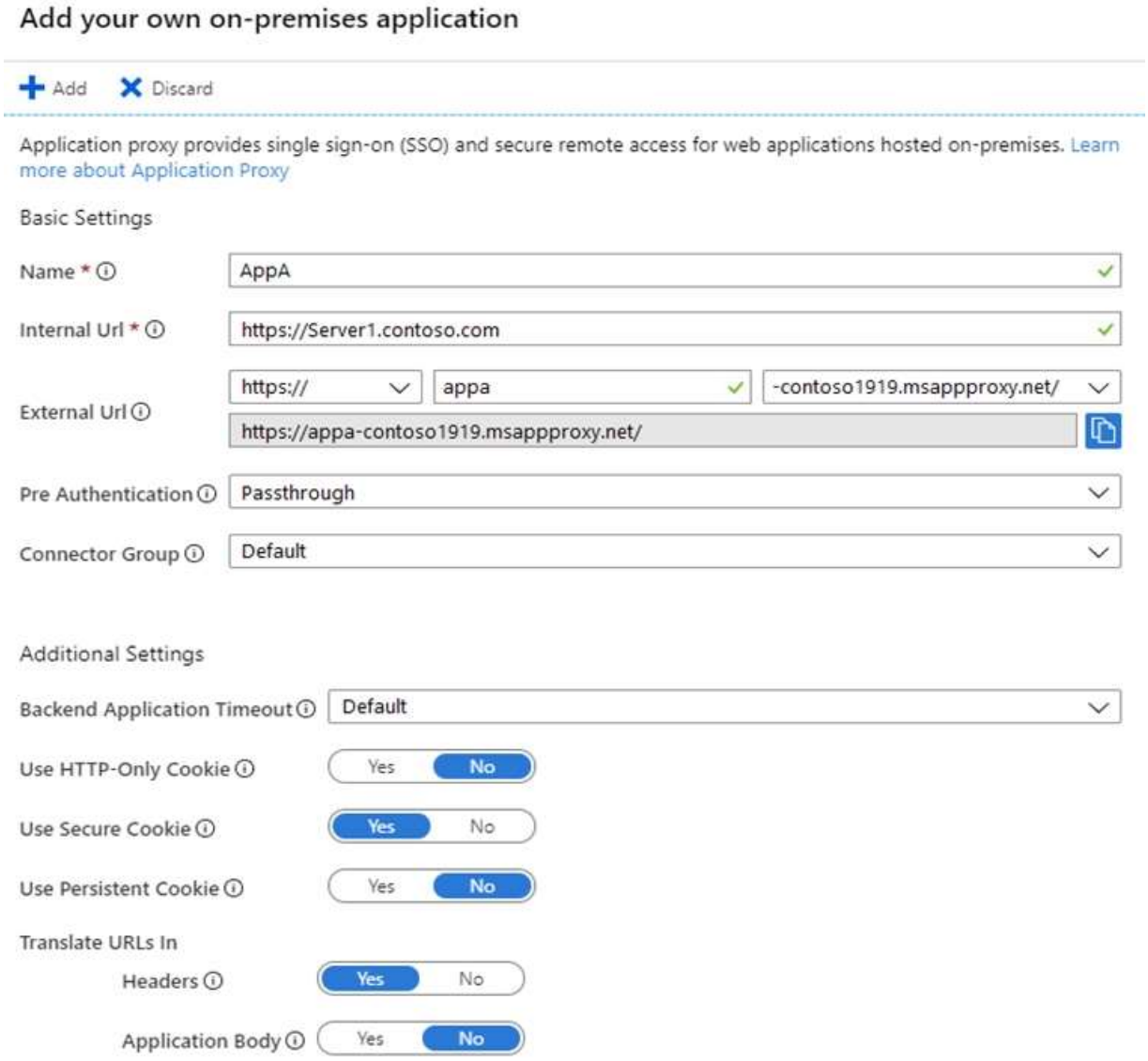
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Member of
User1	Group2
User2	Group1, Group2
User3	Group1

You have an on-premises web app named AppA. Group1 has permissions to access AppA.

You configure an Azure Active Directory (Azure AD) Application Proxy.

You add an Application Proxy entry for AppA as shown the exhibit. (Click the Exhibit tab.)



You assign the AppA enterprise application in Azure to Group2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can access AppA by using the external URL.	○	○
User2 can access AppA in the My Apps portal.	○	○
User3 can access AppA by using the external URL.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can access AppA by using the external URL.	○	●
User2 can access AppA in the My Apps portal.	●	○
User3 can access AppA by using the external URL.	○	●

Box 1: No -

User1 is in Group2. The enterprise app is assigned to Group2. However, the authentication method is ג€Passthroughג€ so the authentication will be passed to the on-premises web app. Only Group1 has access to the web app. Therefore, User1 will not be able to access the web app.

Box 2: Yes.

User2 is in Group1 and Group2. The enterprise app is assigned to Group2. The authentication method is ג€Passthroughג€ so the authentication will be passed to the on-premises web app. Group1 has access to the web app. Therefore, User2 will be able to access the web app in MyApps.

Box 3: No -

User3 is in Group1. Group1 has access to the web app so User3 could access the app on-premises. However, the enterprise app is assigned to Group2 which

User3 is not a member of. Therefore, User3 will not be able to access the external URL of the web app.

ilRobi Highly Voted 1 year, 1 month ago

The app is assigned to Group 2 in Azure. You cannot use the external URL or open the app via My Apps if you are not in Group 2. Therefore, User 3 will only be able to use the app from the on-premise network with the internal URL.

Pre-authentication is pass-through: the on-premise AD wins.
On-premise Group 1 (User 2 and User 3) has acces to the app.
Therefore User 2 can access the app.

User 1 with External URL? No.
User 2 from My Apps? Yes.
User 3 with External URL? No.

Am I missing something? I agree with the provided answers but other commenters' opinions seem to be all over the place?

upvoted 6 times

Durden871 7 months, 1 week ago

I find this question confusing.

User 1/Group 2 is assigned the web app. So, if I understand correctly, they try to authenticate, but because it's PTA it gets to the serv
where they don't have access to the app so they're not able to access the web app simply because they can't authenticate to it?

user3/group1 Have access to the enterprise app on prem, but because they don't have access to the web app, they can't use the external link for access, but can access the app locally.

Since User2 is assigned to both groups, they can authenticate because they're assigned the enterprise app and can access it externa
because they are granted web app access.
upvoted 1 times

Gresch123123 Most Recent 6 months, 2 weeks ago
Provided answer makes sense, NYN
upvoted 1 times

Wojer 8 months, 1 week ago
I am not an expert but because it's PTA auth. everything is sent to on-prem server so in my opinion its NYY as an answer.
upvoted 1 times

joergsi 8 months, 1 week ago
The provided explanation:
Box 3: No -
User3 is in Group1. Group1 has access to the web app so User3 could access the app on-premises. However, the enterprise app is assigned to Group2 which
User3 is not a member of. Therefore, User3 will not be able to access the external URL of the web app.

Does not make sense at all, because => However, the enterprise app is assigned to Group2 is not shown in the screenshot!

It should be Y
upvoted 1 times

tf444 9 months, 2 weeks ago
the explanation is wrong, nowhere in the question indicates Group1 has access to the web. app .
You have an on-premises web app named AppA. Group1 has permissions to access AppA.
upvoted 2 times

gonick 1 year ago
In the properties sheet for the app is a slider "User assignment required?". This is set to Yes as default. When set to 'Yes', users will NOT
able to access using the external URL unless authorised to do so, in this case be a member of Group 2.

since we cant see the slider in this example, assume it's default to 'Yes', so User 3 can't access. NYN.
upvoted 3 times

gkp_br 1 year, 3 months ago
User need to be member of both groups: "You have an on-premises web app named AppA. Group1 has permissions to access AppA." a
"You assign the AppA enterprise application in Azure to Group2."
upvoted 4 times

F_M 1 year, 4 months ago
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application#add-an-on-premise
app-to-azure-ad

I think it's No | Yes | Yes. The reference states that with Passthrough pre-authentication AzureAD auth is bypassed so basically anyone
use the external URL and the authentication is managed by the backend of the App. Since on-prem the app is configured to grant acces
only to group 1 members User1 can't access while User 2 and 3 can. User1 anyway is blocked on the backend side, he can still use the u
but fails the authentication on the app.
upvoted 4 times

ilRobi 1 year, 1 month ago
Pass-through skips the Azure AD authentication steps, but does it also _not_ check wether the user is assigned the app or not? The t
things do not sound mutually exclusive to me.
upvoted 1 times

lucidgreen 1 year, 5 months ago
I'm thinking Y, Y, N...
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn383639(v=ws.11)
upvoted 2 times

melatocaroca 1 year, 4 months ago
usr 1 member of grp 2
usr 2 member of grp 1 and gpr2
usr 3 member of grp 1

You assign the AppA enterprise application in Azure to Group2.

usr 1 member of grp 2 gpr2 have access to app, Y
usr 2 member of grp and 1 gpr2, pr2 have access to app, Y
usr 3 member of grp 1 ; gpr1 have no access to app, N
upvoted 1 times

AlexLiourtas 9 months, 3 weeks ago

group1 not group2, group1 has permissions

upvoted 1 times

TheWallPTA 1 year, 5 months ago

User 3 not having access does not make sense to me? Part of Group 1.

upvoted 2 times

lucidgreen 1 year, 5 months ago

Same here. I'm pretty sure User3 doesn't have access, otherwise, what's the point of assigning access?

upvoted 1 times

balajim212 1 year, 5 months ago

True, Group1 has permissions to access AppA & User3 is a member of Group1. Ans should be Yes.

upvoted 1 times

balajim212 1 year, 5 months ago

My bad, external URL access is via Azure app group access, which is only Group2. Group 1 will give on-premises app access. Henc
no access here.

upvoted 1 times

Question #61 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.
You need to be notified if the SharePoint policy is modified in the future.
Solution: From the SharePoint site, you create an alert.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You need to create a threat management policy in the Security & Compliance admin center.

davem90 10 months ago

Selected Answer: B

From a sharepoint SITE, you can create alerts on files and folders and get notifiied when changes occur

https://support.microsoft.com/en-us/office/create-an-alert-to-get-notified-when-a-file-or-folder-changes-in-sharepoint-e5a79e7b-a146-46da-a9ef-d65409ba8918

upvoted 2 times

bog23 1 year, 6 months ago

FOR SURE NO NO NO

upvoted 2 times

bog23 1 year, 6 months ago

I MENT YES, NOT SORRY

upvoted 1 times

bog23 1 year, 6 months ago

IT'S NO FOR SURE

upvoted 2 times

umpalumpa 1 year, 5 months ago

FUCK U FOR SURE

upvoted 31 times

Luthercrop 1 year, 2 months ago

HAHAHAHA this was a great commercial break

upvoted 2 times

AlexLiourtas 9 months, 4 weeks ago

WHAT IS HAPPENING

upvoted 1 times

mkoprivnj 1 year, 9 months ago

No for sure!

upvoted 4 times

VTHAR 1 year, 11 months ago

The correct answer is A. Yes

It does meet the goal.

upvoted 1 times

Logico 1 year, 11 months ago

Answer is B. An alert in SharePoint covers changes to documents within document libraries, not policy changes.
upvoted 2 times

Logico 1 year, 11 months ago
Answer is B. An alert in SharePoint covers changes to documents within document libraries, not policy changes.
upvoted 7 times

Jhill777 2 years, 4 months ago
No option to alert on policy modification from the SPO site. Only file/folder mods. Not sure where policy mod notifications are set...if th
exist.
upvoted 3 times

Myko 2 years, 3 months ago
In Office 365 Security and Compliance Center, you can create an alert polity based on activity "Changed a sharing policy".
upvoted 12 times

adaniel89 1 year, 3 months ago
Absolutely!

https://protection.office.com/alertpolicies
"Changed a sharing policy"
An administrator changed a SharePoint sharing policy by using the Office 365 Admin center, SharePoint admin center, or ShareP
Online Management Shell. Any change to the settings in the sharing policy in your organization will be logged. The policy that wa
changed is identified in the ModifiedProperty field property when you export the search results.

Answer should be Yes
upvoted 1 times

chaoscreater 1 year, 3 months ago
NONE of that is a "from the Sharepoint site", which is what the question is asking. Sharepoint site alerts are for alerting on e.g
document changes, not policy changes. Did you even read your own answer?
upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.
You need to be notified if the SharePoint policy is modified in the future.
Solution: From the SharePoint admin center, you modify the sharing settings.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You need to create a threat management policy in the Security & Compliance admin center.

melatocaroca 1 year, 3 months ago
If the question is can and alert to send and adviseYES, can be Done from Sharepoint site, answer NO,

An admin in your organization creates, configures, and turns on an alert policy by using the Alert policies page in the compliance cente
You can also create alert policies by using the New-ProtectionAlert cmdlet in Security & Compliance Center PowerShell.

So answer B is correct

https://docs.oracle.com/en/cloud/paas/casb-cloud/palug/creating-policy-alerts-office-365-sharepoint-and-onedrive.html#GUID-95884D
9287-468E-B26D-82CCFF160489
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide
upvoted 1 times

mkoprivnj 1 year, 9 months ago
No for sure!
upvoted 2 times

titan_91 1 year, 10 months ago
The sharing settings in the Sharepoint Admin Center have already been modified to restrict external access. This alert needs to be configured in the Security & Compliance Center.
upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.
You need to be notified if the SharePoint policy is modified in the future.
Solution: From the Security & Compliance admin center, you create a threat management policy.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
We can create a threat management policy to alert us when the sharing policy is changed.
Create a new Alert policy > under Category select Threat Management > under 'Activity is' scroll down to the 'Site administration activities' and select 'Changed a sharing policy'.

sailerjerry Highly Voted 2 years, 8 months ago
An Alert Policy needs to be created not a Threat Management one. But there is no option for that.
upvoted 13 times

J0J0 1 year, 4 months ago
Alerts> Alert Policy
There is an option "Changed a sharing policy" in the Activity list.
upvoted 1 times

ssingh Highly Voted 2 years, 9 months ago
I think answer should be B. I believe an alert need to be created in security and compliance center. Anybody?
upvoted 9 times

itmp 2 years, 4 months ago
Answer is 100% correct.
SCC-> Alerts -> New alert policy -> Threat Management-> Activity is -> Changed a sharing policy.

The text displayed for this selection states:

"An administrator changed a SharePoint sharing policy by using the Office 365 Admin center, SharePoint admin center, or SharePoi
Online Management Shell. Any change to the settings in the sharing policy in your organization will be logged"
upvoted 29 times

mikerss 2 years, 3 months ago
Alert Policy is different from threat management policy
upvoted 9 times

Jayatheerthan 1 year, 11 months ago
ITMP is correct. I have checked in my tenant.
upvoted 6 times

jkklim Most Recent 9 months, 1 week ago
stick to NO.
upvoted 2 times

fofo1960 11 months, 2 weeks ago
Things changes, the new location is
https://security.microsoft.com/ then click on Policies & rules --> Alert Policy --> New Altert Policy --> set the Severity and category to wh
ever and click next ..
Now you can see the Activity is, and you can type the Site Administration ...
upvoted 2 times

girikedar 1 year ago

An Alert Policy Should be create Security & compliance > Alerts > Alert Policy and threat management....this is the correct answer..... so think answer is not right

upvoted 1 times

Mr01z0 1 year, 4 months ago

"Solution: From the Security & Compliance admin center, you create a threat management policy." this is worded poorly, the proposed solution is suggesting creating an alert policy in the category of "thread management".

upvoted 2 times

stromnessian 1 year, 7 months ago

Alert policy. Giving it a category of "Threat management" doesn't make it a threat management policy.

upvoted 4 times

mkoprivnj 1 year, 9 months ago

Yes for sure!

upvoted 3 times

Jake1 1 year, 10 months ago

I've tested this in our tenant and ssingh is right. Threat Management is a type of Alert Policy which you can configure along with DLP, Information Governance, Permissions, Mail Flow, and Others type of Alert Policy. Thus, the answer is correct. YES.

upvoted 3 times

Joshing 1 year, 11 months ago

I don't believe this is Threat Management Policy. Threat Management Policies are in Threat management section, this regards ATP. Tha section will not alert on administrative changes to SharePoint sites. Alerts then creating a New Alert Policy is the solution. You can categories the created alert policy as "Threat Management" but that's only for viewing in the alerts section as a category of alert.

upvoted 1 times

VTHAR 1 year, 11 months ago

The answer is "B. No". It doesn't meet the goal. Alert policy and threat management policy are different.

upvoted 1 times

TimurKazan 1 year, 1 month ago

when you create alert policy, you also choose category of it. So, you can choose threat management policy with required settings

upvoted 1 times

Benjam 2 years, 1 month ago

A is Correct
We can create a threat management policy to alert us when the sharing policy is changed.
Create a new Alert policy > under Category select Threat Management > under `Activity is' scroll down to the `Site administration activities' and select `Changed a sharing policy'.

upvoted 1 times

Benjam 2 years, 1 month ago

Given answer is correct A
We can create a threat management policy to alert us when the sharing policy is changed.
Create a new Alert policy > under Category select Threat Management > under `Activity is' scroll down to the `Site administration activities' and select `Changed a sharing policy'.

upvoted 1 times

shark1 2 years, 3 months ago

Once in a while, it's all No in this series question.

upvoted 4 times

saran1987 2 years, 3 months ago

They didnt provide the correct answer. The corract answer is creating a alert policy in Security in compliance. SCC - > Alerts -> Alert Poli -> New Alert Policy -> (Category: Information Governance) -> Activity: Site Administration Activity -> Changed a Sharing policy

upvoted 5 times

balouchi1964 2 years, 4 months ago

Correct Answer A
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-activity-alerts?view=o365-worldwide

upvoted 1 times

Greysi 2 years, 5 months ago

B is correct.
You must create an "Alert Policy" not a "Threat management Policy"

upvoted 5 times

Question #64 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Device Management admin center, you a trusted location and compliance policy.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You need to configure a conditional access policy, not a compliance policy.
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.
Reference:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

BDuff 8 months, 3 weeks ago
B all the way!
upvoted 1 times

mkoprivnj 1 year, 9 months ago
B for sure! configure a location-based policy must be configured!
upvoted 4 times

Jake1 1 year, 10 months ago
Answer is B is correct. This does NOT meet the requirement. You must configure a location-based policy which is done from AAD Conditional Access.https://docs.microsoft.com/en-us/sharepoint/control-access-based-on-network-location
upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You need to configure a trusted location and a conditional access policy.
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.
Reference:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

mkoprivnj 1 year, 9 months ago
No for sure!
upvoted 2 times

Jake1 1 year, 10 months ago
Answer is correct. Location-based policies are done through AAD Conditional Access Policies.https://docs.microsoft.com/en-us/sharepoint/control-access-based-on-network-location
upvoted 4 times

BRZSZCL 3 months, 3 weeks ago
@jake1
Your answer belongs to the following question 63. The correct answer for Q62 is "no".
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.
With named locations, you can create logical groupings of IP address ranges, for example your office IP range. You can then mark the named location as a trusted location.
Mark as trusted location - A flag you can set for a named location to indicate a trusted location. Typically, trusted locations are network areas that are controlled by your IT department.
You would then configure the conditional access policy to allow access only from the trusted location.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

mkoprivnj Highly Voted 1 year, 9 months ago
Yes for sure!
upvoted 8 times

Jake1 Highly Voted 1 year, 10 months ago
Answer is correct. This is done by creating a location based policy from AAD Conditional Access Polices.https://docs.microsoft.com/en-us/sharepoint/control-access-based-on-network-location
upvoted 5 times

Alv86 Most Recent 6 months, 2 weeks ago
You can also set this through sharepoint access control panel
Control access to SharePoint and OneDrive data based on network location
https://docs.microsoft.com/en-us/sharepoint/control-access-based-on-network-location
upvoted 1 times

[Removed] 1 year, 9 months ago
Answer: A
The previous proofs mentioned the conditional access policy from Sharepoint admin center however here the question mention AAD Admin center
The correct justification are the below
Create a Cloud App restriction:
https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#office-365

Create a location restriction:
https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/concept-conditional-access-conditions#locations
upvoted 4 times

Nunununu 1 year, 6 months ago
This seems to be the correct explanation
upvoted 1 times

HOTSPOT -

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Compliant
User2	Group1, Group2

The domain contains the devices shown in the following table.

Name	Compliance status
Device1	Compliant
Device2	Noncompliant

The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.

Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	*None*	All device states	Devices marked as compliant	Block access
Policy2	Group1	Group2	*None*	*None*	Block Access
Policy3	Group1	*None*	All device states	*None*	Grant access

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	○	○
User2 can access App1 from Device1.	○	○
User2 can access App1 from Device2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	○	○
User2 can access App1 from Device1.	○	○
User2 can access App1 from Device2.	○	○

Box 1: Yes.

User1 is in a group named Compliant. All the conditional access policies apply to Group1 so they don't apply to User1.

As there is no conditional access policy blocking access for the group named Compliant, User1 is able to access App1 using any device.

Box 2: Yes.

User2 is in Group1 so Policy1 applies first. Policy1 excludes compliant devices and Device1 is compliant. Therefore, Policy1 does not apply so we move on to

Policy2.

User2 is also in Group2. Policy2 excludes Group2. Therefore, Policy2 does not apply so we move on to Policy3.

Policy3 applies to Group1 so Policy3 applies to User2. Policy3 applies to 'All device states' so Policy3 applies to Device1. Policy3 grants access. Therefore,
User2 can access App1 using Device1.
Box 3: No.
User2 is in Group1 so Policy1 applies. Policy1 excludes compliant devices but Devices is non-compliant. Therefore, User2 cannot access App1 from Device2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

d3an Highly Voted 2 years, 8 months ago
The core principles here are:
1. All Conditional Access policies in scope are applied and merged together - there is no priority order for CA policies.
2. Block access always wins over Allow access.
3. Exclude always wins over Include.

So on that basis, the answers should be No, Yes, No.
upvoted 24 times

Hani_Ajaj 1 year, 7 months ago
So on that basis, the answers should be No, No, No.
upvoted 2 times

fridrix 2 years, 7 months ago
Should be Yes, Yes, No for me since user1 excluded from policy1 and then N/A at the rest. Isn't it Allow if none of the policies applied
upvoted 16 times

JNeto 1 month, 2 weeks ago
Also agree, only applies for group 1 so Y,Y,Y.
Thanks to all.
upvoted 1 times

WoneSix 2 years, 7 months ago
Fridrix is right, and here's why:
The policies only apply to members of Group1. If you are not a member of Group1, you get access, unless there is a policy that D
apply to your group. No policy applies to the Compliant group, so User1 can access from any device.
For User2, Policies 1 and 3 apply (Group2 is excluded from Policy2). Policy 1 blocks access to noncompliant devices and both allow
access to compliant devices. Since Blocks beat out Allows, User2 can acess from Device1 and not from Device2.
Overall answer is YES YES NO. How the answer supplied was determined is beyond me.
upvoted 45 times

STFN2019 2 years, 2 months ago
That is the best answer and the correct one too! Thanks WoneSix.
upvoted 2 times

donathon 2 years ago
I think likewise. Since the whole purpose of the conditional policy is to control the access of the app name App1, if the user is
even in the include, the user should not have access at all.
upvoted 1 times

Moji1 Highly Voted 2 years, 9 months ago
User 1 should have access because user 1 is neither member of group 1 nor group 2. So, the conditional access should not apply to thi
user because conditional access will only apply to the members of groups 1 or 2. Any idea ???
upvoted 19 times

AlexanderSaad 2 years, 6 months ago
Correct.
upvoted 4 times

davem90 Most Recent 10 months ago
Y,Y,N is correct, just tested!
upvoted 3 times

sabin001 10 months, 2 weeks ago
Answer are correct. Tested!!
upvoted 2 times

TimurKazan 1 year ago

correct
upvoted 1 times

itstudy369 1 year, 3 months ago
Multiple Conditional Access policies may apply to an individual user at any time. In this case, all policies that apply must be satisfied. Fo example, if one policy requires multi-factor authentication (MFA) and another requires a compliant device, you must complete MFA, an use a compliant device. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must b satisfied to trigger a policy.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies
upvoted 1 times

TheWallPTA 1 year, 6 months ago
So if Lynxy is correct and table one is incorrect:

"The first table is incorrect - this should read
User 1 - Group 1"

Would that change the first question? Think it Might be NYN in that case?
Policy 1 should take priority with the block access over Policy 3?
upvoted 2 times

lucidgreen 1 year, 7 months ago
The access is granted by hierarchy. Policy 1 is applied first, Policy 2 second and Policy 3 is the catch all at the end.
User 1 has no policies applied to it. So all access, I believe. There appears to be no policy prohibiting User 1's access to App 1 unless the is a rule that says you have access only if you meet one of these criteria.
User 2 cannot access App 1 on non-compliant devices. Device 1 is compliant. Device 2 is not.
Yes?
Yes.
No.
upvoted 2 times

lucidgreen 1 year, 6 months ago
Also, remember that the policies don't apply to User 1. No policy equals no restrictions.
upvoted 1 times

Mriji 1 year, 8 months ago
The first table is wrong, as Lynxy has stated.
upvoted 1 times

ibalsayed 1 year, 8 months ago
in policy2 the device state include is "none", so I think the policy has no effect even on user1 or user2
upvoted 1 times

us3r 1 year, 8 months ago
Yes
Yes
No
upvoted 6 times

VTHAR 1 year, 11 months ago
I have my doubt on this question and not sure if the first table is accurate. Here is the answers for different scenarios ...

If User1 is member of "Compliant" group, YES YES NO.
If User1 is member of "Group1" group, NO YES NO.
upvoted 11 times

donathon 2 years ago
1. None of the policy will apply to user1 because he is not in Group1.
2. Policy1 will not apply because User2 is in Group1 and device is compliant which is excluded from the policy. Policy2 will not apply to User2 because he is also part of Group2 which means he is excluded. Policy3 will apply because User 2 is in Group1 and Policy3 allows device states. Hence he will be granted access.
3. Policy1 will apply because User2 is in Group1 and the device state is noncompliant which the exclusion does not apply. Hence the ac will be blocked. No need to go to other 2 policy as block wins over grants.
upvoted 1 times

moh15 2 years ago
N N N correct
upvoted 3 times

Mike_Row 2 years ago
Policy 1 does not apply, Device 1 is excluded because it is compliant.
Policy 2 does block access because User 1 is in group 1 and not in the excluded group 2.

Answer N

Policy 1 does not apply, Device 1 is compliant and excluded.
User 2 is member of Group 2, so Policy 2 does not apply because Group 2 is excluded.
Policy 3 does apply, User2 is member of group 1, and there are no device status configured.
Answer Y

Policy 1 does apply, User 2 is member of group 1, Device 2 is Noncompliant.
Answer N

NYN

upvoted 5 times

Mike_Row 2 years ago

Sorry, my question was a bit different.

Name member of
User 1 Group 1
User 2 Group 1, Group 2

But a group named "Compliant" doesn't make sense.., so I think I got the new version.

upvoted 3 times

STFN2019 2 years, 2 months ago

WoneSix explanation is the right answer to this question. It's Y,Y,N thx

upvoted 3 times

Lynxy 2 years, 3 months ago

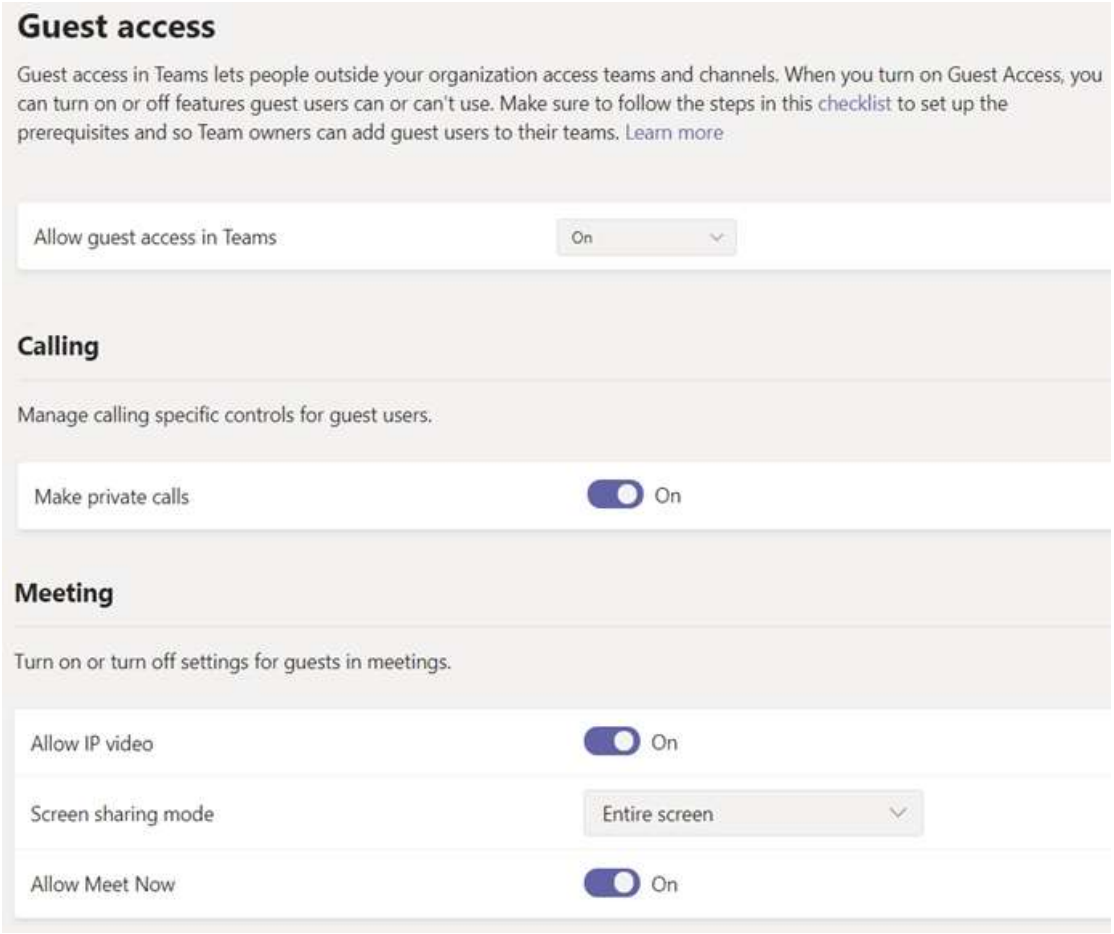
The first table is incorrect - this should read
User 1 - Group 1
User 2 - Group 1, Group 2

upvoted 7 times

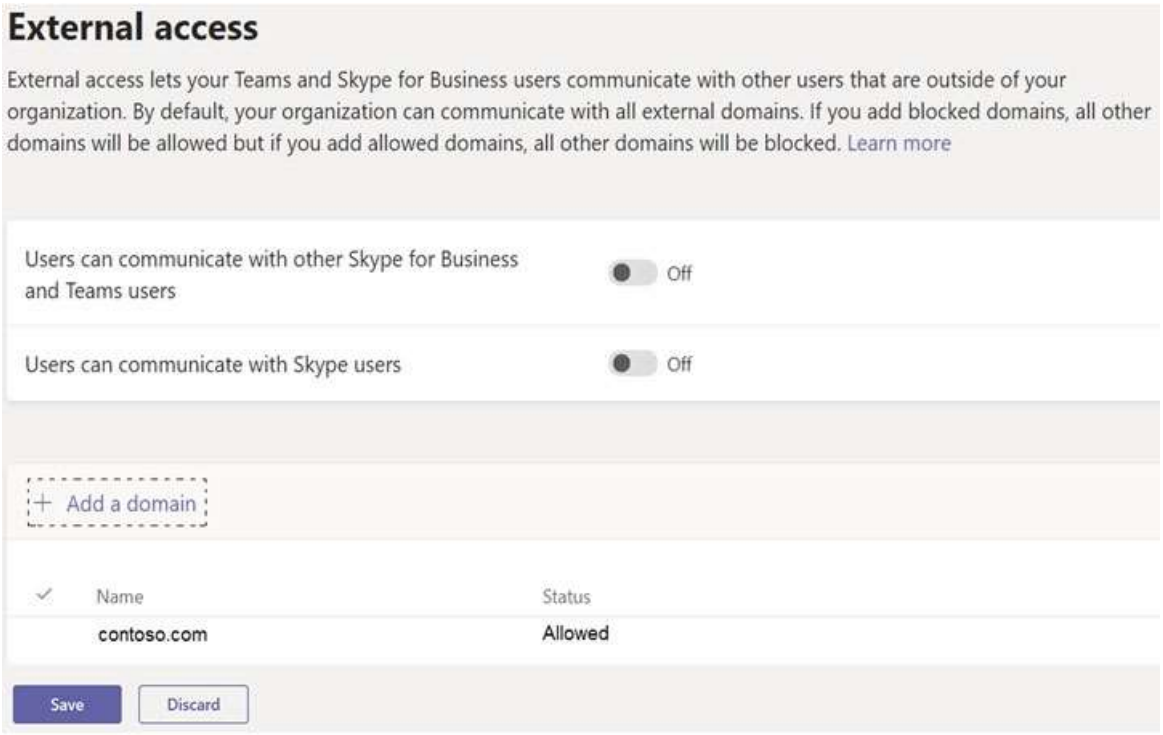
HOTSPOT -

Your company has a Microsoft 365 tenant named litwareinc.com.

The Guest access settings in Microsoft Teams are configured as shown in the following exhibit.



The External access settings in Microsoft Teams are configured as shown in the following exhibit.



The company has a third-party supplier named adventureworks.com. Users in litwareinc.com collaborate with the following users by using Microsoft Teams:

- User1@contoso.com
- User2@adventureworks.com

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User2@adventureworks.com can share files by using a Microsoft Teams channel of litwareinc.com.	○	○
User1@contoso.com can use Meet now in Microsoft Teams.	○	○
Litwareinc.com users can block user1@contoso.com in Microsoft Teams.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User2@adventureworks.com can share files by using a Microsoft Teams channel of litwareinc.com.	○	○
User1@contoso.com can use Meet now in Microsoft Teams.	○	○
Litwareinc.com users can block user1@contoso.com in Microsoft Teams.	○	○

The answer to this question depends on whether User1 and User2 have been added as guests. The question does not say that they are guests so we would have to assume they're not.

External Access is turned off. Even with the Contoso.com domain added as an allowed domain, the Off settings override this. If the external access settings were

'On', they would be on for only the Contoso.com domain.

Box 1: No -

If External Access was On, the answer to this would still be No. If User2 was a guest, the answer to this would be Yes.

Box 2: No -

If External Access was On, the answer to this would still be No. External Access does not enable Meet Now for the external user. If User1 was a guest, the answer to this would be Yes.

Box 3: No -

If External Access was On, the answer to this would still be No. External Access does not allow blocking. If User1 was a guest, the answer to this would be Yes.

Reference:

https://docs.microsoft.com/en-us/microsoftteams/set-up-guests https://docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations

Turak64 Highly Voted 1 year, 1 month ago

Horrible question, you should never had to presume an important piece of info that could change the answers! Shame on MS for puttin low quality, trick question in the exam.

upvoted 25 times

MomoLomo Highly Voted 1 year, 1 month ago

The company has a third-party supplier named adventureworks.com. Users in litwareinc.com collaborate with the following users by us Microsoft Teams:

- User1@contoso.com

User2@adventureworks.com

The are already added as guest if they are already collaborating in teams
upvoted 7 times

MomoLomo 1 year, 1 month ago
Guest access:
"Use guest access to add a person from outside your organization to a team, where they can chat, call, meet, and collaborate on file

And they are already collaborating as the question says therefore they should be added already as guests

Y Y N
upvoted 1 times

allesglar 11 months ago
And why third statement is N?
upvoted 2 times

ACTOSA Most Recent 1 month ago
So i agree the first has to be an N. You cant have external people sharing. Adventureetc is the guest user which it has been shared with
upvoted 1 times

itmaster 5 months, 4 weeks ago
"Users in litwareinc.com collaborate with the following users by using Microsoft Teams" don't we understand from this statement in the question that user1 and user2 are already added as guests?!

I would answer as YYY
upvoted 1 times

Nilz76 6 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 4 times

gottastudyeh 5 months, 3 weeks ago
You have said this on loads of questions but not told us the answer you chose and so it's pointless information really..
upvoted 6 times

Kalzonee3611 4 months, 1 week ago
No it isn't. He's letting us know the question is still relevant.
upvoted 6 times

TashaGirl 8 months, 3 weeks ago
Block is for school, personal or small business only.
https://support.microsoft.com/en-us/office/block-a-contact-025e381e-8bff-4370-9a7f-c7ed7ebdcca7
upvoted 2 times

TashaGirl 8 months, 3 weeks ago
not even school actually
upvoted 1 times

TimurKazan 11 months ago
If it says they collaborate using teams, that should mean they can reach each other, hence they are guests. in this case I would choose Y
upvoted 3 times

Ash473 1 year, 1 month ago
in exam today
upvoted 4 times

melatocaroca 1 year, 3 months ago
IMHO External access (federation) By default, external access is enabled for all domains. they do not tell us, the thirty party company is federated, we assume, NO, they do not Tell us if was invited as guest, so assume NO as well so assuming NO as default when not speci instructions were gave it yo us ANSWER NO, NO, NO
upvoted 2 times

gsmith9897 1 year, 3 months ago
"Users in litwareinc.com collaborate with the following users by using Microsoft Teams: User1@contoso.com, User2@adventureworks.com" If so, they must have been added as guests. It's a question of what access they have, not whether or not they're guests.
upvoted 2 times

adaniel89 1 year, 3 months ago

Whilst they are independent features, Guest Access only come into effect if "Provided that the user has been added as a guest and is signed with the guest account"
https://docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations

Since there is no mention of adventurework.com or contoso.com being invited as Guests, we have to assume that they dont have Gues account and therefore - NO/NO/NO

upvoted 3 times

Ronger 1 year, 3 months ago

There is:
"Users in litwareinc.com collaborate with the following users by using Microsoft Teams: User1@contoso.com, User2@adventureworks.com"

upvoted 2 times

itstudy369 1 year, 3 months ago

Provided answers are correct. ref: https://docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organization

upvoted 1 times

LoremanReturns 1 year, 3 months ago

In my opinion the correct answer is YES, YES, NO. Guest Access and External Access are indipendent features that works on different layers: https://docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations

upvoted 3 times

chaoscreater 1 year, 3 months ago

Agreed.

Did you even bother reading the link you posted?

External access:
"Set up external access if you need to find, call, chat, and set up meetings with people outside your organization who use Teams, Sk for Business (online or on premises) or Skype."

Guest access:
"Use guest access to add a person from outside your organization to a team, where they can chat, call, meet, and collaborate on file

"meet and collaborate on files" is what the question is asking in questions 1 and 2. So no,

upvoted 2 times

michszym 1 year, 3 months ago

I think answer should be YYY:
1st Y - they have already guest accounts ("Users in litwareinc.com collaborate with the following users") so user2 can share files
2nd Y - the same reason - User1 can use Meet now
3rd Y - see link you provided - table "Things your users can do" and there is "Block someone in another organization" - Yes for "Gues access"

upvoted 3 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1, Group2	Enabled
User3	Group2	Disabled

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

Assignments:

▪

- Include: Group1
- Exclude: Group2

⇨ Access controls: Require Azure MFA registration

⇨ Enforce Policy: On

You create a conditional access policy that has the following settings:

⇨ Name: Policy1

⇨ Assignments:

- Include: Group2
- Exclude: Group1

⇨ Access controls:

- Grant, Require multi-factor authentication

⇨ Enable policy: On

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 will be required to use MFA on the next sign-in.	○	○
User2 will be required to use MFA on the next sign-in.	○	○
User3 will be required to use MFA on the next sign-in.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 will be required to use MFA on the next sign-in.	○	○
User2 will be required to use MFA on the next sign-in.	○	○
User3 will be required to use MFA on the next sign-in.	○	○

Box 1: No -

The MFA policy applies to User1 so he will be prompted to register for MFA. He has 14 days to complete the registration. During this 14-day period, he can bypass registration but at the end of the period he will be required to register before he can complete the sign-in process.

The Conditional Access Policy does not apply to User1 so MFA is not required.

Box 2: No -
User2's MFA status is Enabled which means he has been enrolled in MFA but has not yet completed the registration.
The Conditional Access Policy does not apply to User2 because Group1 is excluded so MFA is not required.

Box 3: Yes -
The Conditional Access Policy does apply to User3 so MFA will be required. He will need to be enrolled for MFA first.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy
https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

stromnessian Highly Voted 1 year, 2 months ago
2nd answer should be YES. User2 has MFA enabled in the per-user MFA settings, which means that MFA is enforced for that user - it is n
the same as "registered".
upvoted 12 times

michszym 1 year, 2 months ago
Agree, I've tested it - when you enable per-user MFA for user - he cannot bypass registration for 14 days. He has to use MFA nex sign
This has a priority over Registration policy
upvoted 7 times

MallonoX 10 months, 2 weeks ago
But Eser2 is a member of Group1. Exlusion take precedence over inclusion
upvoted 1 times

Durden871 6 months, 2 weeks ago
Yes, exclusion takes precedence over inclusion; however, block always wins over grant and there are two policies that User 2 belongs to, the second policy requires MFA. So, if policy 2 didn't exist, user 2 wouldn't require MFA. Since it does, most restrict policy wins here.
upvoted 1 times

Jubei612 Most Recent 6 months, 3 weeks ago
User 3 is in group 2 and they are set to exclude, so I'm confused on this one. Can anyone give me the reason why?
upvoted 1 times

Durden871 7 months, 1 week ago
Correct me if I'm wrong (likely am wrong)
Group 1 is no -
MFA is disabled
Policy applied only requires MFA to be registered. Not required to sign-in.

User 2 belongs to both groups. So, yes?
- User 2 has MFA enabled, but not enforced. They have been enrolled, but not completed the registration. Policy 1 will require you to register. Policy 2 is requiring MFA. They're a member of both groups. So both group policies apply.

User 3 is yes because of policy 2.

What am I missing?
upvoted 3 times

LillyLiver 8 months, 1 week ago
I see what's happening here. This was confusing for me to wrap my head around.

User1: No
True, there is an MFA policy applied to Group1. But User1 will not be REQUIRED to use MFA since the CAP is excluding Group1.

User2: No
I had to test this in my tenant. Apparently an explict Grant superceeds an explicit Block. So this ends up being the same as User1. Only already enabled.

User3: Yes
User3 is being targeted by the CAP only. So MFA will be required.

I agree with the given answer.
upvoted 1 times

Rickert 10 months, 2 weeks ago

Correct answer is No-Yes-Yes. Group1 is registration and group2 is require

upvoted 4 times

Zardu 11 months, 1 week ago

Here is a good resource for the differences between Disable, Enrolled and Enforced: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

upvoted 1 times

Aesam 1 year ago

why can't 14 days logic applied to user 3 if it can be applied to user 1? I believe answer should be Y Y Y , if we keep 14 days logic out

upvoted 1 times

jinxie 10 months, 2 weeks ago

because group two will not allow access without MFA. unlike the policy on group 1 which is a request for enrollment that can be postponed for 14 days the policy on group two demands you perform a MFA or you receive no access.

upvoted 2 times

Question #70 *Topic 4*

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure Active Directory (Azure AD).

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1.

What should you do?

A. From the Microsoft 365 admin center, configure the Modern authentication settings.

B. From Multi-Factor Authentication, configure the service settings.

C. From the Enterprise applications blade of the Azure Active Directory admin center, configure the Users settings.

D. From the Azure Active Directory admin center, create a conditional access policy.

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

RiTh73 7 months, 3 weeks ago

Selected Answer: D

Answer is correct

upvoted 1 times

Question #71 *Topic 4*

Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.
You plan to sync contoso.com to an Azure Active Directory (Azure AD) tenant.
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?

A. password synchronization

B. conditional access policies

C. pass-through authentication

D. Azure AD Identity Protection policies

Correct Answer: *C*
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

Topic 5 - Question Set 5

HOTSPOT -

You have a Microsoft 365 subscription that uses Microsoft Power Platform and contains production and sandbox environments.

You discover that a sandbox environment is marked as Inactive.

You need to identify the following:

- How many days before disabling the sandbox environment will administrators first be notified?
- What can you do to reactivate the environment?

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First notification:

- 1 day
- 7 days
- 14 days
- 21 days

To reactivate the environment:

- Convert the environment to production
- Purchase a license for the environment
- Purchase capacity for the environment
- Sign in to the environment

Correct Answer:

Answer Area

First notification:

- 1 day
- 7 days
- **14 days**
- 21 days

To reactivate the environment:

- Convert the environment to production
- Purchase a license for the environment
- **Purchase capacity for the environment**
- Sign in to the environment

Reference:

https://docs.microsoft.com/en-us/power-platform/admin/automatic-environment-cleanup https://docs.microsoft.com/en-us/power-platform/admin/recover-environment

KrisDeb 3 weeks ago

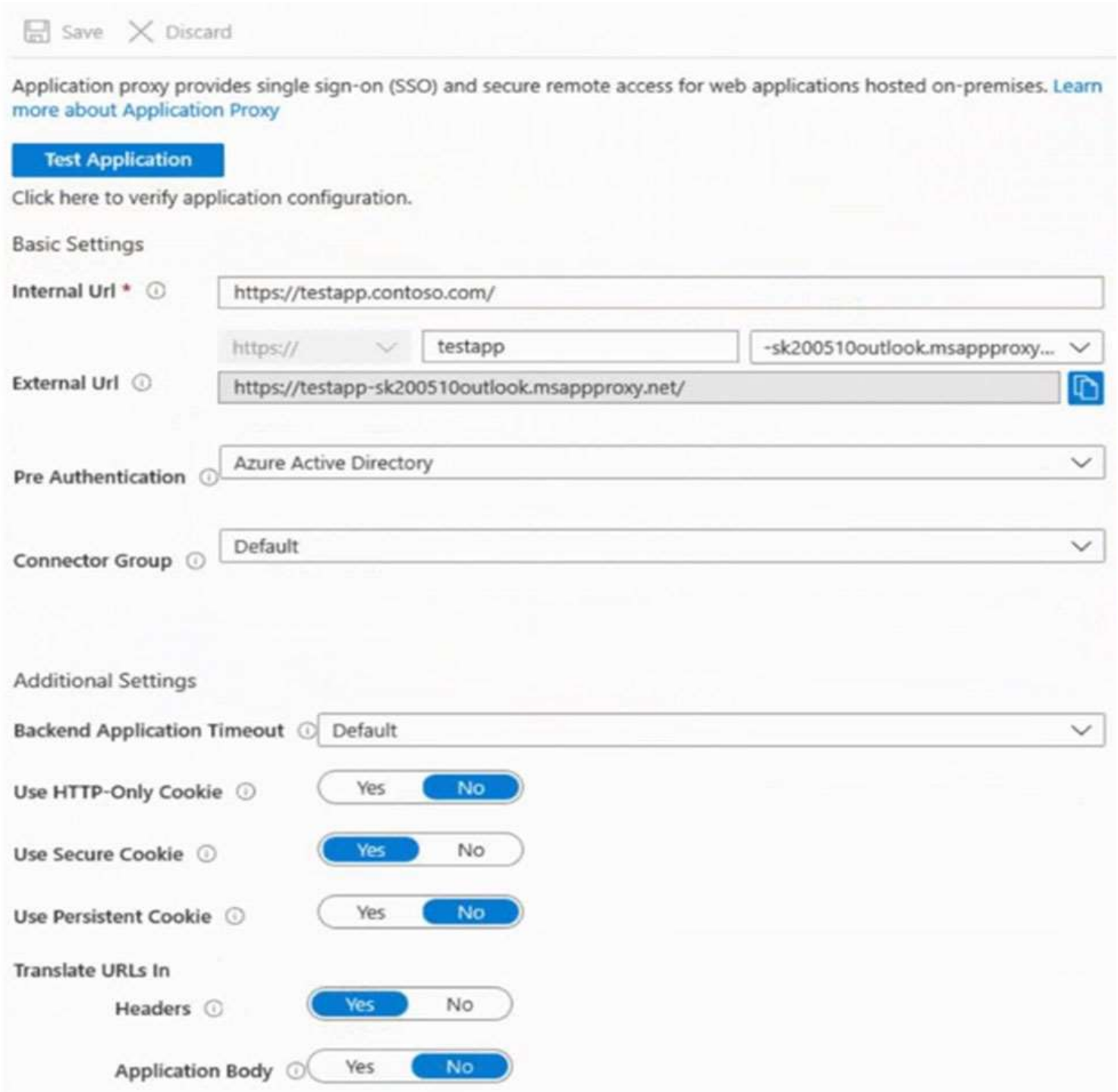
I think you need to buy the licenses, rather than the capacity which I understand are add-ons?

https://docs.microsoft.com/en-us/power-platform/admin/automatic-environment-cleanup#actions-you-can-take-to-prevent-environme
disabling-and-deletion

upvoted 4 times

HOTSPOT -

You are configuring an on-premises application named TestApp in Microsoft Azure as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To ensure that when users access TestApp, the proxy automatically scans for internal URLs published through the Application Proxy, set [**answer choice**].

- Use Http-Only Cookie to Yes
- Translate URLs in Headers to No
- Translate URLs in Application Body to Yes

To protect TestApp from Cross-Site Scripting (XSS), set [**answer choice**].

- Use Http-Only Cookie to Yes
- Translate URLs in Headers to No
- Translate URLs in Application Body to Yes

Correct Answer:

Answer Area

To ensure that when users access TestApp, the proxy automatically scans for internal URLs published through the Application Proxy, set [**answer choice**].

- Use Http-Only Cookie to Yes
- Translate URLs in Headers to No
- **Translate URLs in Application Body to Yes**

To protect TestApp from Cross-Site Scripting (XSS), set [**answer choice**].

- **Use Http-Only Cookie to Yes**
- Translate URLs in Headers to No
- Translate URLs in Application Body to Yes

Box 1: Translate URLs in Application Body to Yes.

If you set Translate URLs in application body to Yes, when your users access this application, the proxy will automatically scan for internal URLs that have been published through Application Proxy on your tenant.

Box 2: Use Http-Only Cookie to Yes.

The Use Http-Only Cookie setting allows Application Proxy to include the HTTPOnly flag in HTTP response headers. This flag provides additional security benefits, for example, it prevents client-side scripting (CSS) from copying or modifying the cookies.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-configure-hard-coded-link-translation

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-configure-cookie-settings

Jelly101 Highly Voted 1 year, 1 month ago

Got this question in the exam today

upvoted 8 times

TimurKazan Most Recent 1 year ago

correct

upvoted 3 times

Your company has an on-premises Microsoft Exchange Server 2013 organization.
The company has 100 users.
The company purchases Microsoft 365 and plans to move its entire infrastructure to the cloud.
The company does NOT plan to sync the on-premises Active Directory domain to Microsoft Azure Active Directory (Azure AD).
You need to recommend which type of migration to use to move all email messages, contacts, and calendar items to Exchange Online.
What should you recommend?

A. cutover migration

B. IMAP migration

C. remote move migration

D. staged migration

Correct Answer: *A*
A cutover migration and an IMAP migration do not require the company to sync the on-premises Active Directory domain to Microsoft Azure Active Directory
(Azure AD). Only a cutover migration meets the requirements in this question.
With a cutover migration, user accounts will need to be created in Azure Active Directory for each user. The mailboxes are all migrated in one go and MX records configured to redirect email to Microsoft 365.
Incorrect Answers:
B: Contacts, calendar items and tasks cannot be migrated with an IMAP migration.
C: A remote move migration requires a hybrid exchange configuration which requires that the on-premises Active Directory domain is synced to Microsoft Azure
Active Directory (Azure AD).
D: A staged migration is recommended when your source email system is Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007. You can't use a staged migration to migrate Exchange 2013 or Exchange 2010 mailboxes to Office 365. A staged migration also requires that the on-premises Active Directory domain is synced to Microsoft Azure Active Directory (Azure AD).
Reference:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365 https://docs.microsoft.com/en-us/exchange/mailbox-migration/what-to-know-about-a-staged-migration

STFN2019 Highly Voted 2 years, 2 months ago
A maximum of 2,000 mailboxes can be migrated to Microsoft 365 or Office 365 by using a cutover Exchange migration. However, it is recommended that you only migrate 150 mailboxes.
upvoted 15 times

titan_91 Highly Voted 1 year, 10 months ago
Answer is correct. Cutover migration is best for scenarios with under 2,000 Exchange mailboxes and a non-hybrid Exchange environme
(this scenario is migrating to Exchange Online from Exchange on-premises.

Reference:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365
upvoted 7 times

RiTh73 Most Recent 7 months, 3 weeks ago
Selected Answer: A
Answer A is correct
upvoted 1 times

mkoprivnj 1 year, 9 months ago
Cutover migration!
upvoted 4 times

HOTSPOT -

You have a Microsoft 365 subscription.

You use the Microsoft Office Deployment Tool to install Microsoft 365 Apps for enterprise.

You create a configuration file that contains the following settings.

```
<Configuration>
  <Add SourcePath="\\Server1\Office"
      OfficeClientEdition="32"
      Channel="SemiAnnual"
      AllowCdnFallback="False">
    <Product ID="0365ProPlusRetail">
      <Language ID="en-us" />
      <Language ID="ja-jp" />
    </Product>
    <Product ID="VisioProRetail">
      <Language ID="en-us" />
      <Language ID="ja-jp" />
    </Product>
  </Add>
  <Remove All="TRUE">
    <Product ID="0365ProPlusRetail">
      <Language ID="en-us" />
    </Product>
    <Product ID="VisioProRetail">
      <Language ID="en-us" />
    </Product>
  </Remove>
  <Updates Enabled="TRUE"
           UpdatePath="\\Server1\Office"
           Channel="SemiAnnual" />
  <Display Level="None" AcceptEULA="TRUE" />
  <Logging Level="Standard" Path="%temp%" />
</Configuration>
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The **[answer choice]** will be uninstalled from the computers.

- MSI version of Microsoft Visio only
- C2R version of Microsoft Visio only
- MSI and C2R versions of Microsoft Visio

If the Office share on Server1 is missing the Japanese language pack, Microsoft 365 Apps for enterprise will **[answer choice]**.

- be installed in English only
- be installed in a randomly selected language
- NOT be installed

Correct Answer:

Answer Area

The **[answer choice]** will be uninstalled from the computers.

- MSI version of Microsoft Visio only
- C2R version of Microsoft Visio only
- MSI and C2R versions of Microsoft Visio

If the Office share on Server1 is missing the Japanese language pack, Microsoft 365 Apps for enterprise will **[answer choice]**.

- be installed in English only
- be installed in a randomly selected language
- NOT be installed

Box 1:

The C2R (click-to-run) version of Microsoft Visio only will be uninstalled from the computers.

To remove the MSI version of Microsoft Visio, you would need to specify the RemoveMSI parameter. The RemoveMSI parameter is not configured in the configuration file in this question. Therefore, only the C2R version will be installed.

Box 2:

If the Office share on Server1 is missing the Japanese language pack, Microsoft 365 Apps for enterprise will be installed in English only.

In the configuration file, English is the first in the list above Japanese. Therefore, English is the primary language and the installation will continue in English only.

Reference:

https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool

Jelly101 Highly Voted 1 year, 1 month ago

Got this question in the exam today

upvoted 5 times

Nilz76 Most Recent 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 1 times

Scuzlebutt 7 months, 1 week ago

looks like microsoft updated this article
https://docs.microsoft.com/en-us/deployoffice/upgrade-from-msi-version

It now says:

If you're installing Microsoft 365 Apps from a location on your local network, such as a shared folder, make sure you've downloaded all possible language files to that folder. If any of the languages needed to install aren't available in that folder, the installation will continu but without those languages being installed. To avoid this situation, we recommend that you include AllowCdnFallback="True" in your configuration.xml file. This will use the Office Content Delivery Network (CDN) on the internet as a backup source from which to install language files.

upvoted 2 times

LillyLiver 8 months, 1 week ago

I set this up in my home lab.

If you set two languages and one isn't available from the source, AND the FallbackCDN is set to FALSE, the installation will not work. It w fail with an error code (which I don't have anymore) and you'll have to either set the FallbackCDN to TRUE or have an installation source that has both languages.

So, the answers are:
A: C2R of Visio, and
B: Not install

upvoted 4 times

jjong 1 year ago

i got this qns today

upvoted 2 times

leirbag 1 year ago

The japanese language pack wont be installed because of
<AllowCdnFallback="False"> - this line makes it so ODT cant goto the Content Delivery Network is anything is missing

https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options#allowcdnfallback-attribute-part-of-add-element

upvoted 4 times

You create a Microsoft 365 Enterprise subscription.
You assign licenses for all products to all users.
You need to prepare the environment to ensure that all Microsoft 365 Apps for enterprise installations occur from a network share. The solution must prevent the users from installing Microsoft 365 Apps for enterprise from the Internet.
You download the Office Deployment Tool (ODT).
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From your computer, run setup.exe /download downloadconfig.xml.

B. Create an XML download file.

C. From the Microsoft 365 admin center, deactivate the Office 365 licenses for all the users.

D. From each client computer, run setup.exe /configure installconfig.xml.

E. From the Microsoft 365 admin center, configure the Software download settings.

Correct Answer: *BDE*
You can use the Office Deployment Tool (ODT) to download the installation files for Microsoft 365 Apps for enterprise from a local source on your network instead of from the Office Content Delivery Network (CDN).
The first step is to create the configuration file. You can download an XML template file and modify that.
The next step to install Microsoft 365 Apps for enterprise is to run the ODT executable in configure mode with a reference to the configuration file you just saved.
In the following example, the configuration file is named installconfig.xml. setup.exe /configure installconfig.xml
After running the command, you should see the Office installation start.
To prevent the users from installing Microsoft 365 Apps for enterprise from the Internet, you need to configure the Software download settings (disallow downloads) in the Microsoft 365 admin center.
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-of-the-office-2016-deployment-tool#download-the-installation-files-for-office-365-proplus-from-a-local- source

lucidgreen Highly Voted 1 year, 5 months ago
You don't run the install when you're preparing the environment.
Create the download config.
Download using the config.
Restrict downloading from M365.
ABE
upvoted 26 times

TimNov 1 year, 4 months ago
You need to reference the xml in the setup.exe install which you can't do unless you create it in the first case. Personally in the past I done this with ABD.
upvoted 2 times

Velda 1 year, 3 months ago
You mean reference for the network share? This is done by option B (specify in the XML file). Option D is not necessary for that. B you have to restrict downloads, so option E has to be checked. -> ABE
upvoted 2 times

manis73 3 months, 2 weeks ago
Yep been looking at this a while now and I agree.
You can restrict downloads in admin portal > settings > org settings > Office Installation options > Installation tab
upvoted 1 times

melatocaroca 1 year, 3 months ago
Right,
1) create, file, downloadconfig.xml,
2) download created file, setup.exe /download downloadconfig.xml

3) From portal configure to avoid users can download,
https://docs.microsoft.com/en-us/deployoffice/manage-software-download-settings-office-365

4) ,copy downloadconfig.xml file and rename it as installconfig.xml,
5) run, setup.exe /configure installconfig.xml

they ask for three actions, so ... IMHO ABE
upvoted 4 times

Turak64 1 year, 1 month ago
Unless your PC is hosting the share for the deployment, option A doesn't apply
upvoted 1 times

mancio 2 months, 2 weeks ago
I can run setup.exe /download downloadconfig.xml and specify into xml file a share located on server.
upvoted 1 times

kanag1 8 months, 2 weeks ago
Thanks for the explanation mate !!
upvoted 1 times

AnoniMouse Highly Voted 1 year, 5 months ago
The correct answers should be ABD. I have been doing this for ages.

First you need to create a configuration XML file. Go to https://config.office.com and create a new XML configuration file that suites you needs. After that you save the file (i.e., download it locally)

The second step is to use the ODT to download the Office packages as stated in your XML configuration file by running SETUP.EXE /DOWNLOAD Name_Of_XML.XML. This will download the exact Office version with the parameters you created in step 1. After some tim the folder will contain the Office installation files ready to setup

The question states: "You need to prepare the environment to ensure that all Microsoft 365 Apps for enterprise installations occur from network share", and this is done by copying the entire folder on a network share, and then running SETUP.EXE /CONFIG Name_Of_XML.XML, this will install Office from your network share and not from other sources
upvoted 8 times

Velda 1 year, 3 months ago
This is not correct. You missing the fact that you need to "PREVENT the users from installing Microsoft 365 Apps for enterprise from Internet" which is done by option E. .First of all, question doesn't says that you need to install O365. Second, even if you install O365 from network share by setup.exe /config, it will not prevent users to install other O365 Apps from internet.
upvoted 6 times

FumerLaMoquette 1 year, 2 months ago
Yeah i agree with Velda. Initially i thought it was ABD, but the question did not require you to install. So no need for D.

Answer is ABE.
upvoted 4 times

Partylad Most Recent 1 month, 4 weeks ago
agree with ABE Question says to 'Prepare' the environment not install the product
upvoted 1 times

gaem 4 months, 2 weeks ago
Selected Answer: ABD
Correct answer is ABD
upvoted 1 times

miry117 8 months ago
Selected Answer: ABD
The same question in others platforms is A,B,D
upvoted 1 times

LillyLiver 8 months, 1 week ago
Answer should be A, B, and D.

This must be an old question with very different results than when I set this up in test.

1. Create the XML file (for ODT)
This sets up the parameters for installing Office on your local system. What languages, whether to use a FallbackCDN, and where the installation source is located. In this case it'll be on a local share.

2. Run .\setup.exe /download .\ODT_XML_Install.xml (From PowerShell)
This downloads the installation based on the configuration in the XML to an "Office" folder from where you launch the ODT setup.exe from.

3. Run .\setup.exe /configure .\ODT_XML_Install.xml (From PowerShell)
Finally, the '/configure' tells ODT to do the actual install using the same configuration in the XML.

I don't see anywhere in M365 to disable downloads. So I'm thinking MS has changed this and the question answers are likely different now.

- ODT XML Creation: https://config.office.com/deploymentsettings
- ODT Overview: https://docs.microsoft.com/en-us/deployoffice/office2019/deploy

upvoted 1 times

miry117 8 months, 2 weeks ago

Selected Answer: ABD

This question is duplicated with another. The correct answer are ABD.

upvoted 1 times

fofo1960 10 months, 3 weeks ago

The answers are between ABD and ABE, for me I will go for ABE, as the question ask to PREVENT users from connecting to the internet
This word make E a must to be selected.
Correct me if I was wrong.

upvoted 1 times

MomoLomo 1 year, 1 month ago

ABE

i will use D if need to download it but i'm only preparing so no need for that step now

upvoted 2 times

Doki 1 year, 1 month ago

Sort of a disingenuous question since really there should be FOUR steps. Since it's "prepare" and not "do the whole job" the given answ is correct though.

upvoted 3 times

MartiFC 1 year, 2 months ago

I sorry but, if the source of installation is avaiable from the network, why we have to download the setup to our computer? Is not installable over network? I think that the answer is correct

upvoted 1 times

F_M 1 year, 4 months ago

I think ABE is the correct solution.

E is needed to prevent users to download the office suite from the internet. I guess there is some kind of typo because the right option stays under M365 Admin Center > Settings > Org-wide settings > Office installation options but this disables the "Download Office" opt that appers in every user office home page.

For what concerns the rest, is required to prepare the environment to distribute Office and not to install it on computers, so D is not needed in this case. Instead is necessary to create a custom XML with the Office Customization Tool (B), place it in a shared folder and the setup.exe in download mode (A).

upvoted 2 times

Velda 1 year, 3 months ago

I agree! ABE is correct for me.
If there will be possible to check 4 correct options, answers will be ABDE. But there are 3 and the question says that you need JUST PREPARE the environment. Therefore D is not the necessary option (you don't need to install O365 yet).
But what question says that you have to do is:
1. Create XML file - you can configure NETWORK SHARE download location in the XML config file - option B.
2. Download O365 - it will be PREPARED on network share with specified parameters (in the XML file) - option A.
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-office-deployment-tool#download-the-installation-files-for-office-365-propl from-a-local-%20source

3. "PREVENT the users from installing Microsoft 365 Apps for enterprise from the Internet" which is done by option E.
Reference:
https://www.slashadmin.co.uk/prevent-users-from-installing-office-applications-themselves-office-365/

upvoted 5 times

DudleyYVR 1 year, 4 months ago

E is wrong - "prevent installing from Internet" so E is wrong. ABD is say

upvoted 1 times

Turak64 1 year, 1 month ago

E is exactly how you prevent users from download it

upvoted 1 times

HOTSPOT -

You create a Microsoft 365 subscription.

You plan to deploy Microsoft 365 Apps for enterprise applications to all the client computers at your company.

You prepare the following XML file for the planned deployment.

```
<Configuration>
 <Add OfficeClientEdition="32"
     Channel="Broad">
 <Product ID="0365ProPlusRetail">
   <Language ID="en-us" />
   </Product>
 </Add>
<Updates Enabled="TRUE"
         UpdatePath=""
         Channel="Targeted" />
<Display Level="None"
         AcceptEULA="TRUE" />
</Configuration>
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Office 365 ProPlus feature updates will be installed **[answer choice]**.

- once a month
- once every six months
- once a year

Office 365 ProPlus security updates will be installed **[answer choice]**.

- once a month
- every six months in January and July
- every six months in March and September

Correct Answer:

Answer Area

Office 365 ProPlus feature updates will be installed **[answer choice]**.

- once a month
- once every six months
- once a year

Office 365 ProPlus security updates will be installed **[answer choice]**.

- once a month
- every six months in January and July
- every six months in March and September

Box 1:

Microsoft 365 Apps for enterprise feature updates will be installed once every six months.

The Channel element in the configuration file is set to 'Targeted'. This means Semi-Annual Targeted.

To help your organization prepare for a Semi-Annual Channel release, Microsoft provides Semi-Annual Channel (Targeted). The primary purpose of this update channel is to give pilot users and application compatibility testers in your organization a chance to work with the upcoming Semi-Annual Channel release

Box 2:

Microsoft 365 Apps for enterprise security updates will be installed every six months in March and September.

A Semi-Annual Channel (Targeted) release with new features is expected to be released twice a year, in March and September.

The March and September feature releases for Semi-Annual Channel (Targeted) also include security and non-security updates that have been released previously in Monthly Channel.

Reference:

https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool#updates-element

https://docs.microsoft.com/en-us/deployoffice/overview-of-update-channels-for-office-365-proplus

Gus01 Highly Voted 1 year, 5 months ago

Box 2 is incorrect Security updates are applied every month no matter what channel you choose
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels

upvoted 23 times

encxorblood Highly Voted 1 year, 3 months ago

Wrong Box B. Security Updates every month.

upvoted 7 times

PmgCosta Most Recent 5 months, 1 week ago

From: https://docs.microsoft.com/en-us/deployoffice/update-channels-changes

Update channel New attribute value Previous attribute value

upvoted 1 times

PmgCosta 5 months, 1 week ago

After June 9, 2020, previous attribute values for each update channel will still be valid. For example, if you use Broad in your configuration XML file, Semi-Annual Enterprise Channel will be installed. We're keeping the previous attribute values valid so that yo don't have to update your existing configuration XML files.

upvoted 2 times

jkklim 9 months, 2 weeks ago

FEATURE update - once every 6 months (Jan and July)
SECURITY update - once a month

upvoted 4 times

junior6995 1 year ago

Outdated question, better skip this one.

upvoted 2 times

TimurKazan 1 year ago

1 - every six months for semi-annual
2 - security updates happen every month for any channel

upvoted 1 times

MomoLomo 1 year, 1 month ago

Security every month
Feature jan and july
https://docs.microsoft.com/en-us/deployoffice/update-channels-changes#office-deployment-tool

upvoted 1 times

melatocaroca 1 year, 3 months ago

Actually the file definition for channels is wrong in terms of Broad,
BOX 2 must be set to monthly

Channel="BetaChannel"
Channel="CurrentPreview"
Channel="Current"
Channel="MonthlyEnterprise"
Channel="SemiAnnualPreview"
Channel="SemiAnnual"

Semi-Annual Enterprise Channel previously was know as Broad
In addition to new features, update channels provide, as needed, security and non-security updates on a regular basis, every month. O a month, on the second Tuesday of the month

Reference

https://docs.microsoft.com/en-us/deployoffice/update-channels-changes
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#semi-annual-enterprise-channel-overview

upvoted 4 times

kkkeji 1 year, 6 months ago

As for Channel, it seems to have been changed to SemiAnnualPreview.
https://docs.microsoft.com/en-us/deployoffice/update-channels-changes#office-deployment-tool

upvoted 5 times

Your network contains the servers shown in the following table.

Server name	Software	Configuration
Server1	Windows Server 2008	Domain controller
Server2	Windows Server 2012	Domain controller
Server3	Microsoft Exchange Server 2007	*Not applicable*
Server4	Microsoft SharePoint Server 2010	*Not applicable*
Server5	Microsoft Lync Server 2013	*Not applicable*

You purchase Microsoft 365 Enterprise E5 and plan to move all workloads to Microsoft 365 by using a hybrid identity solution and a hybrid deployment for all workloads.

You need to identify which server must be upgraded before you move to Microsoft 365.

What should you identify?

A. Server2

B. Server3

C. Server5

D. Server1

E. Server4

Correct Answer: *B*

Exchange Server 2007 is not supported for a hybrid deployment.

Reference:

https://docs.microsoft.com/en-us/exchange/hybrid-deployment-prerequisites

mkoprivnj Highly Voted 1 year, 9 months ago

Server3. Microsoft Exchange Server 2007 is correct.

upvoted 7 times

joergsi Most Recent 8 months, 1 week ago

If you check out the Hybrid Deployment perquisites:
https://docs.microsoft.com/en-us/exchange/hybrid-deployment-prerequisites

Only Exchange is been mentioned!

upvoted 1 times

TimurKazan 1 year ago

E. Sharepoint Server 2010 does not support hybrid solution with Microsoft 365

upvoted 1 times

LoremanReturns 1 year, 3 months ago

Any Exchange version DO NOT SUPPORT upgrade (but side-by-side migration by implementing new Exchange Servers). I believe the correct answer is Server 5. Lync 2013 can be upgraded (in-place) to Skype for Business 2015 and then configured in hybrid with Office 3

upvoted 1 times

F_M 1 year, 3 months ago

Lync 2013 supports Hybrid SfB...
https://docs.microsoft.com/en-us/skypeforbusiness/hybrid/plan-hybrid-connectivity#server-version-requirements

upvoted 3 times

LoremanReturns 1 year, 3 months ago

NOT SUPPORT upgrade (but side-by-side migration by implementing new Exchange Servers). I believe the correct answer is Server 5. Ly 2013 can be upgraded (in-place) to Skype for Business 2015 and then configured in hybrid with Office 365.

upvoted 1 times

F_M 1 year, 4 months ago

By the way Sharepoint hybrid is supported from Sharepoint 2013 on... You can still use the Sharepoint Migration Tool in Sharepoint 201 but that's not hybrid. I think the answer is still correct because if you don't want to update your SP2010 server you can add a SP2013

server to the farm and still set an hybrid deployment
upvoted 1 times

Noppawat 1 year, 9 months ago
Exchange Server 2007 does not support Hybrid Deployment.
Answer B is correct
upvoted 4 times

Alvaroll 2 years ago
4-6 https://www.examtopics.com/exams/microsoft/ms-100/view/23/
upvoted 2 times

minajahan 2 years, 7 months ago
"A staged migration is recommended when:Your source email system is Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007"

https://docs.microsoft.com/en-us/exchange/mailbox-migration/what-to-know-about-a-staged-migration
upvoted 2 times

MerryWeasel 1 year, 8 months ago
Maybe better reference is this: https://docs.microsoft.com/en-us/exchange/exchange-2013-and-2007-hybrid/server-roles but still answer is correct.
upvoted 1 times

[Removed] 2 years, 2 months ago
Server 3
upvoted 1 times

Your on-premises network contains five file servers. The file servers host shares that contain user data.
You plan to migrate the user data to a Microsoft 365 subscription.
You need to recommend a solution to import the user data into Microsoft OneDrive.
What should you include in the recommendation?

A. Configure the settings of the OneDrive client on your Windows 10 device.

B. Configure the Sync settings in the OneDrive admin center.

C. Run the SharePoint Hybrid Configuration Wizard.

D. Run the SharePoint Migration Tool.

Correct Answer: *D*
The SharePoint Migration Tool lets you migrate content to SharePoint Online and OneDrive from the following locations:
- SharePoint Server 2013
- SharePoint Server 2010
- Network and local file shares

Reference:
https://docs.microsoft.com/en-us/sharepointmigration/introducing-the-sharepoint-migration-tool

MartinSt Highly Voted 2 years, 10 months ago
SPMT (SharePoint Migration Tool) lets you migrate content to SharePoint Online and OneDrive from the following locations:

SharePoint Server 2013
SharePoint Server 2010
Network and local file shares
upvoted 35 times

mkoprivnj Highly Voted 1 year, 9 months ago
D for sure. SPO migration tool!
upvoted 10 times

jjong Most Recent 1 year ago
in my exam today
upvoted 3 times

Ash473 1 year, 1 month ago
In exam today
upvoted 4 times

MartiFC 1 year, 2 months ago
Run the SharePoint Migration Tool is correct.
upvoted 2 times

melatocaroca 1 year, 3 months ago
Answer: D

Best option to migrate SPMT (SharePoint Migration Tool)

References
https://docs.microsoft.com/en-us/sharepointmigration/fileshare-to-odsp-migration-guide
https://docs.microsoft.com/en-us/fasttrack/data-migration
https://docs.microsoft.com/en-us/onedrive/plan-onedrive-enterprise
upvoted 1 times

Question #9 *Topic 5*

Your network contains two Active Directory forests. Each forest contains two domains.
You plan to configure Hybrid Azure AD join for the computers.
You create a Microsoft Azure Active Directory (Azure AD) tenant.
You need to ensure that the computers can discover the Azure AD tenant.
What should you create?

A. a new computer account for each computer

B. a new service connection point (SCP) for each domain

C. a new trust relationship for each forest

D. a new service connection point (SCP) for each forest

Correct Answer: *D*
Your devices use a service connection point (SCP) object during the registration to discover Azure AD tenant information. In your on-premises Active Directory instance, the SCP object for the hybrid Azure AD joined devices must exist in the configuration naming context partition of the computer's forest. There is only one configuration naming context per forest. In a multi-forest Active Directory configuration, the service connection point must exist in all forests that contain domain- joined computers.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-manual

MartiFC Highly Voted 1 year, 2 months ago
One per forest. It's important!
upvoted 5 times

Cheekypoo Most Recent 2 months ago
Was in my exam today 05/08/22.
upvoted 1 times

Nilz76 6 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 2 times

miry117 8 months, 2 weeks ago
Selected Answer: D
D is correct.
upvoted 2 times

FumerLaMoquette 1 year, 2 months ago
Missed the reference.

https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-manual#configure-a-service-connection-point
upvoted 1 times

FumerLaMoquette 1 year, 2 months ago
Answer is correct. One Naming Context per Forest, so one SCP per forest.
upvoted 2 times

You have an on-premises Microsoft SharePoint Server 2016 environment.
You create a Microsoft 365 tenant.
You need to migrate some of the SharePoint sites to SharePoint Online. The solution must meet the following requirements:
- Microsoft OneDrive sites must redirect users to online content.
- Users must be able to follow both on-premises and cloud-based sites.
- Users must have a single SharePoint profile for both on-premises and on the cloud.
- When users search for a document by using keywords, the results must include online and on-premises results.

From the SharePoint Hybrid Configuration Wizard, you select the following features:
- Hybrid business to business (B2B) sites
- Hybrid OneDrive
- Hybrid Search

Which two requirements are met by using the SharePoint Hybrid Configuration Wizard features? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Users must have a single SharePoint profile for both on-premises and on the cloud.

B. OneDrive sites must redirect users to online content.

C. Users must be able to follow both on-premises and cloud-based sites.

D. When users search for a document by using keywords, the results must include online and on-premises results.

Correct Answer: *BD*
Hybrid OneDrive - Choosing this option will redirect on-premises My Sites/OneDrive for Business sites to SharePoint Online OneDrive for Business in Office 365.
Once the wizard completes, any click of the OneDrive link from on-premises will redirect to OneDrive for Business in the cloud. This meets the following requirement: OneDrive sites must redirect users to online content.
Cloud hybrid search - Choosing this option creates a cloud Search service application in SharePoint Server and connects the cloud Search service application to your Office 365 tenant. This meets the following requirement: When users search for a document by using keywords, the results must include online and on- premises results.
Reference:
https://docs.microsoft.com/en-us/sharepoint/hybrid/hybrid-picker-in-the-sharepoint-online-admin-center

AlexanderSaad Highly Voted 2 years, 5 months ago
B and D is correct, but enabling the B2B external sites, also enables hybrid site features (uncluding site following) as per: https://docs.microsoft.com/en-us/sharepoint/hybrid/hybrid-picker-in-the-sharepoint-online-admin-center#sharepoint-hybrid-features-offered-in-the-hybrid-picker
upvoted 10 times

F_M 1 year, 4 months ago
And enabling Hybrid One Drive enables Hybrid users
upvoted 1 times

spg987 Most Recent 1 year, 1 month ago
In exam today
upvoted 4 times

MartiFC 1 year, 2 months ago
B and D is correct
upvoted 1 times

mkoprivnj 1 year, 9 months ago
B & D for sure!
upvoted 1 times

donathon 2 years ago

In SharePoint Server, you can redirect users to Microsoft OneDrive when they select OneDrive in the nav bar (SharePoint Server 2010 a SharePoint Server 2013) or in the app launcher (SharePoint Server 2016). This is known as hybrid OneDrive. With this feature, you can continue to use your on-premises SharePoint farm while providing your users with an easy way to store, share, and collaborate in the cloud with OneDrive. This best-of-both-worlds approach lets you keep your key business information in your own environment while allowing users the flexibility to access their documents from anywhere. https://docs.microsoft.com/en-us/sharepoint/hybrid/plan-hybri onedrive-for-business
With the cloud hybrid search solution for SharePoint in Microsoft 365, you index all your crawled content, including on-premises conte in your search index in Office 365. When users query your search index in Office 365, they get search results from both on-premises an Microsoft 365 content. https://docs.microsoft.com/en-us/sharepoint/hybrid/learn-about-cloud-hybrid-search-for-sharepoint
https://docs.microsoft.com/en-us/sharepoint/create-b2b-extranet

upvoted 1 times

Jokke71 2 years, 6 months ago

What does answer C even refer to ? "C. Users must be able to follow both on-premises and cloud-based sites." I'm not sure what 'featur this is or what they mean with it...

upvoted 3 times

stishy 2 years, 8 months ago

Ref: https://docs.microsoft.com/en-us/sharepoint/hybrid/hybrid-picker-in-the-sharepoint-online-admin-center

upvoted 4 times

DRAG DROP -

You have several Microsoft SharePoint document libraries in your on-premises environment.

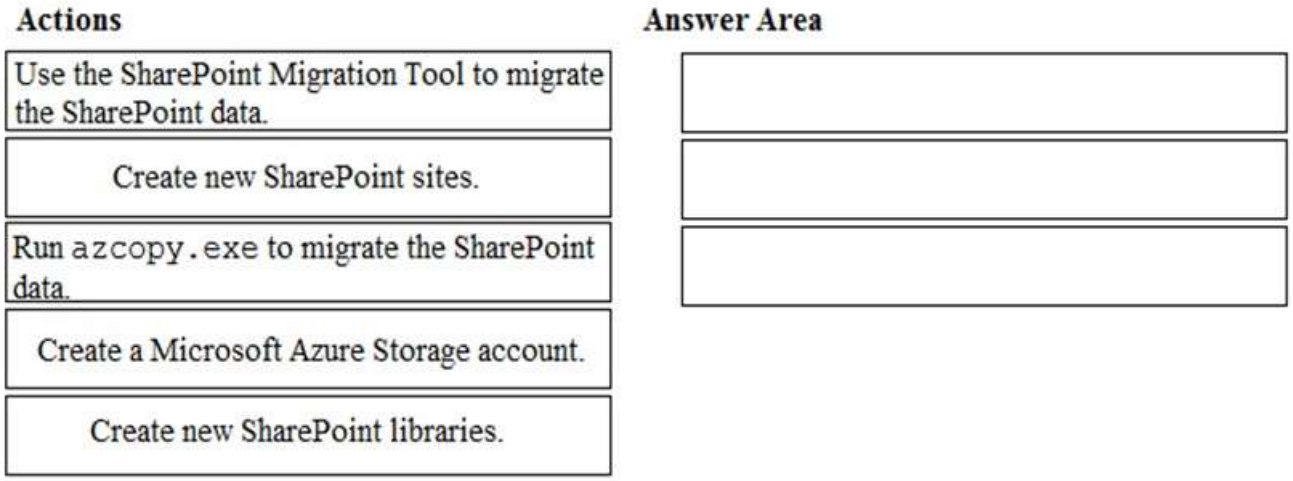
You have a Microsoft 365 tenant that has directory synchronization implemented.

You plan to move all the document libraries to SharePoint Online.

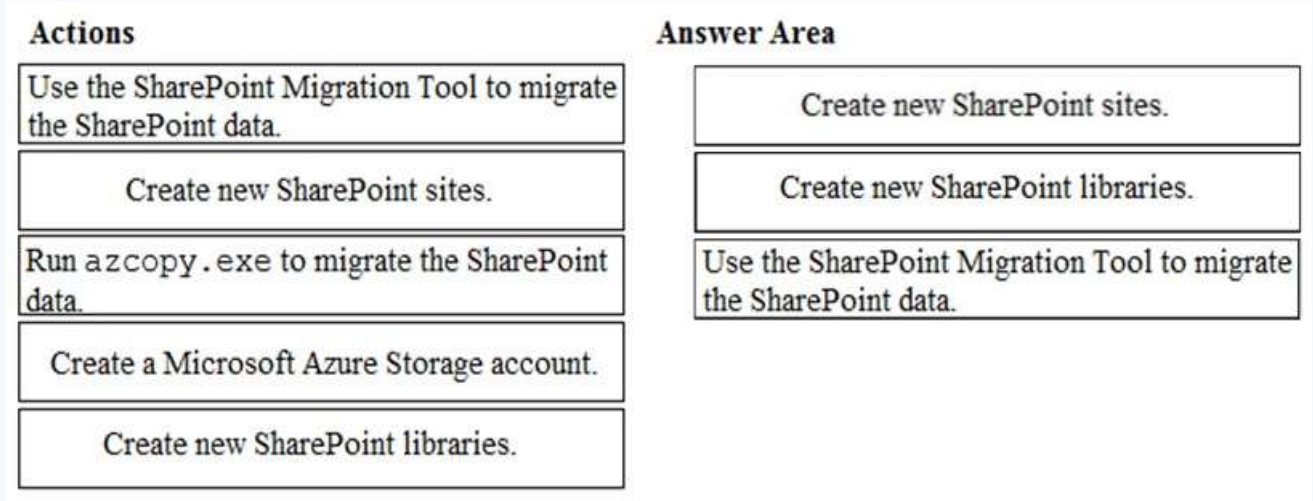
You need to recommend a migration strategy for the document libraries.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



The SharePoint Migration Tool lets you migrate content to SharePoint Online and OneDrive from the following locations:

SharePoint Server 2013 -

- SharePoint Server 2010
- Network and local file shares

The first step is to create new SharePoint sites in SharePoint online. These sites will host the document libraries which will host the migrated content.

The second step is to create the document libraries in the SharePoint sites to host the migrated content.

The final step is to use the SharePoint Migration Tool to migrate the content.

Reference:

https://docs.microsoft.com/en-us/sharepointmigration/how-to-use-the-sharepoint-migration-tool

BDuff 8 months, 3 weeks ago

Agree with the answer.

upvoted 1 times

TimurKazan 11 months ago

Run azcopy.exe is used for copying from storage accounts

upvoted 1 times

junior6995 1 year ago

The Options “Run azcopy.exe” to migrate the SharePoint Data and Create a Microsoft Azure Storage Account has nothing to do with SharePoint Migration, I’d agree with the selected answers, I’m just not sure if they’re in correct order.

upvoted 1 times

DaBummer 1 year ago

Since no one commented yet, I will take it as is.

upvoted 1 times

You have a Microsoft 365 subscription. All users have client computers that run Windows 10 and have Microsoft 365 Apps for enterprise installed.
Some users in the research department work for extended periods of time without an Internet connection.
How many days can the research department users remain offline before they are prevented from editing Office documents?

A. 10

B. 30

C. 90

D. 120

Correct Answer: *B*
After 30 days, Microsoft 365 Apps for enterprise will go into reduced functionality mode. When this happens, users will be able to open files but they won't be able to edit them.
As part of the installation process, Microsoft 365 Apps for enterprise communicates with the Office Licensing Service and the Activation and Validation Service to obtain and activate a product key. Each day, or each time the user logs on to their computer, the computer connects to the Activation and Validation Service to verify the license status and extend the product key. As long as the computer can connect to the Internet at least once every 30 days, Office remains fully functional. If the computer goes offline for more than 30 days, Office enters reduced functionality mode until the next time a connection can be made.
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-of-licensing-and-activation-in-office-365-proplus

Josephsmith Highly Voted 1 year, 4 months ago
It is now 180 days for enterprise

https://office-watch.com/2021/how-to-get-microsoft-365-extended-offline-time/
upvoted 7 times

melatocaroca 1 year, 4 months ago
correct but they do not offer 180 days answer they offer 120
upvoted 1 times

Pucky4485 1 year, 3 months ago
Is only for Entreprise with specific permission.
upvoted 1 times

TimurKazan 11 months, 1 week ago
yes, it is 30 days by default, and from 30 uo to 180 for organizations with specific permissions, since nothing is told about that, I would choose 30 as default value
upvoted 1 times

Nilz76 Most Recent 6 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 1 times

melatocaroca 1 year, 3 months ago
Default still being, 30, can be extended, extension must be configured to right value 180

Reference
https://support.microsoft.com/en-us/office/extend-your-office-license-for-offline-use-06de5162-e230-4ce6-83bb-e6f06190a8f5?ui=en-US&rs=en-US&ad=US
upvoted 3 times

Question #13 *Topic 5*

Your network contains an Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2016. Server1 has a share named
Share1.
You have a hybrid deployment of Microsoft 365.
You need to migrate the content in Share1 to Microsoft OneDrive.
What should you use?

A. Windows Server Migration Tools

B. Microsoft SharePoint Migration Tool

C. Storage Migration Service

Correct Answer: *B*
The SharePoint Migration Tool lets you migrate content to SharePoint Online and OneDrive from the following locations:
⇨ SharePoint Server 2013
⇨ SharePoint Server 2010
⇨ Network and local file shares
Reference:
https://docs.microsoft.com/en-us/sharepointmigration/migrating-content-to-onedrive-for-business https://docs.microsoft.com/en-us/sharepointmigration/introducing-the-sharepoint-migration-tool

mkoprivnj Highly Voted 1 year, 9 months ago
SPO migration tool! B is correct!
upvoted 9 times

ALPHA_DELTA 1 year, 7 months ago
For sure!
upvoted 5 times

Cheekypoo Most Recent 2 months ago
Was in my exam today 05/08/22.
upvoted 1 times

RiTh73 7 months, 3 weeks ago
Selected Answer: B
B for sure
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a main office and three branch offices. All the branch offices connect to the main office by using a WAN link. The main office has a high-speed
Internet connection. All the branch offices connect to the Internet by using the main office connection.
Users use Microsoft Outlook 2016 to connect to a Microsoft Exchange Server mailbox hosted in the main office.
The users report that when the WAN link in their office becomes unavailable, they cannot access their mailbox.
You create a Microsoft 365 subscription, and then migrate all the user data to Microsoft 365.
You need to ensure that all the users can continue to use Outlook to receive email messages if a WAN link fails.
Solution: You enable Cached Exchange Mode for all the Outlook profiles.
Does this meet the goal?

A. Yes

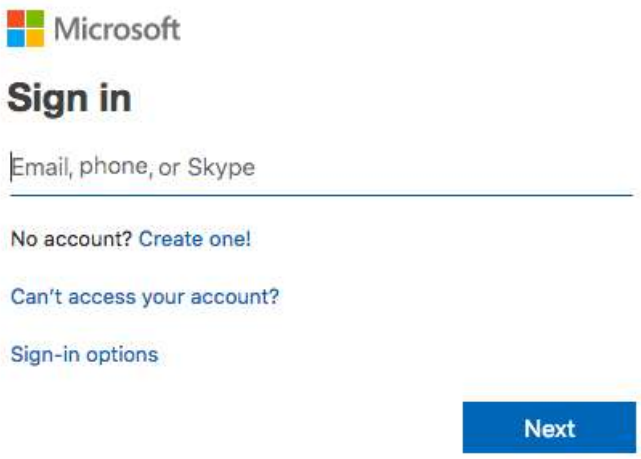
B. No

Correct Answer: *B*
The question states that the branch offices connect to the Internet by using the main office connections. Therefore, all Internet traffic goes over the WAN link between the branch office and main office.
After the migration, the users connect to their mailboxes hosted in Exchange Online over the Internet and therefore over the WAN link.
If the WAN link goes down, the branch office users will not be able to connect to the Internet and therefore will not be able to access their email using Outlook.
Using Cached mode would enable users to access emails that have already been downloaded as they would be cached in Outlook. However, the users would not be able to download new email or send email if the WAN link failed.
The solution is to add a direct connection to the Internet from the branch offices, so their Internet traffic does not go over the WAN link.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



Your organization plans to start a new collaborative project that will contain email and chat communications, as well as regular meetings.
You need to create a team in Microsoft Teams for the planned project. The team must have the following configurations:
- Be named Project1.
- Have an owner named Lee Gu.
- Have a channel named Channel1.

To answer, sign in to the Microsoft 365 portal.

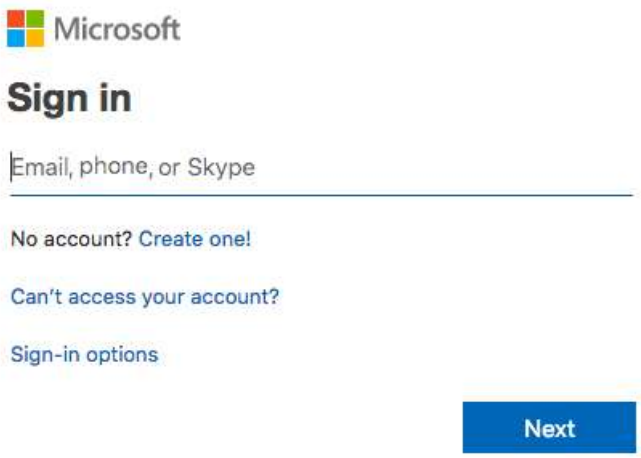
Correct Answer: *See explanation below.*
You need to create a team. You can create a team in the Microsoft Teams Admin Center or in the Microsoft Teams app. However, to be able to specify the team owner when creating the team, you need to use the Teams Admin Center.
1. Go to the Microsoft Teams Admin Center.
2. In the left navigation pane, expand the Teams section and select 'Manage Teams'.
3. Click the '+ Add' link to add a new team.
4. Give the team the name Project1.
5. In the Team Owner field, remove your name which is there by default and add Lee Gu.

6. Click the 'Create a team' button to create the team.
7. In the teams list, select the Project1 team.
8. Click on 'Channels'.
9. Click the '+ Add' link to add a new channel.
10. Give the channel the name Channel1.
11. Click the Apply button to create the channel.

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username: admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -



Your organization recently purchased a projector that can be moved easily between conference rooms.
You need to ensure that any user in the organization can add the projector to a Microsoft Outlook meeting request. The solution must ensure that a user named
Lee Gu must approve all meeting requests.
To answer, sign in to the Microsoft 365 portal.

Correct Answer: *See explanation below.*
You need to create a resource mailbox in Exchange.
1. Go to the Exchange Admin Center.
2. In the left navigation pane, select Recipients.
3. Click the Resources link.
4. Click the plus (+) icon and select 'Equipment Mailbox'.
5. Give the mailbox a name such as 'Projector1'.
6. Enter the name projector1 in the email address field.
7. Click the Save button to create the equipment mailbox.

8. In the resource mailbox list, select the new mailbox and click the Edit icon (pencil icon).
9. Select 'Booking Delegates' in the menu list.
10. Select the option, ɹ€Select delegates who can accept or decline booking requestsɹ€.
11. Click the plus (+) icon and add Lee Gu as a delegate.
12. Click the Save button to save the changes.

Your company has an on-premises Microsoft Exchange Server 2016 organization. The organization is in the company's main office in Melbourne.
The main office has a low-bandwidth connection to the Internet.
The organization contains 250 mailboxes.
You purchase a Microsoft 365 subscription and plan to migrate to Exchange Online next month.
In 12 months, you plan to increase the bandwidth available for the Internet connection.
You need to recommend the best migration strategy for the organization. The solution must minimize administrative effort.
What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. network upload

B. cutover migration

C. hybrid migration

D. staged migration

Correct Answer: *C*
With a hybrid migration, you can migrate the mailboxes in small batches over a period of time which will help to avoid saturating the bandwidth. With the migration wizard, you can configure a migration batch to start outside office hours which would minimize bandwidth usage during office hours.
With a hybrid migration, you do not need to reconfigure Outlook to connect to the migrated mailbox. Outlook will automatically detect the new mailbox location.
This reduces administrative effort.
Incorrect Answers:
A: 'Network upload' is not a defined migration strategy.
B: With a cutover migration, all mailboxes are migrated in one go. This is not suitable for a low bandwidth Internet connection. You would also need to manually reconfigure Outlook for each user which does not meet the requirement of minimizing administrative effort.
D: With a staged migration, mailboxes are migrated in batches. However, Microsoft recommends using a staged migration when you have more than 2000 mailboxes. You would also need to manually reconfigure Outlook for each user which does not meet the requirement of minimizing administrative effort.
Reference:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration

Myko Highly Voted 2 years, 2 months ago
https://docs.microsoft.com/en-us/exchange/mailbox-migration/decide-on-a-migration-path
upvoted 11 times

AnasKh Highly Voted 1 year, 7 months ago
Answer is C:
With a hybrid migration, you can migrate the mailboxes in small batches over a period of time which will help to avoid saturating the bandwidth. With the migration wizard, you can configure a migration batch to start outside office hours which would minimize bandwi usage during office hours.
With a hybrid migration, you do not need to reconfigure Outlook to connect to the migrated mailbox. Outlook will automatically detect new mailbox location. This reduces administrative effort.
upvoted 5 times

estarisbourne Most Recent 1 year, 8 months ago
ahh, I get it, see over 150 so can't use cutover, its exchange 2016 so staged is not an option which by default gives us hybrid option for win. If I did not go look this up I would have totally guessed staged incorrectly
upvoted 3 times

Turak64 1 year, 1 month ago
You can use cutover for upto 2,000 mailboxes in theory. Staged is possible on 2016, but Hybrid is the answer because it allows you t move the mailboxes in small batches at a time.
upvoted 1 times

xamastrok 1 year, 9 months ago

But I am confused by the requirement stated: "the solution must minimize administrative effort". Hybrid should be the solution with th most administrative effort.

upvoted 3 times

mkoprivnj 1 year, 9 months ago

hybrid!

upvoted 4 times

Halipot 1 year, 11 months ago

https://docs.microsoft.com/en-us/exchange/mail-migration-jump

upvoted 1 times

HOTSPOT -

Your company has 500 client computers that run Windows 10.

You plan to deploy Microsoft 365 Apps for enterprise to all the computers.

You create the following XML file for the planned deployment.

```
<Configuration>
 <Add OfficeClientEdition="64" Channel="Broad" ForceUpgrade="TRUE">
     <Product ID="O365ProPlusRetail">
          <Language ID="en-us"/>
          <ExcludeApp ID="Groove"/>
          <ExcludeApp ID="Publisher"/>
     </Product>
 </Add>
 <Updates Enabled="TRUE" Channel="Broad" Deadline="03/31/2019, 00:00"
UpdatePath="\\sccm\updates"/>
 <Display Level="Full" AcceptEULA="TRUE"/>
 <Property Name="FORCEAPPSHUTDOWN" Value="TRUE"/>
 <Property Name="SharedComputerLicensing" Value="0"/>
 <Property Name="PinIconsToTaskbar" Value="TRUE"/>
</Configuration>
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

When the installation is complete [**answer choice**].

- all users will be prompted to accept the EULA
- all users will be prompted to install several updates
- all semi-annual channel updates will be installed automatically

Office 365 ProPlus will [**answer choice**].

- include Microsoft OneDrive for Business and Microsoft Outlook only
- be installed on all the computers
- be installed only on the computers that run a 64-bit version of Windows 10

Correct Answer:

Answer Area

When the installation is complete [**answer choice**].

- all users will be prompted to accept the EULA
- all users will be prompted to install several updates
- all semi-annual channel updates will be installed automatically

Office 365 ProPlus will [**answer choice**].

- include Microsoft OneDrive for Business and Microsoft Outlook only
- be installed on all the computers
- be installed only on the computers that run a 64-bit version of Windows 10

Box 1:

When the installation is complete, all users will be prompted to install several updates.

In the configuration file, the Updates Enabled element is set to True. This means that Office will check for updates after the installation.

The Channel element set to Broad means that all semi-annual channel updates will be installed.

Box 2:

Microsoft 365 Apps for enterprise will be installed only on the computers that run a 64-bit version of Windows 10.

The OfficeClientEdition element defines whether the 32-bit or 64-bit edition of Microsoft 365 Apps for enterprise is downloaded or installed. In the configuration file, it is set to '64'. The 64-bit version will only install on a 64-bit client computer.

Reference:

https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool

itmaster 5 months, 4 weeks ago

Box1 should be first option, because display level is set to "full" in the configuration file. Referance: https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options#:~:text=If%20Level%20is,normal%20installation%20experience

upvoted 1 times

gonick 1 year ago

Box 1 should be middle option. Deadline will prompt users to install updates:

https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options#deadline-attribute-part-of-updates-eleme

upvoted 1 times

Marcelmikael 11 months ago

https://docs.microsoft.com/en-us/deployoffice/update-channels-changes

The answer in box one is correct. Check the link.

upvoted 1 times

Eggsamine 11 months, 2 weeks ago

But that document pretty much says that after deadline updates will be installed automatically so users won't be prompted to instal

https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options#:~:text=Prior%20to%20the%20deadline%2C%20users%20receive%20multiple%20reminders%20to%20install%20the%20up
s.%20If%20Office%20isn%27t%20updated%20by%20the%20deadline%2C%20users%20see%20a%20notification%20that%20the%20
dates%20will%20be%20applied%20in%2015%20minutes.

I think the answers are correct.

upvoted 1 times

jinxie 10 months, 2 weeks ago

I agree, both answers are technically correct. the updates will auto install after the deadline if the user did not do it themselves. however after the update the user will also be prompted to install the updates. personally I think middle option is more correct a the last option, to me atleast, implies that once office is installed the updates are also there which is not the case. As such i'd go w middle option

upvoted 1 times

jinxie 10 months, 2 weeks ago

Slight correction I mean "after the installation the user will be prompted etc. etc."

upvoted 1 times

gsmith9897 1 year, 3 months ago

The answer for box 1 says, "When the installation is complete, all users will be prompted to install several updates" but the graphic sho "all semi-annual channel updates will be installed automatically".

upvoted 3 times

Bobalo 1 year, 2 months ago

I'm going to go with what it says in the box.

upvoted 1 times

Question #19 *Topic 5*

Your company has a Microsoft Azure Active Directory (Azure AD) directory tenant named contoso.onmicrosoft.com.
All users have client computers that run Windows 10 Pro and are joined to Azure AD.
The company purchases a Microsoft 365 E3 subscription.
You need to upgrade all the computers to Windows 10 Enterprise. The solution must minimize administrative effort.
You assign licenses from the Microsoft 365 admin center.
What should you do next?

A. Add a custom domain name to the subscription.

B. Deploy Windows 10 Enterprise by using Windows Autopilot.

C. Create a provisioning package, and then deploy the package to all the computers.

D. Instruct all the users to log off of their computer, and then to log in again.

Correct Answer: *B*
With Windows Autopilot the user can set up pre-configure devices without the need consult their IT administrator.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

TommyTommy Highly Voted 2 years, 11 months ago
Answer is wrong. There is no need to use autopilot for Pro -> Enterprise SKU update. With subscription based activation PRO -> Enterpr
happens automatically when user has the license assigned and log in to device
upvoted 38 times

Hamster5000 2 years, 8 months ago
Agreed! Answer is 'D'. Done this on 20 workstations.
upvoted 29 times

ExAmMs Highly Voted 2 years, 8 months ago
Answer D is correct. This is the documentation:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#how-it-works
"When a licensed user signs in to a device that meets requirements using their Azure AD credentials, the operating system steps up fro
Windows 10 Pro to Windows 10 Enterprise"
Devices are AAD joined. A license was assigned. The missing peace is only the sign in and out
upvoted 22 times

samstorm10 Most Recent 1 week ago
Selected Answer: D
D for sure.
upvoted 1 times

k9_bern_001 1 month, 1 week ago
D is the correct answer
upvoted 1 times

bedny22 7 months, 4 weeks ago
Selected Answer: D
Just restart :)
upvoted 1 times

AlexLiourtas 8 months, 1 week ago
Selected Answer: D
D, please update the answers. I have paid for this exam.
upvoted 6 times

AlexLiourtas 8 months, 1 week ago
The solution must minimize administrative effort.

D
upvoted 1 times

Jeff8989 8 months, 3 weeks ago
In exam today and D is the correct answer.
upvoted 1 times

Davidchercm 9 months, 1 week ago
Selected Answer: D
D is correct
upvoted 1 times

Joshycannon 9 months, 2 weeks ago
Selected Answer: B
For sure B. While having the user log on and off may seem the easiest and simplest, it would not be. Even if this would be for 15 users, unless ~you~ are physically present and doing it, that would require overhead and is still not requiring the least amount of administrat overhead. I work for an MSP and getting just 5 users that we work with remotely for one of our companies to reboot is a PITA, and it's better for us to schedule a reboot instead, which is what AutoPilot can enable you to do in a sense.

https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot#:~:text=Traditionally%2C%20IT%20pros,that%20is%20automated
upvoted 1 times

lucidgreen 1 year, 7 months ago
I love the D. This is literally one of the easiest ways to fix things when something is wrong. Rebooting the second easiest. But it makes sense because when licensing is changed, you have to sync the changes with a log on or go to Settings > Users > etc and sync.
upvoted 6 times

NikPat3125 1 year, 7 months ago
I think D is not right as this needs on and off. Which means need administrative effort.
We need minimum administrative effort so I think D is not right option.
upvoted 2 times

RNG60FR 1 year, 8 months ago
This is an MS-101 Exam Question I think
upvoted 2 times

mkoprivnj 1 year, 9 months ago
D for sure!
upvoted 5 times

casti 1 year, 11 months ago
D is the correct answer.
Microsoft 365 E3 include Windows 10 enterprise, but Office 365 E3 not. keep in mind this in de cuestion.
upvoted 7 times

VTHAR 1 year, 11 months ago
Ref : https://youtu.be/bk9wWc7x_m4

Take a look at this question https://www.examtopics.com/discussions/microsoft/view/2545-exam-ms-101-topic-1-question-33-discussio which is asked in last week MS-101 exam, the answer is subscription activation.

The correct answer for this question is D.
upvoted 6 times

Sango 2 years, 1 month ago
D. The question specifies "minimize administrative effort."
upvoted 5 times

Your company has a Microsoft 365 subscription.
You plan to move several archived PST files to Microsoft Exchange Online mailboxes.
You need to create an import job for the PST files.
Which three actions should you perform before you create the import job? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a Microsoft Azure Storage account.

B. From the Microsoft 365 compliance center, retrieve the SAS key.

C. Run azcopy.exe to copy the PST files to Microsoft Azure Storage

D. From Exchange admin center, run a new migration batch.

E. Create a PST import mapping file.

Correct Answer: *BCE*
The first step is to download and install the Azure AzCopy tool, which is the tool that you run in Step 2 to upload PST files to Office 365. You also copy the SAS
URL for your organization. This URL is a combination of the network URL for the Azure Storage location in the Microsoft cloud for your organization and a Shared
Access Signature (SAS) key. This key provides you with the necessary permissions to upload PST files to your Azure Storage location.
Now you're ready to use the AzCopy.exe tool to upload PST files to Office 365. This tool uploads and stores them in an Azure Storage location in the Microsoft cloud.
After the PST files have been uploaded to the Azure Storage location for your Office 365 organization, the next step is to create a comma-separated value (CSV) file that specifies which user mailboxes the PST files will be imported to. You'll submit this CSV file when you create a PST Import job.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files

joergsi 8 months, 1 week ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-network-upload-to-import-pst-files?view=o365-worldwide

Step 1: Copy the SAS URL and download AzCopy
The first step is to download the AzCopy tool, which is the tool that you run in Step 2 to upload PST files to Microsoft 365. You also copy
SAS URL for your organization. This URL is a combination of the network URL for the Azure Storage location in the Microsoft cloud for y
organization and a Shared Access Signature (SAS) key.

Step 2: Upload your PST files to Microsoft 365
Now you're ready to use the AzCopy tool to upload PST files to Microsoft 365

Step 4: Create the PST Import mapping file
After the PST files have been uploaded to the Azure Storage location for your organization, the next step is to create a comma-separate
value (CSV) file that specifies which user mailboxes the PST files will be imported to. You'll submit this CSV file in the next step when you
create a PST Import job.
upvoted 3 times

TimurKazan 11 months, 1 week ago
correct
upvoted 1 times

Ash473 1 year, 1 month ago
In Exam today
upvoted 4 times

Ronger 1 year, 3 months ago
BCE is correct
upvoted 2 times

Question #21 *Topic 5*

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. All the devices have Microsoft Office 365 apps installed.
You need to configure the proofing tool settings for the Office 365 apps.
From the Microsoft Endpoint Manager admin center, what should you create?

A. a device compliance policy

B. an app configuration policy

C. an app

D. a device configuration profile

Correct Answer: *B*
An app configuration setting, for example, might require you to specify any of the following details:
- A custom port number
- Language settings
- Security settings
- Branding settings such as a company logo

Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

mkoprivnj Highly Voted 1 year, 9 months ago
B for sure!
upvoted 6 times

Mario007 1 year, 4 months ago
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview
upvoted 1 times

ezapper2 Highly Voted 1 year, 8 months ago
isnt this ms-101?
upvoted 6 times

dumpmaster Most Recent 7 months, 3 weeks ago
Selected Answer: C
It is C:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365
upvoted 2 times

TimurKazan 11 months, 1 week ago
C - create an app. App configuration has nothing to do with Win10
upvoted 2 times

jjong 1 year ago
In Exam today
upvoted 3 times

spg987 1 year, 1 month ago
In exam today
upvoted 6 times

Ash473 1 year, 1 month ago
In Exam today
upvoted 4 times

subbuhotmail 1 year, 2 months ago
Its C.... App configuration policy only for ios or anroid.

You need to create a new xml file to install proofing tools and push it as Windows app. So its C only.
upvoted 2 times

stromnessian 1 year, 2 months ago

C or D are possible answers but since the app is already installed, it's D.

upvoted 1 times

melatocaroca 1 year, 3 months ago

Answer: B
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview
An app configuration setting, for example, might require you to specify any of the following details:

A custom port number
Language settings
Security settings
Branding settings such as a company logo

Other References
https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365
https://docs.microsoft.com/en-us/deployoffice/overview-deploying-languages-microsoft-365-apps
https://docs.microsoft.com/en-us/deployoffice/office2016/customize-language-setup-and-settings-for-office-2016

upvoted 1 times

michszym 1 year, 2 months ago

melatocaroca read link you provided - "app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps" and it's for Intune, not for Endpoint Manager.

upvoted 1 times

Said_kram 1 year, 3 months ago

App configuration only for Android/iOS devices, i'll go with app, C.

upvoted 1 times

encxorblood 1 year, 3 months ago

Not shure. For Intune answer B is correct. With ECM I think C.

upvoted 1 times

F_M 1 year, 4 months ago

This can be done with an app. Create a new app for WIndows 10 under the category Microsoft 365 Apps. When configuring you select t
Enter XML option and paste the XML snippet from this source: https://docs.microsoft.com/en-us/deployoffice/overview-deploying-languages-microsoft-365-apps#deploy-proofing-tools .
That should do the trick, so C.
Please correct me if I'm wrong!

upvoted 5 times

jaolbreak 1 year, 4 months ago

Answer: D
App policies apply to mobile devices not Win10.
A Device Configuration > Custom profile allows OMA-URI settings
https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10

upvoted 3 times

McAlec 1 year, 4 months ago

With Custom profile using Office CSP you can add install instructions to an ODT prepared package.
https://docs.microsoft.com/en-us/windows/client-management/mdm/office-csp
Though it works, needs more efforts.

I believe that creating an M365 Apps app with the right parameters would be less time consuming.
I am for C, creating an App.

upvoted 2 times

Question #22 *Topic 5*

You publish an enterprise application named App1 that processes financial data.

You need to ensure that access to App1 is revoked for users who no longer require viewing the processed financial data.

What should you configure?

A. an owner

B. an app protection policy

C. an access review

D. a conditional access policy

Correct Answer: *C*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

mkoprivnj Highly Voted 1 year, 9 months ago

C for sure!

upvoted 9 times

ALPHA_DELTA 1 year, 7 months ago

For sure!

upvoted 2 times

SwapnilChavan 1 year, 7 months ago

mkoprivnj for sure :P

upvoted 10 times

AlexLiourtas 9 months, 4 weeks ago

for sure

upvoted 1 times

WassimCloudLife 9 months, 1 week ago

ITS C FOR SURE!!

upvoted 1 times

MitalWulf 8 months ago

FUUURSHO!

upvoted 1 times

Joshycannon Highly Voted 9 months, 2 weeks ago

Since no one like to provide proof, its C because "Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access."

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review#:~:text=Access%20to%20groups%20and%20applications%20for%20employees%20and%20guests%20changes%20over%20time.%20To%20reduce%20the%20risk%20associated%20with%20stale%20access%20assignments%2C%20administrators%20can%20use%20Azure%20Active%20Directory%20(Azure%20AD)%20to%20create%20access%20reviews%20for%20group%20members%20or%20application%20access.

upvoted 8 times

HOTSPOT -

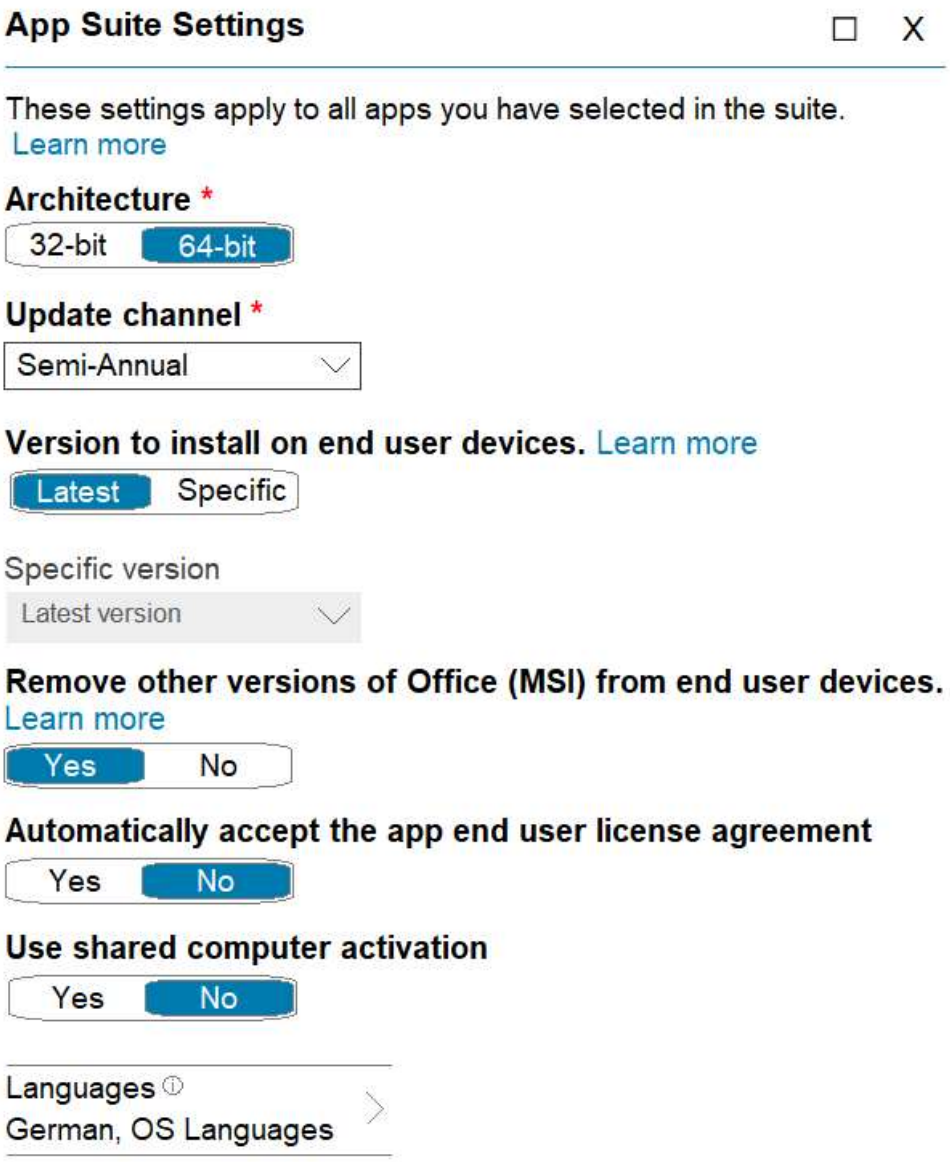
You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the Windows 10 devices shown in the following table.

Name	Version	Language
Device1	x86	German
Device2	x64	English
Device3	x64	French

All the devices are managed by using Microsoft Endpoint Manager and are members of a group named Group1.

From the Microsoft Endpoint Manager admin center, you create an app suite named App1 for Microsoft Office 365 apps.

You configure the App1 settings as shown in the exhibit.



You assign App1 to Group1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Note: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On Device1, Office 365 ProPlus will be installed and the display language will be German.	○	○
On Device2, Office 365 ProPlus will be installed and both the German and English display languages will be installed.	○	○
On Device3, Office 365 ProPlus will be installed and both the German and French display languages will be installed.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On Device1, Office 365 ProPlus will be installed and the display language will be German.	○	●
On Device2, Office 365 ProPlus will be installed and both the German and English display languages will be installed.	●	○
On Device3, Office 365 ProPlus will be installed and both the German and French display languages will be installed.	●	○

Box 1: No -

Device1 is x86 (32-bit) so Office 365 will not be installed.

Box 2: Yes -

Device2 is x64 (64-bit) so Office 365 will be installed. The German language pack will be installed and the OS language pack (English) will be installed.

Box 3: Yes -

Device2 is x64 (64-bit) so Office 365 will be installed. The German language pack will be installed and the OS language pack (French) will be installed.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

LillyLiver 8 months, 1 week ago

I had to check this. By default, InTune will install the default language found on the OS, then any additional languages.

Going by the exhibit, I thought it was going to try and install only German. Guess I learned something today.

upvoted 1 times

rfox321 1 year ago

Should be Y-Y-Y | x86 is compatible with x64 and 32 bit apps.

upvoted 1 times

Azuz 1 year ago

Wrong, you cant install x64 365 apps on x86 Operating system.
upvoted 7 times

rfox321 1 year ago
I stand corrected
upvoted 5 times

Turak64 1 year, 1 month ago
I really hope this is a ms-101 question and it's been put in here by accident!
upvoted 2 times

gonick 1 year ago
Definitely an MS-100 question
upvoted 2 times

Eggsamine 11 months, 2 weeks ago
Endpoint Manager is a MS-101 skill, is this definitely on the MS-100 exam?
upvoted 2 times

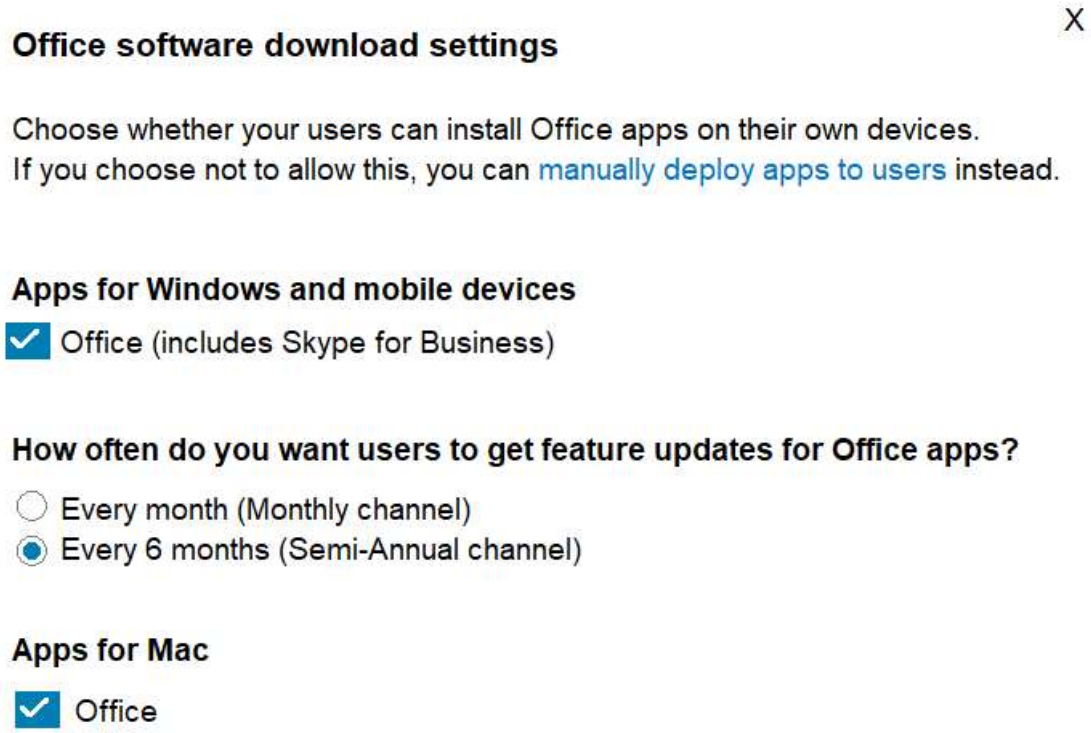
Claire91 10 months ago
I had it on my ms100 exam
upvoted 2 times

HOTSPOT -

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Device type	License
User1	Windows 10	*None*
User2	Windows 10	Microsoft Office 365 E5
User3	Android	Microsoft Office 365 E5

You configure the Office software download settings as shown in the exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

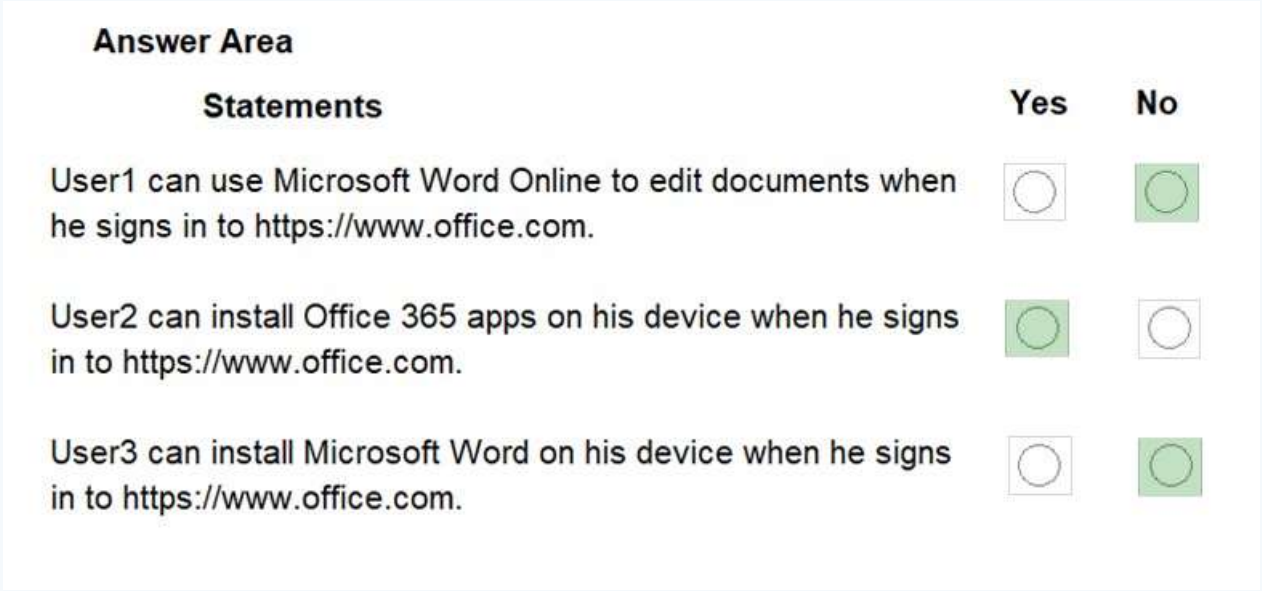
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can use Microsoft Word Online to edit documents when he signs in to https://www.office.com.	○	○
User2 can install Office 365 apps on his device when he signs in to https://www.office.com.	○	○
User3 can install Microsoft Word on his device when he signs in to https://www.office.com.	○	○

Correct Answer:



Box 1: No.

User1 does not have an Office 365 license so will be unable to use edit documents in Word online.

Box 2: Yes.

User2 has a Windows device and an Office 365 license.

Box 3: No -

Although, User 3 has an Office 365 license, you cannot download Android apps from the Office 365 portal. You need to download the apps from the Android app store.

kanag1 8 months, 2 weeks ago

The given answers are correct. Tested.

upvoted 4 times

tcmaggio 10 months ago

Wouldnt User1 be able to USE and EDIT documents once Office OnLine is a free tool?

upvoted 1 times

joergsi 8 months, 1 week ago

To my best knowledge, you have got three levels to handle Office Documents:
- Read Only (Doc Viewer for example) + Mobile App without associated Office Account (unlicensed)
- Web App (license required) => Editing function
- Desktop/Mobile App with Editing function (license required)

Everything that includes editing requires a license.

If you log-in with a business account, without a license associated, no app will be displayed!

upvoted 1 times

junior6995 1 year ago

If the user is licensed he should be able to use Word in Android right?

upvoted 1 times

allesglar 11 months ago

Using is one thing and installing another. I think the answer is correct.

upvoted 2 times

TimurKazan 1 year ago

though, your information doesn't make sense

upvoted 1 times

TimurKazan 1 year ago

we are very glad for you, guys

upvoted 1 times

Jelly101 1 year, 1 month ago

in exam last week

upvoted 3 times

spg987 1 year, 1 month ago

In exam today

upvoted 4 times

Question #25 *Topic 5*

Your network contains an Active Directory forest named contoso.local.
You purchase a Microsoft 365 subscription.
You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.
You need to prepare for the planned move to Microsoft 365.
What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

A. Purchase a third-party X.509 certificate.

B. Rename the Active Directory forest.

C. Purchase a custom domain name.

D. Create an external forest trust.

Correct Answer: *C*
The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on-premise Active Directory if it's a routable domain name, for example, contoso.com.
If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active
Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization

Dylan Highly Voted 2 years, 12 months ago
And domain name (contoso.com), more to the point
upvoted 12 times

Ash473 Highly Voted 1 year, 1 month ago
In exam today
upvoted 7 times

estarisbourne Most Recent 1 year, 8 months ago
I guess you need a custom domain that you own to register and verify but like not sure that is the best way to spend 12 months of development :) answer is correct though.
upvoted 1 times

Durden871 7 months, 2 weeks ago
I took it as, you need a hybrid solution for 12 months. Could maybe migrate to cloud thereafter. Either way, if you're going to sync y domain to 365, probably should make sure you own it first.
upvoted 2 times

PattiD 1 year, 9 months ago
https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide
upvoted 3 times

PattiD 1 year, 9 months ago
YOU MUST HAVE/BUY A ROUTABLE DOMAIN FIRST. ANSWER IS 10000% CORRECT.
upvoted 7 times

ARYMBS 5 months, 1 week ago
NO you must not i (you can leave, theoretically with onmicrosoft.com). But it is best answer in this case.
upvoted 1 times

mkoprivnj 1 year, 9 months ago
C for sure!
upvoted 5 times

Sango 2 years ago

The .local is an invalid UPN for all users that will be synced. All the users on-premise UPNs must be changed to match the custom AAD domain. The closest answer is B.

upvoted 2 times

donathon 2 years ago

No you just have to create the new custom domain UPN in AD Forest and Trust. SO the answer to purchase a custom domain name correct. Without a custom domain name which also makes your domain public, you cannot have Hybrid deployment unless you wan the users to sign-in using @<domain>.onmicrosoft.com.

upvoted 4 times

afbnfz 1 year, 4 months ago

The on-prem UPNs must be changed to match the custom AAD domain, yes - but you can't do that until you purchase the custom domain.

upvoted 1 times

riccardo 2 years, 1 month ago

I don't understand why I should buy a custom domain name. I should register the custom domain name, not buy.
question stated that I want to implement an hybrid deployment so I have already a custom domain name acquired and I have an Exchange on premise as far I undestand. perhaps I use a private CA for virtual directories, so it make sense that I buy a third party certificate. for me the right answer is A

upvoted 2 times

nicknameitis 2 years ago

what domain would you buy the certificate for? third parties will not issue certificates for a .local domain name. I would go with add custom domain name.

upvoted 3 times

AADapson 1 year, 10 months ago

The question never made mention of Exchange Server is available. You will need to buy custom domain.

upvoted 2 times

WoneSix 2 years, 7 months ago

Dylan, the question doesn't say anything about Exchange.

upvoted 2 times

Dylan 2 years, 12 months ago

This implies that Exchange already exists - I'd assume that you already own a certificate if this is the case...maybe not!

upvoted 3 times

HvD 2 years, 2 months ago

There are several hybrid-possibilities: Exchange, Sharepoint. But that doesn't matter here, the question is: what to do before setting a directory synchronization. Well, set up your domain(name) first.

upvoted 3 times

HOTSPOT -

Your company uses Gmail as a corporate email solution.

You purchase a Microsoft 365 subscription and plan to move all email data to Microsoft Exchange Online.

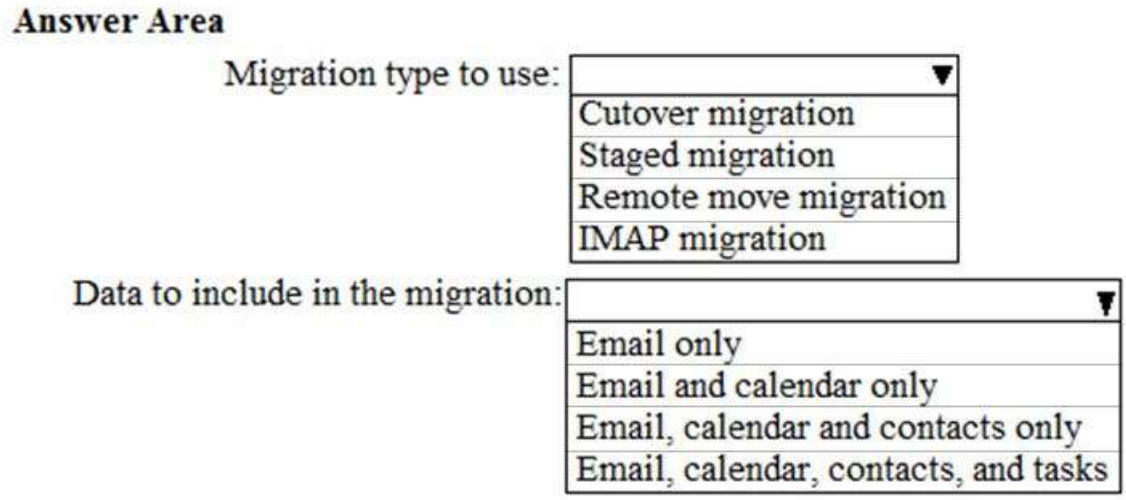
You plan to perform the migration by using the Exchange admin center.

You need to recommend which type of migration to use and which type of data to migrate.

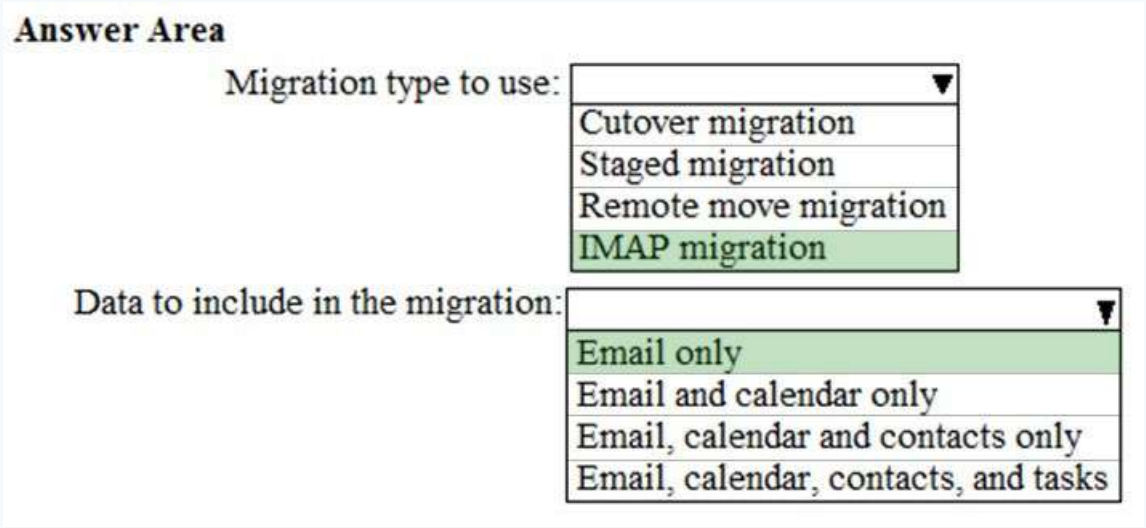
What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



You'll need to use the IMAP migration method. You can use the setup wizard in the Microsoft 365 admin center for an IMAP migration to migrate mailboxes from

Gmail to Microsoft 365.

IMAP migration will only migrate emails, not calendar and contact information. Users can import their own email, contacts, and other mailbox information to Office

365 after the mailboxes have been migrated.

Reference:

https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrate-g-suite-mailboxes

[Removed] Highly Voted 2 years, 2 months ago

Correct

upvoted 8 times

mkoprivnj Highly Voted 1 year, 9 months ago

IMAP + email only!

upvoted 6 times

Ronger 1 year, 3 months ago

for sure1!11!!!!

upvoted 3 times

Lundar Most Recent 3 months, 1 week ago

Correct but you can do a gsuite migration of email from gsuite. but it says Gmail so imap "This is the way"

upvoted 1 times

tejb 1 year, 2 months ago

done this in live environment. Correct answer

upvoted 2 times

Spacedust 1 year, 11 months ago

Answer is correct but Gsuite migration batches are now available which would be a better option: https://docs.microsoft.com/en-us/exchange/mailbox-migration/perform-g-suite-migration

upvoted 1 times

MichaelJS 1 year, 9 months ago

Probably not possible because Gmail and G-Suite are not the same. But I have no prove.

upvoted 1 times

Alvaroll 2 years ago

4-17 https://www.examtopics.com/exams/microsoft/ms-100/view/26/

upvoted 3 times

Question #27 *Topic 5*

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You add an app named App1 to the enterprise applications in contoso.com.
You need to configure self-service app access for App1.
What should you do first?

A. Assign App1 to users and groups.

B. Add an owner to App1.

C. Configure the provisioning mode for App1.

D. Configure an SSO method for App1.

Correct Answer: *C*
The provisioning mode (manual or automatic) needs to be configured for an app before you can enable self-service application access.
Incorrect Answers:
A: If you're assign App1 to users and groups, the users will not need to use self-service to request access to the App. They would already have access to the app.
B: The app does not need an owner. You would configure an owner to delegate control of the app. Without an owner, a Global Admin could configure self- service.
D: The SSO method depends on the provisioning mode.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access
https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Employee-Self-Service-App-Access-for-Azure-AD-now-in-preview/ba-p/243966

F_M Highly Voted 1 year, 4 months ago
In Azure AD > Enterprise Application, creating a new application the first suggested step is to enable SSO to allow user log-in the application using Azure AD credentials. Provisioning mode is set to manual by default and can be left as is. When opening the self-serv pane, in addition, you are prompted to configure SSO before.

The right answer should be D therefore.
upvoted 14 times

F_M 1 year, 4 months ago
This is the same thing that the second link in the answer states...
upvoted 1 times

T10T Most Recent 1 month, 3 weeks ago
Selected Answer: C
I agree with Digida for two reasons.

1. When I deploy a new Enterprise Application in my lab, under the App1 Overview this is the text for the Self service box, "Enable users request access to the application using their Azure AD credentials". It says Azure AD credentials not SSO, these two items are not mutu exclusive, but you would specify SAML/SSO if that was a requirement.

2. In the Microsoft doc for Enable self-service application assignment, it says nothing about SSO in the Prerequisites section either.

To enable self-service application access, you need:
-An Azure account with an active subscription.
-One of the following roles: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.
-An Azure Active Directory Premium (P1 or P2) license is required for users to request to join a self-service app and for owners to appro or deny requests.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access
upvoted 1 times

Digida 2 months ago
Selected Answer: C

Wouldn't the provided answer be correct? The default provisioning method is manual so you would first have to change it to Self-Servic
While some have pointed out that when creating any Ent App it prompts you to setup SSO, but it is not required to be setup before switching the provisioning method.

upvoted 2 times

manis73 3 months, 2 weeks ago

Selected Answer: D

Just tested

upvoted 3 times

Abdulrahman_Salah_2021 5 months, 4 weeks ago

Selected Answer: D

I think D is correct

upvoted 2 times

Alv86 6 months, 1 week ago

Selected Answer: D

the answer is SSO

upvoted 2 times

BDuff 8 months, 3 weeks ago

D for sure.

upvoted 2 times

TimurKazan 11 months ago

you need to set up SSO first

upvoted 3 times

itstudy369 1 year, 3 months ago

D is the correct answer

upvoted 2 times

PeterC 1 year, 3 months ago

If you create a new Ent. App and select "Self-service" you see a message: "Configure single sign-on to this application to use Self-ser
Application Access"

upvoted 4 times

afbnfz 1 year, 4 months ago

This type of key, showing not only why the right answer is right, but why each of the wrong answers is wrong, is just so good. \m/

upvoted 4 times

Your on-premises network contains the web applications shown in the following table.

Name	Hosted on server
App1	Web1
App2	Web1
App3	Web2
App4	Web2

You purchase Microsoft 365, and then implement directory synchronization.

You plan to publish the web applications.

You need to ensure that all the applications are accessible by using the My Apps portal. The solution must minimize administrative effort.

What should you do first?

A. Deploy one conditional access policy.

B. Deploy one Application Proxy connector.

C. Create four application registrations.

D. Create a site-to-site VPN from Microsoft Azure to the on-premises network.

Correct Answer: *B*

The Application Proxy connector is what connects the on-premises environment to the Azure Application Proxy.

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the

Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. Azure AD, the Application Proxy service, and the Application Proxy connector work together to securely pass the user sign-on token from Azure AD to the web application.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-connectors

Pr9 Highly Voted 8 months, 1 week ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-connectors
The Application Proxy connector is what connects the on-premises environment to the Azure Application Proxy.

upvoted 5 times

PmgCosta Most Recent 5 months, 1 week ago

Selected Answer: B

B. Deploy one Application Proxy connector.

upvoted 1 times

RazielLycas 7 months, 2 weeks ago

Selected Answer: B

they are on prem so first of all you need the proxy connector

upvoted 2 times

R3DSh33P 8 months, 3 weeks ago

Selected Answer: C

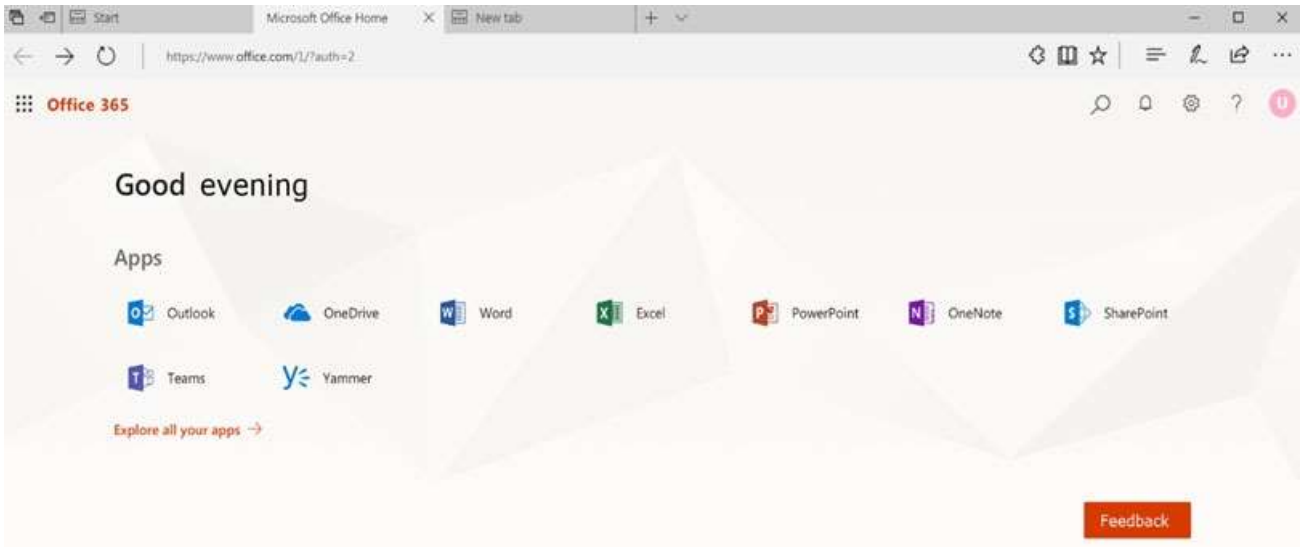
C for sure!

upvoted 2 times

You have a Microsoft 365 E5 subscription.

All users are assigned a license to Microsoft 365 Apps for enterprise.

The users report that they do not have the option to install Microsoft 365 apps on their device as shown in the following exhibit.



You need to ensure that the users can install Microsoft 365 apps from the Office 365 portal.

What should you do?

A. From the Microsoft 365 admin center, modify the user license settings.

B. From the Microsoft Endpoint Manager admin center, create a Microsoft 365 Apps app and assign the app to the devices.

C. From the Microsoft Endpoint Manager admin center, create a Microsoft 365 Apps app and assign the app to the users.

D. From the Microsoft 365 admin center, modify the Services settings.

Correct Answer: *D*

lucidgreen Highly Voted 1 year, 5 months ago

Settings > Org Settings >Services > Office installation options, to be precise.

upvoted 25 times

TimurKazan 1 year ago

Agree with you, the answers look like not up to date

upvoted 1 times

jinxie 10 months, 3 weeks ago

yes makes sense, also if you do not have the license would you even see the apps to begin with?

upvoted 2 times

adaniel89 1 year, 5 months ago

Yes thats right, the answer given is misleading.

upvoted 2 times

Davidchercm 1 year, 1 month ago

what should be the answer ?

upvoted 2 times

T10T Most Recent 1 month, 3 weeks ago

Selected Answer: D

Settings >> Org settings >> Office installation options >> Installation "tab" >> Office apps that users can install >> "Choose whether you users can install Office apps on their own devices."

M365 admin center link:
https://admin.microsoft.com/Adminportal/Home#/Settings/Services/:/Settings/L1/SoftwareDownload

https://admin.microsoft.com/Adminportal/Home#/Settings/Services/:/Settings/L1/SoftwareDownload

upvoted 1 times

Cheekypoo 2 months ago

Was in my exam today 05/08/22.

upvoted 1 times

PmgCosta 5 months, 1 week ago

Selected Answer: D

https://admin.microsoft.com/Adminportal/Home#/Settings/Services/:/Settings/L1/SoftwareDownload

upvoted 2 times

Nilz76 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 3 times

ahmadibrahim2022 6 months, 3 weeks ago

Hi, so what is the answer, please?Thanks

upvoted 1 times

farhadd4 9 months ago

in a normal setting, this is automatically enabled, you have to think of this i see as a fresh setup that is rather custom to this company. Anytime i add a E5 license the option to install has always been there.

upvoted 1 times

Zunedjm 1 year, 3 months ago

If you user has basic licenses (basic licenses only gives you online version of the office) then they need to change the licenses to standa or premium to install the office on thier devices

upvoted 2 times

michszym 1 year, 3 months ago

Read the 1st line: You have a Microsoft 365 E5 subscription. - This is not basic licenses

upvoted 4 times

Your network contains an Active Directory domain named contoso.com.
You have a Microsoft 365 subscription.
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
You implement directory synchronization.
The developers at your company plan to build an app named App1. App1 will connect to the Microsoft Graph API to provide access to several Microsoft Office 365 services.
You need to provide the URI for the authorization endpoint that App1 must use.
What should you provide?

A. https://login.microsoftonline.com/

B. https://contoso.com/contoso.onmicrosoft.com/app1

C. https://login.microsoftonline.com/contoso.onmicrosoft.com/

D. https://myapps.microsoft.com

Correct Answer: *C*
In a single tenant application, sign-in requests are sent to the tenant's sign-in endpoint. For example, for contoso.onmicrosoft.com the endpoint would be: https:// login.microsoftonline.com/contoso.onmicrosoft.com. Requests sent to a tenant's endpoint can sign in users (or guests) in that tenant to applications in that tenant.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant

AlexanderSaad Highly Voted 2 years, 6 months ago
In a single tenant application, sign-in requests are sent to the tenant's sign-in endpoint. For example, for contoso.onmicrosoft.com the endpoint would be: https://login.microsoftonline.com/contoso.onmicrosoft.com.
Ref: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant#update-your-code-to-sen requests-to-common
upvoted 24 times

stoneface 9 months ago
Agreed with this.
More specifications can be found here:
https://docs.microsoft.com/en-us/graph/auth-v2-user
upvoted 1 times

lilalex 2 years, 5 months ago
Confirm. The answer is correct. You can see :https://docs.microsoft.com/en-us/graph/auth-v2-user
https://login.microsoftonline.com/{tenant}/oauth2/v2.0/authorize?
client_id=6731de76-14a6-49ae-97bc-6eba6914391e
&response_type=code
&redirect_uri=http%3A%2F%2Flocalhost%2Fmyapp%2F
&response_mode=query
&scope=offline_access%20user.read%20mail.read
&state=12345
upvoted 5 times

gaem Most Recent 4 months, 1 week ago
Selected Answer: C
C is the answer.
upvoted 1 times

Nilz76 6 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 1 times

Wearsy 1 year, 5 months ago
C
https://docs.microsoft.com/en-us/graph/auth-v2-user
The {tenant} value in the path of the request can be used to control who can sign into the application. The allowed values are common

both Microsoft accounts and work or school accounts, organizations for work or school accounts only, consumers for Microsoft accoun
only, and tenant identifiers such as the tenant ID or domain name. For more detail, see protocol basics.

This then refers you to check the protocols:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols#endpoints
upvoted 1 times

barba76 1 year, 9 months ago
C is correct. A is tricky
https://login.microsoftonline.com/contoso.onmicrosoft.com/ - works for users of that tenant
https://login.microsoftonline.com/common/ - works for any users of any tenant
upvoted 2 times

mkoprivnj 1 year, 9 months ago
C for sure!
upvoted 2 times

Karl12347 1 year, 10 months ago
correct answer is A
https://docs.microsoft.com/en-us/graph/auth/auth-concepts
upvoted 1 times

Fcnet 2 years, 4 months ago
As Alexander Said
The C answer is correct :
In a single tenant application, sign-in requests are sent to the tenant's sign-in endpoint. For example, for contoso.onmicrosoft.com the
endpoint would be: https://login.microsoftonline.com/contoso.onmicrosoft.com
from
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant#update-your-code-to-send-
requests-to-common
upvoted 4 times

zorro1 1 year, 4 months ago
It's Alexander Saad, not Alexander Said
upvoted 6 times

Ama100 2 years, 6 months ago
A is the correct answer. The login URL for apps is https://login.microsoftonline.com/" followed by tenant iD and tokens
upvoted 3 times

mgmjtech 2 years, 6 months ago
I don't think C is the answer. I leaning toward D.
upvoted 1 times

DRAG DROP -

Your company has a hybrid deployment of Azure Active Directory (Azure AD).

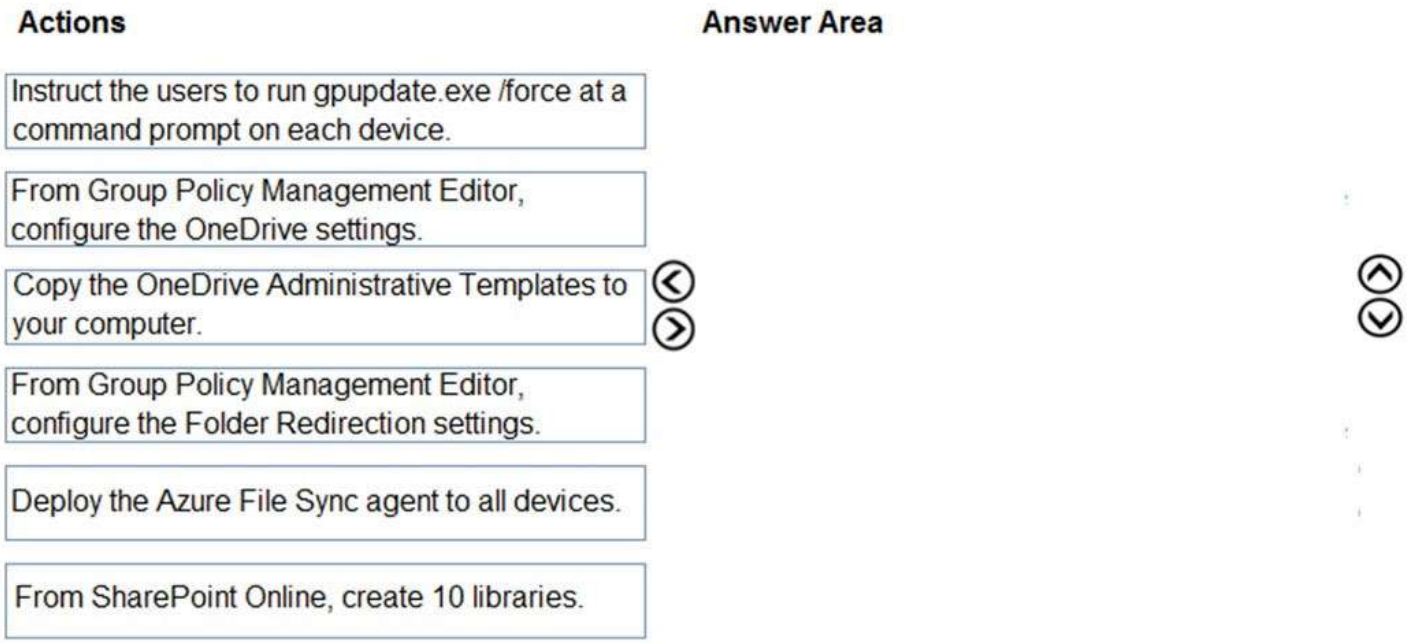
You purchase a Microsoft 365 subscription.

You plan to migrate the Home folder of each user to Microsoft 365 during several weeks. Each user has a device that runs Windows 10.

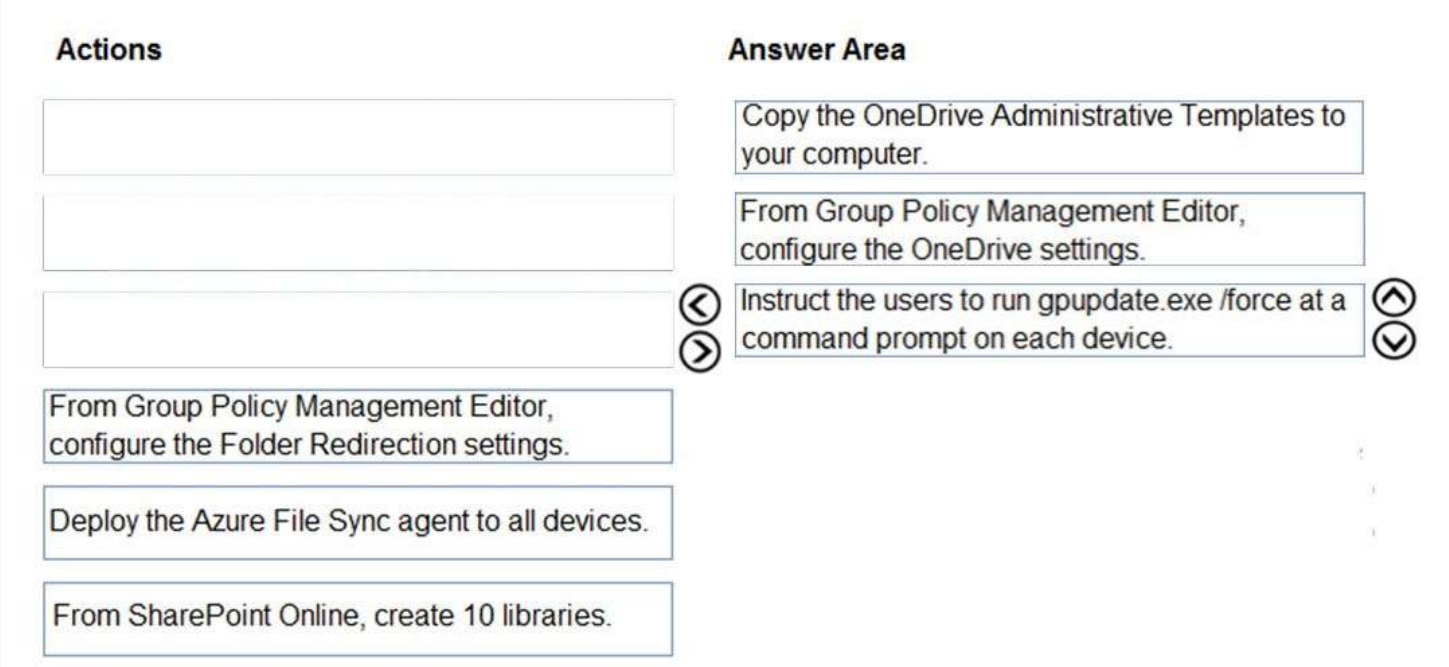
You need to recommend a solution to migrate the Home folder of five administrative users as quickly as possible.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



You need to configure a Group Policy Object (GPO) with the OneDrive settings required to redirect the Home folder of each user to Microsoft 365.

Before you can configure the Group Policy, you need to download the OneDrive Administrative Templates. These templates add the required OneDrive settings to Group Policy so you can configure the settings as required.

After the OneDrive settings have been configured in Group Policy, you can run the gpupdate /force command on the five computers to apply the

new Group Policy settings immediately.

Reference:

https://docs.microsoft.com/en-us/onedrive/use-group-policy

spg987 Highly Voted 1 year, 1 month ago

In exam today

upvoted 6 times

gaem Most Recent 4 months, 1 week ago

BDA, I would say...

upvoted 1 times

gaem 4 months, 2 weeks ago

DBA I suppose!
Please correct if I am wrong

upvoted 1 times

LoremanReturns 1 year, 3 months ago

"Copy the Onedrive administrative template to your computer" is wrong. Assuming that the Home Folder is located on a File Server an folder redirection GPO is applied to user devices to redirect home folders to the file server. So you need first change the Folder Redirec GPO to remove redirection to the file server, than create the new Onedrive GPO, finally instruct users to run gpupdate:
https://docs.microsoft.com/en-us/onedrive/redirect-known-folders#transition-from-the-windows-folder-redirection-group-policy-objec

upvoted 4 times

michszym 1 year, 3 months ago

Home Folder is not the same as Folder Redirection. Home Folder you can configure from AD account - Profile tab.

upvoted 1 times

Nilzuka 1 year, 4 months ago

Afterwards you need to use the sharepoint migration tool to migrate the files on the home folders to OneDrive, no? Why is it not in the answers?

upvoted 2 times

Turak64 1 year, 1 month ago

You'll need to run the SPMT for each user. I'd question why using the OneDrive known folders move isn't ine the list of answers, as that'll be much quicker.

upvoted 1 times

Ghostman 1 year, 4 months ago

For some reason you need to copy the amdx files from your local computer to the sysvol folder... the answer may be not completely correct.. thats were u start.. so it makes sort of sense

upvoted 3 times

adaniel89 1 year, 5 months ago

"Copy OneDrive Administrative Templates to your computer" - doesnt make any sense, just copying admx files doesnt do a thing, you need to also place is under \\yourdomainname\sysvol\domain\Policies\PolicyDefinitions

upvoted 1 times

Mujja 3 months, 3 weeks ago

You can copy the ADMX templates to PolicyDefinitions on your local computer then start GPMC to configure OneDrive settings. No need to copy to the CentralStore first.

upvoted 1 times

zorro1 1 year, 5 months ago

That's not an available answer. So copying makes most sense.
Answer looks reasonable to me.

upvoted 5 times

BDuff 8 months, 3 weeks ago

Agree with zorro1

upvoted 1 times

michszym 1 year, 3 months ago

In production environment this would be prefered solution - use Central Store to store admx files (you can manage GPO from any computer - no need to copy them to all workstations you want to modify GPO settings)
but as zorro1 wrote we have no such answer.

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a main office and three branch offices. All the branch offices connect to the main office by using a WAN link. The main office has a high-speed
Internet connection. All the branch offices connect to the Internet by using the main office connection.
Users use Microsoft Outlook 2016 to connect to a Microsoft Exchange Server mailbox hosted in the main office.
The users report that when the WAN link in their office becomes unavailable, they cannot access their mailbox.
You create a Microsoft 365 subscription, and then migrate all the user data to Microsoft 365.
You need to ensure that all the users can continue to use Outlook to receive email messages if a WAN link fails.
Solution: For each device, you configure an additional Outlook profile that uses IMAP.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The question states that the branch offices connect to the Internet by using the main office connections. Therefore, all Internet traffic goes over the WAN link between the branch office and main office.
After the migration, the users connect to their mailboxes hosted in Exchange Online over the Internet and therefore over the WAN link.
If the WAN link goes down, the branch office users will not be able to connect to the Internet and therefore will not be able to access their email using Outlook.
Using IMAP to access the mailboxes would still use the WAN link so this answer does achieve the goal.
The solution is to add a direct connection to the Internet from the branch offices, so their Internet traffic does not go over the WAN link.

mkoprivnj Highly Voted 1 year, 9 months ago
No for sure!
upvoted 7 times

T10T Most Recent 1 month, 3 weeks ago
Selected Answer: B
Solution: In each branch office, you add a direct connection to the Internet.
upvoted 1 times

shaan6810 1 year, 9 months ago
Why is this wrong? If your data is already in M365 can you not setup an outlook IMAP profile for your users?
upvoted 1 times

McAlec 1 year, 4 months ago
Because all the branch offices connect to the Internet by using the main office connection. Which means if the WAN is down, the branches have no connection to the Internet and tehy can't connect to M365 Services. IMAP will not solve that problem.
upvoted 1 times

chaoscreater 1 year, 3 months ago
what part of - "You need to ensure that all the users can continue to use Outlook to receive email messages if a WAN link fails." do y not understand? So you're saying that if any network link goes down, somehow using IMAP will address the issue? This is so basic.
upvoted 2 times

Durden871 7 months, 2 weeks ago
To be fair, the question is so stupid that I at first thought it was asking about your ability to read emails off-line with IMAP or something of the sort, but that didn't make sense either.
upvoted 1 times

titan_91 2 years ago
https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide#microsoft-365-connectivity-principles

"Enterprise WANs are often designed to backhaul network traffic to a central company head office for inspection before egress to the Internet, usually through one or more proxy servers. The diagram below illustrates such a network topology.

Because Microsoft 365 runs on the Microsoft Global Network, which includes front-end servers around the world, there will often be a front-end server close to the user's location. By providing local Internet egress and by configuring internal DNS servers to provide local name resolution for Microsoft 365 endpoints, network traffic destined for Microsoft 365 can connect to Microsoft 365 front end servers close as possible to the user."

upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a main office and three branch offices. All the branch offices connect to the main office by using a WAN link. The main office has a high-speed
Internet connection. All the branch offices connect to the Internet by using the main office connection.
Users use Microsoft Outlook 2016 to connect to a Microsoft Exchange Server mailbox hosted in the main office.
The users report that when the WAN link in their office becomes unavailable, they cannot access their mailbox.
You create a Microsoft 365 subscription, and then migrate all the user data to Microsoft 365.
You need to ensure that all the users can continue to use Outlook to receive email messages if a WAN link fails.
Solution: In each branch office, you add a direct connection to the Internet.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
The question states that the branch offices connect to the Internet by using the main office connections. Therefore, all Internet traffic goes over the WAN link between the branch office and main office.
After the migration, the users connect to their mailboxes hosted in Exchange Online over the Internet and therefore over the WAN link.
If the WAN link goes down, the branch office users will not be able to connect to the Internet and therefore will not be able to access their email using Outlook.
Adding a direct connection to the Internet from the branch offices would mean that the Internet traffic does not go over the WAN link. Therefore, if the WAN link fails, the users would still be able to access their email. Therefore, this solution does ensure that all the users can continue to use Outlook to receive email messages if a WAN link fails.

de_liberate Highly Voted 2 years, 5 months ago
Answer 'A' stands.
'You create a Microsoft 365 subscription, and then migrate all the user data to Microsoft 365' implies that the mailboxes are now in the EXO (Office 365).
Whether or not the Autodiscover record points to on-prem server or to the EXO directly (in case of Exchange Hybrid) is irrelevant as AutoDiscover will use fallback methods to get to the cloud mailboxes.
https://support.microsoft.com/en-us/help/3211279/outlook-2016-implementation-of-autodiscover
So SCP first and then , if not reachable, the published autodiscover point via local internet breakout.
upvoted 11 times

STFN2019 2 years, 2 months ago
precisely mate
upvoted 2 times

T10T Most Recent 1 month, 3 weeks ago
Selected Answer: A
I feel like this is common sense. I'd rather route straight to Microsoft 365 rather than hair-pinning through the corporate network anyw
This would be my default topology in the cloud-centric world we live in.
upvoted 2 times

mkoprivnj 1 year, 9 months ago
Yes, direct connection to internet!
upvoted 3 times

titan_91 2 years ago
https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide#microsoft-365-connectivity-principles

"Enterprise WANs are often designed to backhaul network traffic to a central company head office for inspection before egress to the Internet, usually through one or more proxy servers. The diagram below illustrates such a network topology.

Because Microsoft 365 runs on the Microsoft Global Network, which includes front-end servers around the world, there will often be a front-end server close to the user's location. By providing local Internet egress and by configuring internal DNS servers to provide local name resolution for Microsoft 365 endpoints, network traffic destined for Microsoft 365 can connect to Microsoft 365 front end servers close as possible to the user."

upvoted 1 times

zordss 2 years, 5 months ago

this is more like a question that would appear on network exams not on systems.

upvoted 4 times

WoneSix 2 years, 7 months ago

A direct connection to the Internet in the discussed scenario is not going to enable users to access email if the WAN link is saturated without first enabling Outlook Anywhere externally. By default, this is not enabled, so this is not a valid solution.

upvoted 4 times

STFN2019 2 years, 2 months ago

nah, it should work, direct connection mate

upvoted 1 times

Davidf 2 years, 4 months ago

"You create a Microsoft 365 subscription, and then migrate all the user data to Microsoft 365."

upvoted 9 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a main office and three branch offices. All the branch offices connect to the main office by using a WAN link. The main office has a high-speed
Internet connection. All the branch offices connect to the Internet by using the main office connection.
Users use Microsoft Outlook 2016 to connect to a Microsoft Exchange Server mailbox hosted in the main office.
The users report that when the WAN link in their office becomes unavailable, they cannot access their mailbox.
You create a Microsoft 365 subscription, and then migrate all the user data to Microsoft 365.
You need to ensure that all the users can continue to use Outlook to receive email messages if a WAN link fails.
Solution: You deploy a site-to-site VPN from each branch office to Microsoft Azure.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
The question states that the branch offices connect to the Internet by using the main office connections. Therefore, all Internet traffic goes over the WAN link between the branch office and main office.
After the migration, the users connect to their mailboxes hosted in Exchange Online over the Internet and therefore over the WAN link.
If the WAN link goes down, the branch office users will not be able to connect to the Internet and therefore will not be able to access their email using Outlook.
A site-to-site VPN from each branch office to Microsoft Azure would still use the WAN link so this answer does achieve the goal.
The solution is to add a direct connection to the Internet from the branch offices, so their Internet traffic does not go over the WAN link.

T10T 1 month, 3 weeks ago
Selected Answer: B
Solution: In each branch office, you add a direct connection to the Internet.
upvoted 1 times

harburn422 1 year, 7 months ago
Site 2 Site VPN to Azure, not happening. Answer is "B" for sure!
upvoted 1 times

mkoprivnj 1 year, 9 months ago
No for sure!
upvoted 2 times

phvogel 1 year, 12 months ago
I think this would solve the problem related to the WAN being down because the individual offices would communicate with Azure dire through their VPN -- the offices would no longer be dependent on the web. Microsoft says that VPNs aren't optimal (because of the additional encryption)...but it would solve the WAN problem.
upvoted 1 times

VTHAR 1 year, 11 months ago
Site-to-site VPN to Microsoft Azure would NOT solve WAN being down. One fundamental requirement to use M365 services is that y need to have Internet connection and Azure is not Internet. Related discussion here => https://techcommunity.microsoft.com/t5/azu active-directory-identity/create-site-to-site-vpn-to-azure-active-directory/m-p/1296089
upvoted 4 times

Question #35 *Topic 5*

You have an on-premises web application that is published by using a URL of https://app.contoso.local.
You purchase a Microsoft 365 subscription.
Several external users must be able to connect to the web application.
You need to recommend a solution for external access to the application. The solution must support multi-factor authentication.
Which two actions should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From an on-premises server, install a connector, and then publish the app.

B. From the Azure Active Directory admin center, enable an Application Proxy.

C. From the Azure Active Directory admin center, create a conditional access policy.

D. From an on-premises server, install an Authentication Agent.

E. Republish the web application by using https://app.contoso.com.

Correct Answer: *AB*
Azure Active Directory (Azure AD) has an Application Proxy service that enables users to access on-premises applications by signing in with their Azure AD account. The application proxy enables you to take advantage of Azure AD security features like Conditional Access and Multi-Factor Authentication.
To use Application Proxy, install a connector on each Windows server you're using with the Application Proxy service. The connector is an agent that manages the outbound connection from the on-premises application servers to Application Proxy in Azure AD.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

Daffygasbag Highly Voted 2 years, 7 months ago
Says in the question that it has to specifically support MFA, not implement it. So A/B would set up initially so that you can implement M after. To me, it seems they are just trying to catch you out with the wording...
upvoted 29 times

Carlos1787 1 year, 11 months ago
agree here, the key word is support
upvoted 3 times

ranc1d 2 years, 6 months ago
Yes: The solution must support multi-factor authentication, not enforce.
So A and B is correct.
upvoted 18 times

mkoprivnj Highly Voted 1 year, 9 months ago
A & C for sure!
upvoted 9 times

lfbustamante 1 year, 7 months ago
Totally Agree - (A) - https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application#install-and-register-a-connector // (C) - https://thesleepyadmins.com/2019/02/10/configure-mfa-for-azure-application-proxy/
upvoted 3 times

Mr01z0 1 year, 4 months ago
the question states: "must support MFA" it does not state "must have MFA configured"
upvoted 2 times

Alv86 Most Recent 6 months, 1 week ago
A & C
Why is the "Enable Application Proxy button grayed out?
Make sure you have at least an Azure AD Premium P1 or P2 license and an Azure AD Application Proxy Connector installed. After you successfully install your first connector, the Azure AD Application Proxy service will be enabled automatically.
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-faq
upvoted 1 times

jjong 1 year ago

came out in exam today

upvoted 2 times

Redrock2063 1 year, 1 month ago

Whether A & B, or A&C, or A,B &C, all three answer selections ignore the element of the question that states the URL is published as https://app.contoso.local. This makes it incompatible with a synchronized connection with Azure AAD M365. An unmentioned step of purchasing a viable domain name is absolutely necessary along with the step mentioned in E. to republish the web application using https://app.contoso.com.

upvoted 3 times

MomoLomo 1 year, 1 month ago

A and C

upvoted 1 times

Ash473 1 year, 1 month ago

In exam today

upvoted 3 times

melatocaroca 1 year, 4 months ago

They told
You need to recommend a solution for external access to the application.
The solution must support multi-factor authentication

A. From an on-premises server, install a connector, and then publish the app.
B. From the Azure Active Directory admin center, enable an Application Proxy.
C. From the Azure Active Directory admin center, create a conditional access policy.

A
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application
B
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-config-how-to
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application
C means enable MFA
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

They ask for two, when must be three, sio my guest is, A and B, or A and C, or B and C,

if you got this question mark for comments

upvoted 1 times

Nilzuka 1 year, 4 months ago

This question is outdated and has a dumb wordplay in it... I seriously hope I don't have it during the exam.

upvoted 4 times

AlexLiourtas 9 months, 4 weeks ago

only this? more than half of the test...

upvoted 1 times

VTHAR 1 year, 11 months ago

This question seems to be outdated. Step B is no longer required. https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-faq#why-is-the-enable-application-proxy-button-grayed-out

upvoted 6 times

VTHAR 1 year, 11 months ago

It was required in Azure classic portal. https://github.com/uglide/azure-content/blob/master/articles/active-directory/active-director
application-proxy-enable.md#step-1-enable-application-proxy-in-azure-ad

upvoted 2 times

AlexanderSaad 2 years, 5 months ago

App proxy is automatically enabled when you install the connector:
After you successfully install your first connector, the Azure AD Application Proxy service will be enabled automatically.
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-faq
So you don't have to enable it as stated in B?

upvoted 1 times

AlexanderSaad 2 years, 5 months ago

Unless the are talking about the legacy portal, which is depicted
https://github.com/uglide/azure-content/blob/master/articles/active-directory/active-directory-application-proxy-enable.md

upvoted 2 times

VTHAR 1 year, 11 months ago

Yes, it must be the reason.

upvoted 1 times

Voitec 2 years, 7 months ago

doco from references doesn't say that we need to enable connector in Azure portal, it says only that we need to download and install th connector. My guess is also A and C

upvoted 3 times

sailerjerry 2 years, 8 months ago

This doesn't make sense. Surely there are 3 steps required. A,B and C.

upvoted 3 times

sailerjerry 2 years, 8 months ago

Actually I guess you dont register the connector in Azure you do that during the installation of the connector. So it must be A and C.

upvoted 6 times

Fala_Fel 2 years, 7 months ago

Yes I'm going with A and C, if only 2 options are allowed. Installing the connector on the server registers the app with Azure.

upvoted 4 times

Goofer 2 years, 8 months ago

I don't get it.
1. install a application proxy on-premise
2. Create an Enterprise Application in Azure
3. Create a Conditional Access policy --> enable MFA

upvoted 5 times

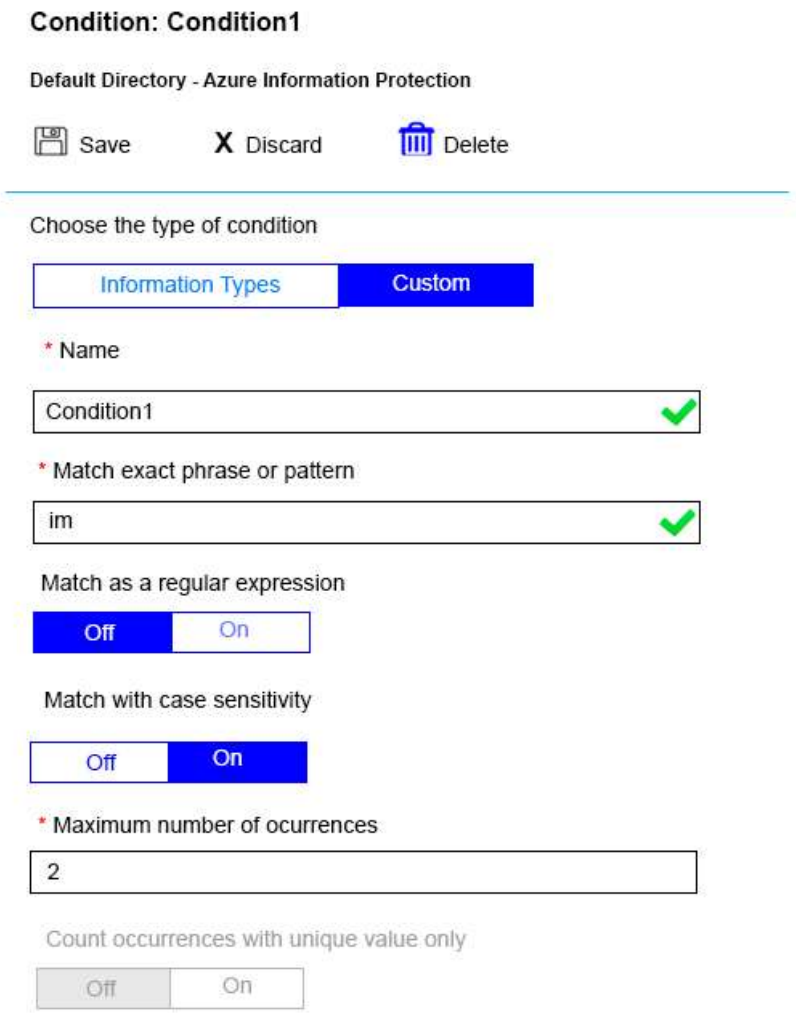
HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

A user named User1 has files on a Windows 10 device as shown in the following table.

Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Label1 applies to File1.docx.	○	○
Label1 applies to File2.docx.	○	○
Label1 applies to File3.docx.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Label1 applies to File1.docx.	○	●
Label1 applies to File2.docx.	●	○
Label1 applies to File3.docx.	○	●

The phrase to match is "im" and it is case sensitive. The phrase must also appear at least twice.

Box 1: No -

File1.docx contain the word "import" once only

Box 2: Yes -

File2.docx contains two occurrences of the word "import" as well as the word "imported"

Box 3: No -

File3.docx contains "IM" but his is not the correct letter case.

Reference:

https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

Benjam Highly Voted 2 years, 1 month ago

The phrase to match is "im" and it is case sensitive. The phrase must also appear at least twice.
Box 1: No
File1.docx contain the word "import" once only
Box 2: Yes
File2.docx contains two occurrences of the word "import" as well as the word "imported"
Box 3: No
File3.docx contains "IM" but his is not the correct letter case.

upvoted 15 times

txrocker13 Highly Voted 1 year, 9 months ago

I'm thinking Y, N, N.
File 1 only has one occurrence of im and the Max setting is set to 2
File 2 has 3 occurrences of im, which exceeds Max setting of 2
File 3 has no occurrences of lowercase im, so no match at all

upvoted 14 times

melatocaroca 1 year, 4 months ago

im is case sensitive. im must appear twice

Box 1: File1.docx contain the word "import" so im ocurr once Answer N

Box 2: File2.docx contains twice the word "import" and one "imported"
Max was set to 2, so there is three occurrences Answer N

Box 3: File3.docx contains "IM" but in upper case not lower case. Answer N
So my guest N, N, N

upvoted 5 times

dodzylla 10 months, 1 week ago

Actually, the "Maximum number of occurrences" means it can be 1 or 2. Even if it should be minimum.
im is case sensitive

Box 1 contains 1 im - Y
Box 2 contains 3 im - N
Box 3 0 - N

upvoted 5 times

FatsoGums Most Recent 11 months, 1 week ago

N.Y.N . Its on MS-101

upvoted 3 times

mkoprivnj 1 year, 9 months ago
Yes, No, No.
upvoted 5 times

PJR 2 years, 1 month ago
AIP in MS-101 - not MS-100
upvoted 5 times

STFN2019 2 years, 2 months ago
Shouldn't the answer be Y,Y,Y?
upvoted 1 times

STFN2019 2 years, 2 months ago
Sry, case sensitive enabled. The answer seems correct.
upvoted 4 times

hitten_za 2 years, 4 months ago
This is actually just confusing. There are the words "importing" and "import" in File 1 but the label doesn't apply?
upvoted 2 times

cloudnewb 2 years, 3 months ago
First word is with capitalized I so it's is "Importing" and the settings have case sensitive match so it won't be counted. Only one mat
in File 1.
upvoted 5 times

KINGisDEAD 2 years, 3 months ago
The first Importing is with a capital I
upvoted 2 times

itmp 2 years, 5 months ago
Answer is correct, but there is no "Maximum*" in AIP -> Labels -> Custom.
It is "Minimum*"
upvoted 6 times

ExamStudy68 2 years, 9 months ago
The question is almost cryptogamic in itself... wasn't quite sure what they were asking but makes sense after looking at the question
upvoted 3 times

Couch 2 years, 9 months ago
The image shows "Maximum" number of ocurrences...shouldn't it be "Minimum" ?
upvoted 9 times

d3an 2 years, 8 months ago
Yes, it should read 'Minimum number of occurrences'.
upvoted 6 times

HOTSPOT -

You have a Microsoft 365 subscription that uses a default named contoso.com.

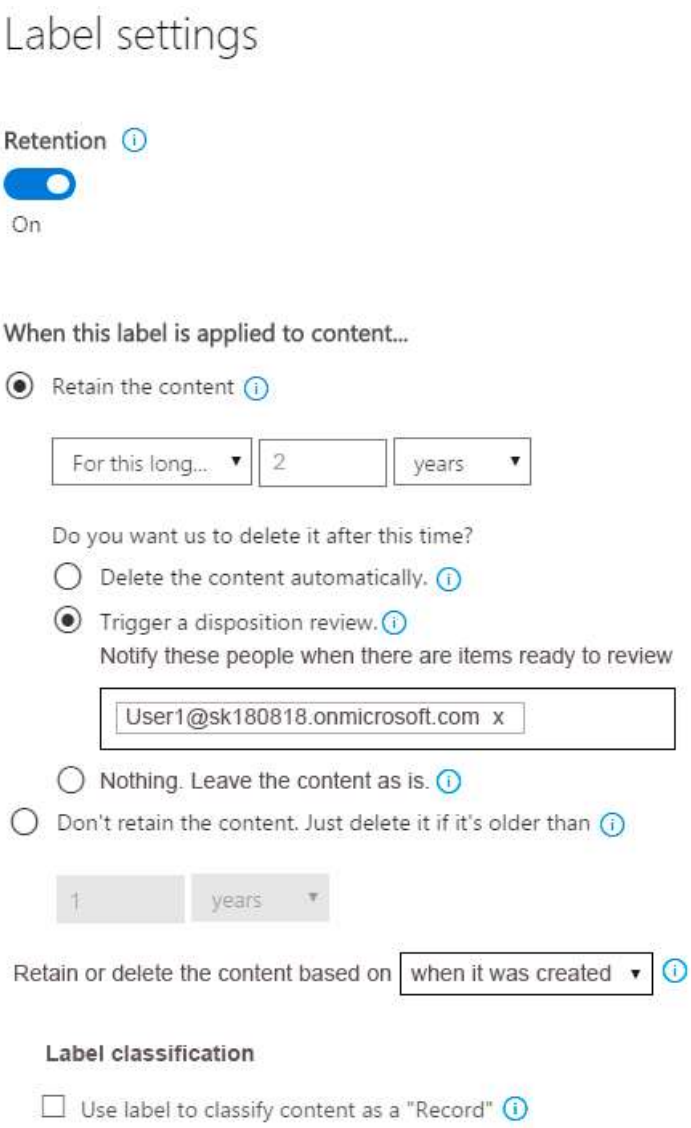
Three files were created on February 1, 2019, as shown in the following table.

Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

On March 1, 2019, you create two retention labels named Label1 and label2.

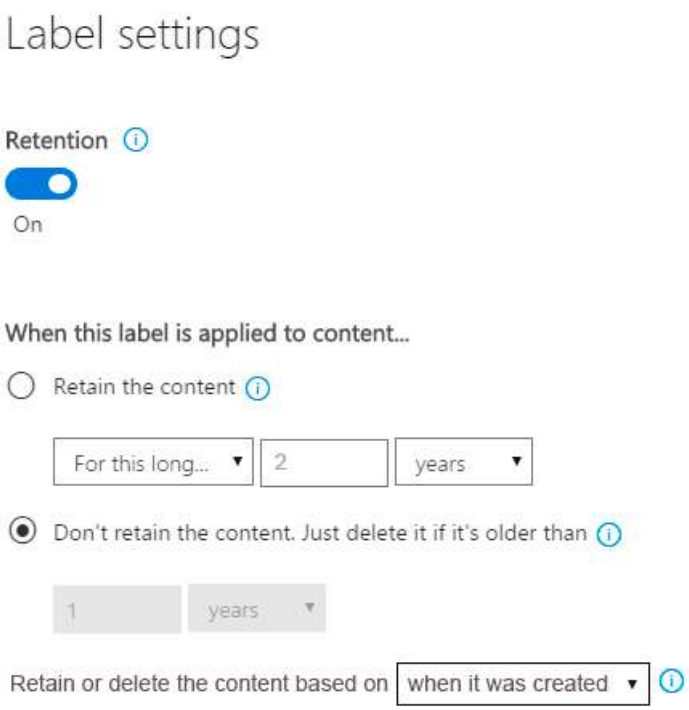
The settings for Label1 are configured as shown in the Label1 exhibit.

Label 1 -



The settings for Label2 are configured as shown in the Label1 exhibit.

Label 2 -



You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	○	○
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	○	○
File3 will be deleted automatically after February 1, 2021.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	○	○
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	○	○
File3 will be deleted automatically after February 1, 2021.	○	○

Box 1: No -

Retention overrides deletion.

Box 2: No -

Content in a document library will be moved to the first-stage Recycle Bin within 7 days of disposition, and then permanently deleted another 93 days after that.

Thus 100 days in total.

Box 3: No -

Items in an Exchange mailbox will be permanently deleted within 14 days of disposition.

Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews

stromnessian Highly Voted 1 year, 2 months ago
Question makes no sense.
upvoted 11 times

Gracha 8 months, 3 weeks ago
i agree with you on this one
upvoted 1 times

jkklim Most Recent 9 months, 2 weeks ago
NNN

as long as the person does not perform disposition, all files RETAINED.
upvoted 2 times

GoodLookingConsultant 10 months, 1 week ago
On Exam Nov 12
upvoted 4 times

jj2345 10 months, 2 weeks ago
There is nothing in the Question about Soft- and Harddelete so why should the answer include the retention times of Exchange or Sharepoint?
I would go with N Y Y - because the FIles are getting soft deleted wich is some kind of deletion. Aside from that you can change the retention times for example in Exchange Online from default 14 up to 30 days https://docs.microsoft.com/en-gb/exchange/recipients-i exchange-online/manage-user-mailboxes/change-deleted-item-retention
upvoted 1 times

allesglar 10 months, 3 weeks ago
The explanations and question really do not make any sense.
What has the recycle bin to do with an automatic deletion!? The question does not ask if the document gets retained or is accessible in some bin, but if the document gets deleted.
upvoted 2 times

Eggsamine 11 months, 2 weeks ago
MS-101?
upvoted 1 times

michszym 1 year, 3 months ago
I don't understand this question - The rule is "Only one retention label at a time. An email or document can have only a single retentior label applied to it at a time. " - see link in Ref: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldv --> so how can we know which retention label is for which File?

2nd link about Disposition review says: "Content pending a disposition review in those locations is permanently deleted only after a reviewer for the final stage of disposition chooses to permanently delete the content." So there is no such option like move to Recycle B and delete item after number of days
upvoted 1 times

chaoscreater 1 year, 2 months ago
Agreed, you can have multiple retention policies assigned to a content, but you can have only one retention label assigned to a content. I think when in doubt, just keep to the principle of retention wins over deletion and apply whatever policy that fits that principle.
upvoted 2 times

gsmith9897 1 year, 4 months ago
I don't understand the answer for Box 3. Is it saying File3 won't be deleted automatically or that it won't be deleted after February 1, 20 Disposition would take place on 1 February 2021 and, if the user doesn't complete the review, the file would be deleted on 15 February 2021, which would be both automatic and after February 1.
upvoted 3 times

lucidgreen 1 year, 5 months ago
Label 1 makes a requirement of dispositions. Dispositions do not expire.
upvoted 3 times

You manage multiple devices by using Microsoft Endpoint Manager. The devices run on the following operating systems:

- Android 8.0, Android 8.1.0, and Android 9
- iOS 12 and iOS 13
- MacOS 10.14
- Windows 10

You need to deploy Microsoft 365 apps to the devices.

From the Microsoft Endpoint Manager admin center, what is the minimum number of apps you should create?

A. 1

B. 3

C. 4

D. 7

Correct Answer: *C*

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

spg987 Highly Voted 1 year, 1 month ago

In exam today

upvoted 5 times

barthinho Most Recent 3 months, 3 weeks ago

M365 Enterprise apps - only WIN10 and MacOS, rest all.

upvoted 2 times

Nilz76 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 3 times

GoodLookingConsultant 10 months, 3 weeks ago

In exam on Nov 12

upvoted 4 times

Eggsamine 11 months, 2 weeks ago

MS-101?

upvoted 2 times

MartiFC 1 year, 2 months ago

We need to create 4 apps

upvoted 2 times

MartiFC 1 year, 2 months ago

So, the answer is correct

upvoted 1 times

Niro37 1 year, 2 months ago

This was a Question in the Exam i took on 27th July

upvoted 2 times

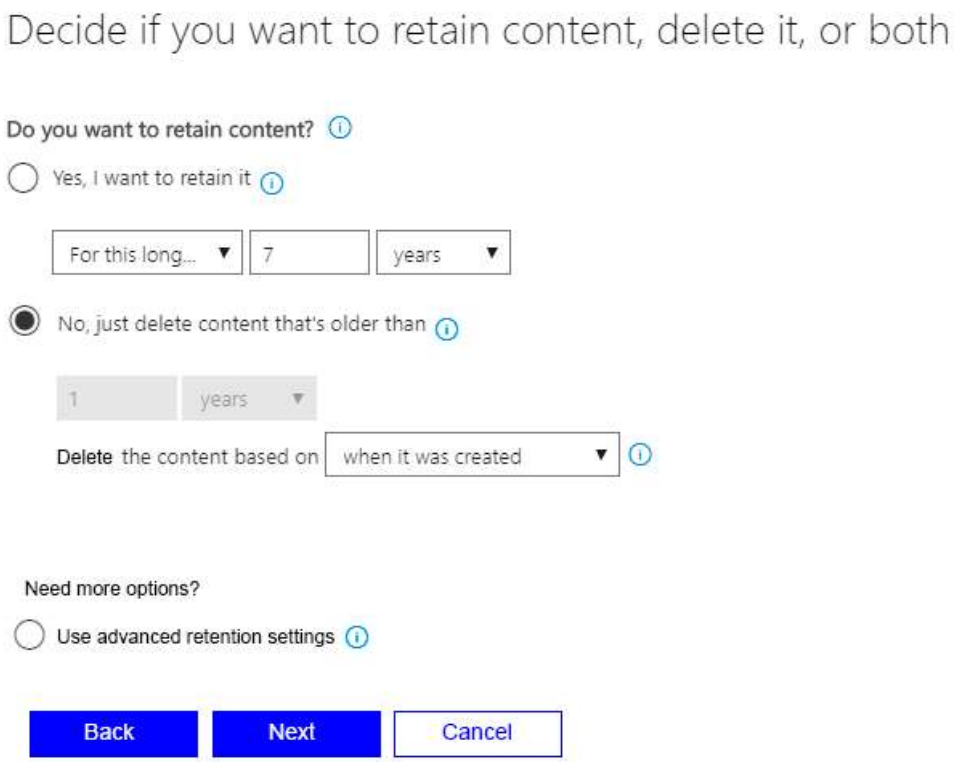
HOTSPOT -

You have retention policies in Microsoft 365 as shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

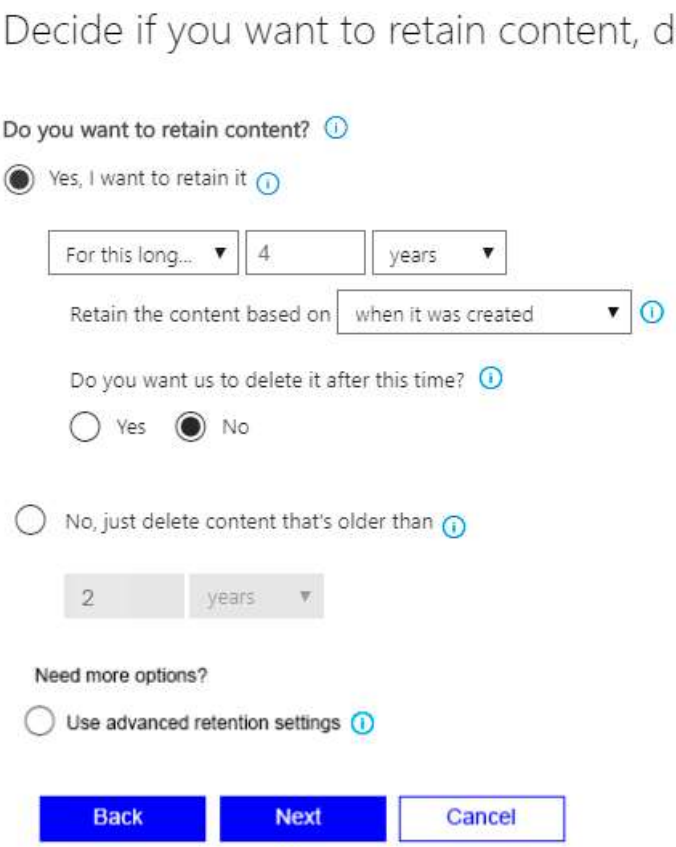
Policy1 is configured as shown in the Policy1 exhibit.

Policy1 -



Policy1 is configured as shown in the Policy2 exhibit.

Policy2 -



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, and administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, and administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

1. Retention wins over deletion. Suppose that one retention policy says to delete Exchange email after three years, but another retention policy says to retain

Exchange email for five years and then delete it. Any content that reaches three years old will be deleted and hidden from the users' view, but still retained in the Recoverable Items folder until the content reaches five years old, when it is permanently deleted.

2. The longest retention period wins. If content is subject to multiple policies that retain content, it will be retained until the end of the longest retention period.
Box 1: No.
The file will be deleted and hidden from the users' view, but still retained in the Recoverable Items folder. An administrator would need to recover the file.
Box 2: Yes.
The file will be deleted and hidden from the users' view, but still retained in the Recoverable Items folder. An administrator will be able to recover the file.
Box 3: Yes.
2018 to 2023 is five years. Policy2 has a retention period of four years. However, Policy2 is configured to not delete the files after the four-year retention period.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence

AnoniMouse Highly Voted 1 year, 5 months ago
I don't get it, deletion is after 7 years, but retention is for 4 years. So a file on Jan 2018 will still be available on Feb 2020 (only 2 years passed), so why the answer is NO?
upvoted 10 times

chaoscreater 1 year, 2 months ago
Deletion is after 1 year, not 7 years.....read the question again
upvoted 1 times

stromnessian 1 year, 2 months ago
Retention wins.
upvoted 3 times

stromnessian 1 year, 2 months ago
OK, I see - you're right, it would be deleted from the users' view.
upvoted 1 times

MessageMeThis 1 year, 1 month ago
The pic for Policy1 shows the wrong drop downs enabled/greyed out. The drop downs to set the delete time are greyed out even though that option is selected. Makes it seem like the drop downs above the delete radial are what's setting the time frame. It's a bit confusing and it got me as well until I read these comments.
upvoted 2 times

allesglar Highly Voted 11 months ago
I vote for Y,Y,N
Third answer is imo also wrong. It doesnt really matter if the second policy does not delete the documents after the retention period, t wont be retained if deleted and therefore the first policy applies.
upvoted 6 times

allesglar 10 months, 3 weeks ago
After more digging I'll go for N,Y,N. Indeed the users are not able to access the documents as it gets deleted automatically, only adm has access to it.
Q3 is N and here is the reason:
A timer job periodically cleans up the Preservation Hold library. For content that has been in the Preservation Hold library for more than 30 days, this job compares the content to all queries used by the retention settings for that content. Content that is older than their configured retention period is then deleted from the Preservation Hold library, and the original location if it is still there. This timer job runs every seven days, which means that together with the minimal 30 days, it can take up to 37 days for content to be deleted from the Preservation Hold library.
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide
upvoted 1 times

tcmaggio Most Recent 9 months, 2 weeks ago
YYN for me!
upvoted 4 times

jill44 9 months ago
I agree!
upvoted 2 times

GoodLookingConsultant 10 months, 1 week ago
On Exam Nov 12

upvoted 2 times

Eggsamine 11 months, 2 weeks ago
MS-101?
upvoted 1 times

TimurKazan 1 year ago
I would choose Y,Y,N
upvoted 4 times

TimurKazan 11 months ago
incorrect
upvoted 1 times

MartiFC 1 year, 1 month ago
Sorry but I don't understand the answers of first ask. "If a user creates a file..." no say DELETE, say CREATE, so why you don't access the file?
upvoted 3 times

Notorious19 1 year, 2 months ago
I don't get it, if both policy 1 and 2 are applied to OneDrive, and retention wins over deletion, how come the user is not able to access t file 2 years after it was created? should it not be retained for 4 years?
upvoted 3 times

joergsi 8 months, 1 week ago
It's in the 1. trashbin, only accessible for the admin not for a user.
upvoted 1 times

stromnessian 1 year, 2 months ago
YYN would be my guess.
upvoted 2 times

stromnessian 1 year, 2 months ago
On second thoughts NYN
upvoted 3 times

Wearsy 1 year, 5 months ago
Poor explination since there is no 'recoverable items' folder within OneDrive however after research this answer looks to be correct. So first retention policy will run and delete the file from user 1's OneDrive, however policy2 will keep a copy of the file indefinitely, going o the screenshot
upvoted 3 times

chaoscreater 1 year, 2 months ago
Man are you guys blind or what? File is not kept "indefinitely". It is kept for 4 years
upvoted 1 times

chaoscreater 1 year, 2 months ago
Sorry I missed the part where it says never delete after the 4 years period, which basically keeps the file indefinitely. You're right.
upvoted 1 times

michszym 1 year, 3 months ago
Where you found that 1st policy delete file from user? see section "The principles of retention, or what takes precedence?" here: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide - and this sentence: "The outcome isn' which single retention policy or single retention label wins, but how long an item is retained (if applicable) and when an item is dele (if applicable). These two actions are calculated independently from each other, from all the retention settings applied to an item."
I think Files from OneDrive will retain for 4 years and delete after this date because of Policy1

So in my opinion answers should be: Y, Y, N
upvoted 2 times

chaoscreater 1 year, 2 months ago
After a bit more researching and reading, I believe you are correct here.

- You can apply multiple retention policies to a file.
- You can apply only one retention label to a file.
- You can combine retention policies and label on the same content.
- The delete action from a retention label always takes precedence over the delete action from a retention policy.

- When there is a conflict between policies and label, the outcome isn't which single retention policy or single retention label wins but how long an item is retained (if applicable) and when an item is deleted (if applicable). These two actions are calculated independently from each other, from all of the retention settings that are applied to an item.

1. Retention wins over deletion
2. Longest retention period wins
3. Explicit wins over implicit for deletions
4. Shortest deletion period wins

- Content won't be permanently deleted when it has deletion policy and also retention policy applied to it. The delete process is s initiated and can remove the content from user view and searches. For example, a Sharepoint document is moved from the origi folder to the Preservation Holds folder. However, permanent deletion is suspended.

upvoted 4 times

michszym 1 year, 2 months ago

Ok I change my mind after read chaoscreater posts, so it shoud be NYN - after 4 years file from OneDrive will be deleted beca of Policy1

upvoted 1 times

chaoscreater 1 year, 2 months ago

Example: An email message is subject to a retention policy for Exchange that is configured to delete items after three years ar also has a retention label applied that is configured to retain items for five years.

The email message is retained for five years because this retention action takes precedence over deletion.

Any content that reaches three years old will be deleted and hidden from the users' view, but still retained in the Recoverable Items folder until the content reaches five years old, when it is permanently deleted.

The email message is permanently deleted at the end of the five years because of the delete action that was suspended while retention action was in effect.

From <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide>
From <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retenti or-what-takes-precedence>

upvoted 2 times

Alv86 6 months, 2 weeks ago

So the answer is NYN

upvoted 2 times

HOTSPOT -

You have a Microsoft SharePoint Online site and an on-premises file server.

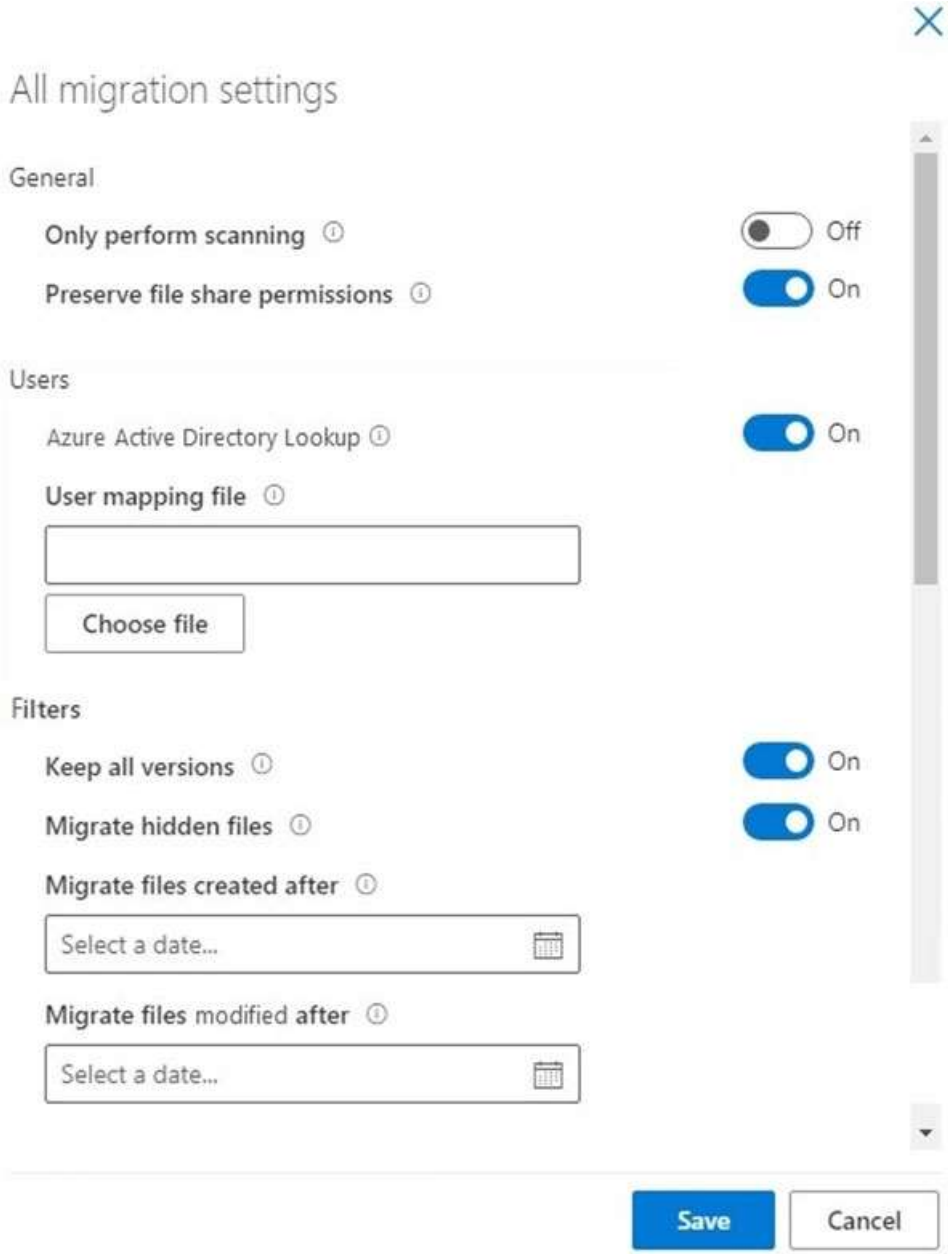
The site contains the files shown in the following table.

Name	In SharePoint library	Last modified
File1.docx	Documents	1/11/2019
File2.docx	Documents	1/12/2019

The file server contains the files shown in the following table.

Name	In folder	Last modified
File1.docx	D:\Folder1	1/1/2020
File2.xlsx	D:\Folder1	1/13/2020
File2.xlsx	D:\Folder2	1/7/2020
File3.pptx	D:\Folder2	1/20/2020

You migrate D:\Folder1 and D:\Folder2 to the Documents library by using the SharePoint Migration Tool as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
There will be two versions of File1.docx in the Documents library.	○	○
There will be two copies of File2.xlsx in the Documents library.	○	○
There will be a single copy of File3.pptx in the Documents library.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
There will be two versions of File1.docx in the Documents library.	○	○
There will be two copies of File2.xlsx in the Documents library.	○	○
There will be a single copy of File3.pptx in the Documents library.	○	○

You can't have two files with the same name and extension in a SharePoint documents library. If a file on the source server has the same and extension as an existing file in the document library, this will cause a conflict. The options for dealing with a conflict are: Skip, Merge, or Overwrite.

The ɹ€Keep all versionsɹ€ setting in the exhibit is used to retain the file history for a migrated file. It does not create multiple versions of a file in a document library.

Box 1: No -

File1.docx exists in the document library so this will cause a conflict.

Box 2: No -

Migrating two File2.xlsx files will cause a conflict.

Box 3: Yes -

There is only one File3.pptx in the source server and none in the document library so there will be no conflict.

jamspurple 2 months, 1 week ago

There seems to be different ways of approaching this question, the way i approach it is that they are migrating the folders, not the con of the folders.
Meaning the structure of the library will be as follows
Documents
-Folder1
-Folder2

Not a lot of merging happening here, so the answer will be
N (These are separate documents, not versions)
Y (Technically yes there are two copies in the library)
Y (lol)

upvoted 1 times

Nilz76 6 months ago

This question was in my exam on 06/April/2022. I passed.

upvoted 3 times

Alv86 6 months, 2 weeks ago

Merging Behavior
Possible values: “Never overwrite an existing file”, “Overwrite only if the source file is newer” and “Always overwrite an existing file”
Default Value: “Overwrite only if the source file is newer”
This setting defines, if the tool should overwrite existing files during merging local folder structure with existing structure in SharePoin you are going to use the tool for incremental migration, this setting option may be very helpful.

upvoted 1 times

TashaGirl 8 months, 3 weeks ago

Answer is correct but explanation does not make sense in its current wording. Here is the exercise:

First things first - no information about SPMT version, but let's take the newest general availability one:
Step 1: Copy content from > File share
Step 2: Select source Folder 1 > options: Migrate only folder contents(!)
Step 3: Destination SPO site - Documents library
Step 4: Name your migration + add another and configure as above for Folder 2
Step 5: Choose your settings (match the picture).
Step 6: migrate
This results in 0 errors. Items migrated.

Now, back to the SPO library:

File1.docx WAS replaced by the file migrated - no other versions exist.
File2.xlsx WAS migrated as ONE file (based on dates) and there is only ONE file.
Fil3.pptx was migrated and seems to be in this question just for fun.

upvoted 3 times

BDuff 8 months, 3 weeks ago

Very tricky question. Typical Microsoft.

--There will be two versions of File1.docx in the Documents library.
Technically there will be two copies, one in the root and one in Folder1. However, if "versions" refers to SharePoint versioning, then the will only be one SharePoint version of each file. Assuming "versions" refers to SharePoint versioning, then the answer would be no. If "versions" means a copy of the file, then the answer would be yes. Since the second question mentions "copies" I'll assume this one is referring to SharePoint versioning and go with No.

--There will be two copies of File2.xlsx in the Documents Library.
No. There will be 3 copies: the existing one in the root, one in Folder1 and one in Folder2.

--There will be a single copy of File3.pptx in the Documents Library.
Clearly yes. It does not exist and we migrated it.

So I'm going with NNY

upvoted 2 times

mib1024 6 months, 1 week ago

I think it should be NYY - read carefully

1. NO - as you say, two COPIES but only one VERSION
2. Yes - two copies, one in Folder1 and one in Folder2; the existing file in the root is File2.DOCX not File2.XLSX
3. Yes

upvoted 2 times

Davidchercm 9 months, 1 week ago

the answer should be YNY

upvoted 2 times

stoneface 9 months ago

YNY for sure!

upvoted 1 times

itmaster 5 months, 4 weeks ago

Are you serious guys? Why would be 2 versions as a result of migration? New versions are added when you modify a file, not whe you copy a second file to the same directory!

upvoted 1 times

GoodLookingConsultant 10 months, 1 week ago

In exam on Nov 12

upvoted 1 times

jjong 1 year ago

this came out in exam today

upvoted 3 times

MartiFC 1 year, 1 month ago

File1 may be Y?

upvoted 2 times

dminerva94 1 year, 1 month ago

There can never be 2 copys of the same exact file name/type in the same directory. Maybe you will be able to access different versions/revisions. But not as 2 different copies

upvoted 2 times

allesglar 10 months, 3 weeks ago

Yeah but File1 refers to 2 versions not copies...

upvoted 1 times

Question #41 *Topic 5*

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the word ProjectX.

You need to export the results of the content search.

What do you need to download the report?

A. an export key

B. a password

C. a user certificate

D. a certification authority (CA) certificate

Correct Answer: *A*

When you export a report, the data is temporarily stored in a unique Azure Storage area in the Microsoft cloud before it's downloaded to your local computer.

To download the report from the Azure Storage Area, you need an export key.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/export-a-content-search-report

mackypatio Highly Voted 1 year, 4 months ago

A for sure. Export key. doing this on a regular basis.
pro tip: must use microsoft edge. does not fully work on other browser.

upvoted 9 times

mkoprivnj Most Recent 1 year, 9 months ago

A for sure!

upvoted 4 times

Jake1 1 year, 10 months ago

Answer is correct.On the flyout page under Export key, click Copy to clipboard. You use this key in step 6 to download the search results

upvoted 4 times

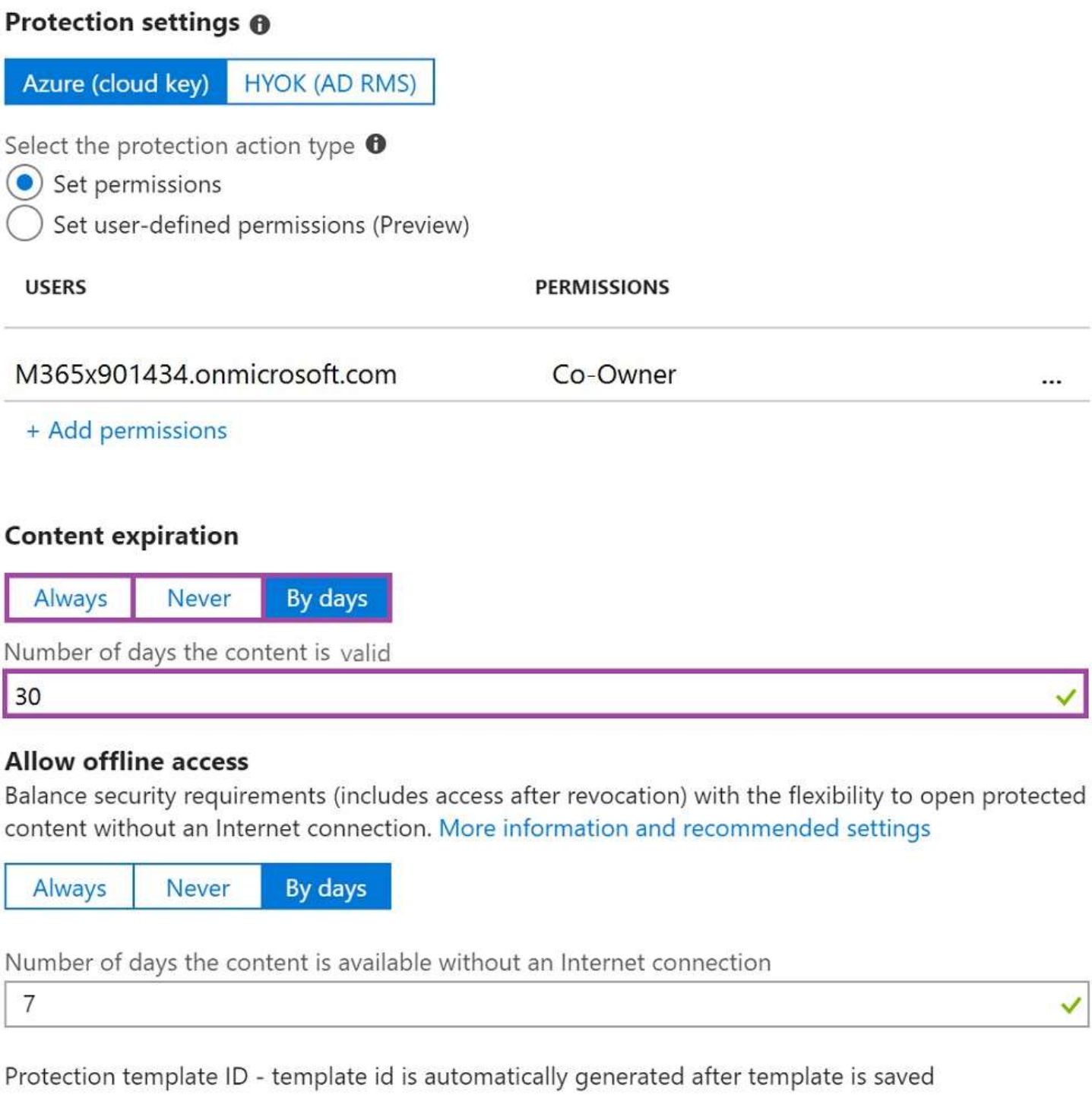
Annna 2 years ago

https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results

upvoted 4 times

HOTSPOT -

You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you copy the file from OneDrive to your internet connected computer, you [answer choice].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

If you email the document to a user outside your organization, the user [answer choice].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

Correct Answer:

Answer Area

If you copy the file from OneDrive to your internet connected computer, you [answer choice].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- **can open the document for up to 30 days**

If you email the document to a user outside your organization, the user [answer choice].

- **cannot open the document**
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

Box 1:

If you copy the file from OneDrive to your internet connected computer, you can open the document for up to 30 days. This is because the ג€Number of days the content is validג€ setting is set to 30 days.

Box 2:

If you email the document to a user outside your organization, the user cannot open the document. To open the document, the user would need to be added to the Users list and assigned permission. With the configuration in the exhibit, only the user listed in the Users list and the creator of the document can open the document.

Reference:

https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection

mkoprivnj Highly Voted 1 year, 9 months ago

4 & 1. PC has access to internet hence 30 days.

upvoted 5 times

Eggsamine Most Recent 11 months, 2 weeks ago

MS-101?

upvoted 2 times

donathon 1 year, 12 months ago

The computer is connected to the internet and hence you will have access for 30 days. The access is granted only to the user with that specific mailbox.

upvoted 4 times

Annna 2 years ago

How I can access Azure Information protection? (I can't find i in azure aztive directory)

upvoted 3 times

chaoscreater 1 year, 3 months ago

Ever heard of this amazing tool called Google?

upvoted 5 times

Durden871 7 months, 1 week ago

I'm assuming you got 100% on this and every test you've taken given some of the comments you make on here.

upvoted 1 times

Turak64 1 year, 1 month ago

Helpful

upvoted 1 times

zyir 11 months, 3 weeks ago

Not funny lad

upvoted 2 times

melatocaroca 1 year, 3 months ago

https://portal.azurerms.com/

upvoted 2 times

manis73 3 months, 2 weeks ago

in the compliance admin portal

upvoted 1 times

manis73 3 months, 2 weeks ago

sorry ignore that, you can find in in the security services in the azure portal. (just search for it when in the portal)

upvoted 1 times

Question #43 *Topic 5*

You have a Microsoft 365 subscription that contains a user named User1.

You need to ensure that User1 receives Microsoft 365 feature and service updates before the updates are released to all users.

What should you do in the Microsoft 365 admin center?

A. Modify the privileged access management settings.

B. Modify Office software download settings.

C. Modify the Release preferences settings.

D. Submit a new service request.

Correct Answer: *C*

Reference:

https://practical365.com/blog/first-steps-configure-office-365-first-release-settings/

joergsi Highly Voted 8 months, 1 week ago

https://docs.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide#set-up-the-releas
option-in-the-admin-center

- In the admin center, go to the Settings > Org Setting, and under the Organization profile tab, choose Release preferences.

- To enable targeted release for some people in your organization, select Targeted release for selected users, then select Save changes

upvoted 6 times

You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online
In the mailbox of a user named User, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do first?

A. From the Exchange admin center, start a mail flow message trace.

B. From the Security & Compliance admin center, start a message trace.

C. From the Security & Compliance admin center, create a label and label policy.

D. From the Exchange admin center, create a mail flow rule.

Correct Answer: *C*
When you configure conditions for a label, you can automatically assign a label to a document or email. In this case, we would create a label to label all email messages that contain the word ProjectX. We would then create a label policy to preserve a copy of all message that have the label assigned.
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

Martyvdb Highly Voted 1 year, 10 months ago
Mail Flow would make sense for any NEW emails, but does not address existing ones, so it would have to be a label situation.
upvoted 9 times

mkoprivnj Highly Voted 1 year, 9 months ago
C for sure!
upvoted 5 times

renrenren Most Recent 3 months, 2 weeks ago
How do I make lables and retention policy to identify the words ProjectX? in the lab I can not specify.
upvoted 1 times

renrenren 3 months, 2 weeks ago
It can be done by: Create Labels-->Auto-apply a label in Label policies, you can specify words. Therefore C is correct.
upvoted 1 times

jkklim 9 months, 2 weeks ago
C. - PRESERVE A COPY.

Even if new mail comes in, the label policy can PRESERVE both new and existing copy with the word ProjectX
upvoted 1 times

Eggsamine 11 months, 2 weeks ago
MS-101?
upvoted 1 times

subbuhotmail 1 year, 2 months ago
But in Label or Retention policy, is there any option to search for like ProjectX?

As far as i tested in the lab, while creating the label it just ask for whether to retain or delete and the location only. In the location, choo
Exchange and specify the user, thats it.

I dont see any option to mention the search word. I'm not sure about the other answers, but to me C is not the correct one.
upvoted 2 times

PJR 2 years, 1 month ago
I think its correct - in order to apply the label using any of the options listed it will have to be created first, in order for you to select it.
upvoted 1 times

moh15 2 years, 1 month ago
all ans are wrong eDiscovery

upvoted 3 times

Dimonchik 2 years ago
There is no eDiscovery in the question, man.
upvoted 2 times

moh15 2 years ago
i mean expected great proper ans. as mail flow rule will be not prof. solution for such case
upvoted 1 times

VTHAR 1 year, 11 months ago
eDiscovery is not the only way to achieve its objective. The question and answer make sense as well as it's correct.
upvoted 3 times

SinghG 2 years, 1 month ago
Answer C is correct but reference link provided is wrong. Instead of AIP label, a retention label and a policy will be required to automatically apply the label to emails with keyword.
upvoted 1 times

JaBe 2 years, 2 months ago
Labeling the message is not the same thing as preserving a copy. So a mail flow rule may indeed be the better answer.
upvoted 1 times

FableFa 2 years, 3 months ago
Answer A - Create a mailflow based on a DLP condition...
upvoted 1 times

FableFa 2 years, 3 months ago
Sorry type - Answer D. Mailflow rules
upvoted 1 times

Taksaka 2 years, 3 months ago
We can create a mail flow policy, set bcc and preserve the email in another mailbox.
upvoted 3 times

AADapson 1 year, 8 months ago
You can't create a mail flow policy for mails already in the user's mailbox.

Retention Label to hold content is the solution
upvoted 2 times

lilalex 2 years, 5 months ago
the others option not make sense
upvoted 1 times

zordss 2 years, 5 months ago
What kind of label & label policy?
upvoted 2 times

Shar9y 2 years, 4 months ago
Retention Label/Policy I'd assume..
upvoted 3 times

HOTSPOT -

You have a Microsoft 365 subscription.

You have a group named Support. Users in the Support group frequently send email messages to external users.

The manager of the Support group wants to randomly review messages that contain attachments.

You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To meet the goal for the manager, create: [▼]
- A label policy
- A retention policy
- A supervisor policy
- An alert policy
- MyAnalytics

To review the messages, the manager must use: [▼]
- A message trace
- An eDiscovery case
- MyAnalytics
- Outlook Web App

Correct Answer:

Answer Area

To meet the goal for the manager, create: [▼]
- A label policy
- A retention policy
- **A supervisor policy**
- An alert policy
- MyAnalytics

To review the messages, the manager must use: [▼]
- A message trace
- An eDiscovery case
- MyAnalytics
- **Outlook Web App**

Supervision policies in Office 365 allow you to capture employee communications for examination by designated reviewers. You can define specific policies that capture internal and external email, Microsoft Teams, or 3rd-party communications in your organization.

You create supervision policies in the Compliance center. These policies define which communications and users are subject to review in your organization and specify who should perform reviews.

If you want to reduce the amount of content to review, you can specify a percentage of all the communications governed by a supervision policy. A real-time, random sample of content is selected from the total percentage of content that matches chosen policy conditions.

Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/supervision-policies

T_B Highly Voted 2 years, 3 months ago

The use of supervison policy is just retired: https://docs.microsoft.com/en-us/microsoft-365/compliance/supervision-policies?view=o36 worldwide

upvoted 10 times

mkoprivnj Highly Voted 1 year, 9 months ago

A supervisor policy.
OWA

upvoted 8 times

PowerTrompStomp Most Recent 7 months, 1 week ago

Supervisor policy was retired and replaced by Communication Compliance policy from the compliance center.

upvoted 2 times

Eggsamine 11 months, 2 weeks ago

MS-101?

upvoted 3 times

donathon 1 year, 12 months ago

Answer
• A supervisor policy.
• An eDiscovery case
https://docs.microsoft.com/en-us/microsoft-365/compliance/supervision-policies?view=o365-worldwide >> This actually shows it shoul
be compliance center so eDiscovery case is the closest answer. As we speak, this feature is being replaced by communication complian
policies. https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide
MyAnalytics: The MyAnalytics Network page shows how many people you actively connect with in the last month and gives you suggestions on how to improve connections with your most important contacts, such as your manager or your direct reports.

upvoted 1 times

VTHAR 1 year, 11 months ago

No, the correct answer is OWA. https://www.enowsoftware.com/solutions-engine/supervisory-review-in-office-365

upvoted 7 times

melatocaroca 1 year, 3 months ago

ediscovery require more work Ned to install Microsoft has created an app that can be installed in OWA for Supervisory Review. To in
the app, run the following command in remote PowerShell connected to your Exchange Online tenant.

upvoted 1 times

Raj2020 2 years, 3 months ago

Communication and compliance policy from compliance center full fill this request.
https://docs.microsoft.com/en-us/microsoft-365/compliance/supervision-policies?view=o365-worldwide#:~:text=Supervision%20policies%20in%20Microsoft%20365,party%20communications%20in%20your%20organization.

upvoted 5 times

HOTSPOT -

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the
.abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

- Exempt apps: App2
- Protected apps: App1
- Windows Information Protection mode: Block
- Network boundary: IPv4 range of 192.168.1.1-192.168.1.255

You need to identify the apps from which you can open File1.abc

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can open File1.abc in App1.	○	○
You can open File1.abc in App2.	○	○
You can open File1.abc in App3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can open File1.abc in App1.	○	○
You can open File1.abc in App2.	○	○
You can open File1.abc in App3.	○	○

Box 1: Yes.

App1 is a protect app in the Windows Information Protection policy. File1 is stored on Server1 which is in the Network Boundary defined in the policy. Therefore, you can open File1 in App1.

Box 2: Yes.

App2 is exempt in the Windows Information Protection policy. The protection mode in the policy is block so all apps that are not included in the policy cannot be used to open the fileא€¦ except for exempt apps. Therefore, you can open File1 in App2.

Box 3: No.

The protection mode in the policy is block so all apps that are not included in the policy as protected apps or listed as exempt from the policy cannot be used to open the file. Therefore, you cannot open File from in App3.

Reference:

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

Asser Highly Voted 2 years, 7 months ago

Protected apps: These apps are the apps that need to adhere to this policy.
Exempt apps: These apps are exempt from this policy and can access corporate data without restrictions.
--> Given answer seems to be correct
upvoted 14 times

minajahan 2 years, 7 months ago
Windows Information Protection mode: Block
and App1 is a protected app...

so answer for 1st option should be "NO" since access of App1 to File1.abc should be blocked...?
upvoted 1 times

FableFa 2 years, 3 months ago
yes but Server 1 is in the network boundary and then consiodered as "enterprise data" -> answer 1 is YES
upvoted 4 times

moh15 Highly Voted 2 years, 3 months ago
Ans. Is Correct
upvoted 6 times

Eggsamine Most Recent 11 months, 2 weeks ago
MS-101?
upvoted 3 times

marco12345678 1 year, 6 months ago
why is app3 no
upvoted 2 times

Razuli 1 year, 4 months ago
Because of the block rule and the app not being in policy I think
upvoted 1 times

chaoscreater 1 year, 3 months ago
Everytime I see your comment, it's absolutely incorrect. Don't bother commenting if you're unsure, it just misleads others and we have enough idiots here as it is.

The answer is because App3 is accessing File1.abc, which is stored on Server1. Server 1 is included in the network boundary of th policy and therefore the policy applies.
upvoted 9 times

mkoprivnj 1 year, 9 months ago
Yes, Yes, No!
upvoted 3 times

Gresch123123 6 months, 1 week ago
for sure
upvoted 3 times

Mary_Yvette 2 years, 6 months ago
Using protected apps. Managed apps (apps that you've included on the Protected apps list in your WIP policy) are allowed to access yo enterprise data and will interact differently when used with unallowed, non-enterprise aware, or personal-only apps. For example, if W management is set to Block, your employees can copy and paste from one protected app to another protected app, but not to persona apps.
upvoted 1 times

Infinity 2 years, 6 months ago
Shouldn't App3 can open file1.abc as the WIP is not applied on it?
upvoted 2 times

MerryWeasel 1 year, 8 months ago
Given answer seems to be correct, Y - Y - N.
Explanation:
Protected apps - These apps are the apps that need to comply with policy.
Exempt apps: These apps are exempt from this policy and can access corporate data without any restrictions.
As for App3: "Managed apps and restrictions. With WIP you can control which apps can access and use your enterprise data. After adding an app to your protected apps list, the app is trusted with enterprise data. All apps not on this list are stopped from accessin your enterprise data, depending on your WIP management-mode." Since App3 is not on WIP list it cannot access the corporate data
References:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-usin intune-azure

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/protect-enterprise-dat using-wip#why-use-wip

upvoted 7 times

painkillers 2 years, 9 months ago

I think app1 cannot open file1.abc in app1. File1.abc is in the network boundary, the protection mode is "block". Can someone let me know?

upvoted 4 times

Sisko 2 years, 8 months ago

I agree with you. Why is App1 a yes?

upvoted 1 times

steven1 2 years, 8 months ago

Because App3 is not included in the WIP label.

upvoted 1 times

ExamStudy68 2 years, 8 months ago

I think the network boundary is where apps CAN access the data - see this link about half way down https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-usin intune-azure

upvoted 3 times

Hamster5000 2 years, 7 months ago

Network boundary is an inclusion, meaning allowed network addresses, anything outside of it will be blocked. When WIP is configur to 'Blocked', it restricts anything that does not comply with the rule, NOT what matches it. Which is why your conclusion is incorrect.

upvoted 7 times

FcoGlezRoy 2 years, 4 months ago

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure#choose-where-apps-can-access-enterprise-data

upvoted 1 times

Davidf 2 years, 4 months ago

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/protect-enterprise-dat using-wip

"if WIP management is set to Block, your employees can copy and paste from one protected app to another protected app, but not t personal apps."

It's not referring to blocking the file being opened, but where data can be copied to

upvoted 3 times

You have a Microsoft Power Platform production environment that contains a custom model-driven Microsoft Power Apps app.
How many days will system backups be retained for the environment?

A. 7

B. 14

C. 28

D. 90

Correct Answer: *C*
All your environments, except Trial environments (standard and subscription-based), are backed up. System backups for production environments that have been created with a database and have one or more Dynamics 365 applications installed are retained up to 28 days. System backups for production environments which do not have Dynamics 365 applications deployed in them will be retained for 7 days. System backups for sandbox environments will be retained for 7 days.
Reference:
https://docs.microsoft.com/en-us/power-platform/admin/backup-restore-environments

PmgCosta 5 months, 1 week ago

Selected Answer: A

From: https://docs.microsoft.com/en-us/power-platform/admin/backup-restore-environments

System backups for production environments that have been created with a database and have one or more Dynamics 365 application installed are retained up to 28 days. System backups for production environments which don't have Dynamics 365 applications deploye in them will be retained for 7 days. System backups for sandbox environments will be retained for 7 days.

upvoted 1 times

jkklim 9 months, 1 week ago

custom driven will be 28 days

upvoted 2 times

GoodLookingConsultant 10 months, 3 weeks ago

In exam on Nov 12

upvoted 4 times

melatocaroca 1 year, 3 months ago

They do not tell us Dynamics 365 applications installed Answer 7

System backups for production environments that have been created with a database and have one or more Dynamics 365 application installed are retained up to 28 days.

System backups for production environments which do not have Dynamics 365 applications deployed in them will be retained for 7 day

System backups for sandbox environments will be retained for 7 days.

upvoted 1 times

melatocaroca 1 year, 3 months ago

Correct myself, 28 days

PowerApps is the platform on which Dynamics 365 apps are natively built. Model-driven apps provides a no-code or low-code component approach to app development. Model-driven apps run with the new Unified Interface client which provides a responsive accessible design running in browsers and on popular mobile devices.

upvoted 2 times

itstudy369 1 year, 3 months ago

This should be 7 days

upvoted 3 times

F_M 1 year, 3 months ago

A custom model-driven Microsoft Power Apps app is not a Dynamic 365 app. So the answer should be 7 as no Dynamic 365 app is in th environment. Am i wrong?

upvoted 4 times

F_M 1 year, 3 months ago

https://www.arbelatech.com/insights-resources/blog/what-is-powerapps-and-what-does-it-mean-for-dynamics-365-customer-engagement.html

Looks like a model-driven app relies on the Dynamic365 framework so 28 days should be the correct answer

upvoted 4 times

zorro1 1 year, 5 months ago

Correct

upvoted 2 times

HOTSPOT -

You need to ensure that a user named User1 can create documents by using Office for the web.

Which two Microsoft Office 365 license options should you turn on for User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct section is worth one point.

Hot Area:

Answer Area

Office 365 E3

Azure Rights Management	Off	On
Exchange Online (Plan 2)	Off	On
Flow for Office 365	Off	On
Information Protection for Office 365 - Standard	Off	On
Insights by MyAnalytics	Off	On
Microsoft 365 Apps for enterprise	Off	On
Microsoft Bookings	Off	On
Microsoft Forms (Plan E3)	Off	On
Microsoft Kaizala Pro	Off	On
Microsoft Planner	Off	On
Microsoft StaffHub	Off	On
Microsoft Stream for O365 E3 SKU	Off	On
Microsoft Teams	Off	On
Office for the web	Off	On
PowerApps for Office 365	Off	On
SharePoint Online (Plan 2)	Off	On
Skype for Business Online (Plan 2)	Off	On
Sway	Off	On
To-Do (Plan 2)	Off	On

Correct Answer:

Answer Area



Rjnagoo Highly Voted 1 year, 5 months ago

Wrong! This is Office on the Web and SharePoint Online as you need somewhere to store/access documents

upvoted 48 times

TashaGirl 8 months, 3 weeks ago

SharePoint Online license is a dependency for Office on the Web license - you cannot assign this without SPO license.

upvoted 4 times

adaniel89 1 year, 5 months ago

Exactly my answer too!

upvoted 7 times

TimNov Highly Voted 1 year, 4 months ago

My instinct was Office on the Web (Create and Edit) and SharePoint Online (Save and access).

upvoted 13 times

allesglar Most Recent 11 months ago

Yep the answer is wrong. M365 Apps for Enterprise is needed only for using the M365 client apps but not for creating content in office the web. One just need a storage space, OneDrive or SharePoint, meaning the SharePoint license.

upvoted 1 times

MomoLomo 1 year, 2 months ago

Did a repro and when assigning only office for the web you get an error

To assign a license that contains Office for the web, you must also assign one of the following service plans: SharePoint (Plan 2), SharePoint (Plan 1).

upvoted 3 times

Noie 1 year, 2 months ago

Microsoft 365 Apps includes OneDrive to store the files.

upvoted 1 times

joergsi 8 months ago

And OneDrive is a "masked" SharePoint Online!

upvoted 1 times

melatocaroca 1 year, 4 months ago

Office for the web (formerly Office Web Apps) opens Word, Excel, OneNote, and PowerPoint documents in your web browser. Office for the web makes it easier to work and share Office files from anywhere with an internet connection, from almost any device. Microsoft 3 customers with Word, Excel, OneNote, or PowerPoint can view, create, and edit files on the go. they do not mention SPS, so only Office the web, you can create and save locally to your computer if you consider sharepoint as repository to save choose sharepoint option to

upvoted 1 times

exaja 1 year, 4 months ago

There was an identical question earlier (https://www.examtopics.com/discussions/microsoft/view/51069-exam-ms-100-topic-2-question 43-discussion/) but the difference here is that the license and question wording is about "Office for the web", whereas the other questi writes about "Office Online", but it is the same thing.
Surely, the answer should be the same as in the earlier question – Office for the web and SharePoint Online (Plan 2), because you need Office for the web (Office Online) to create documents and SharePoint to store them.

upvoted 6 times

HOTSPOT -

You have a data loss prevention (DLP) policy.

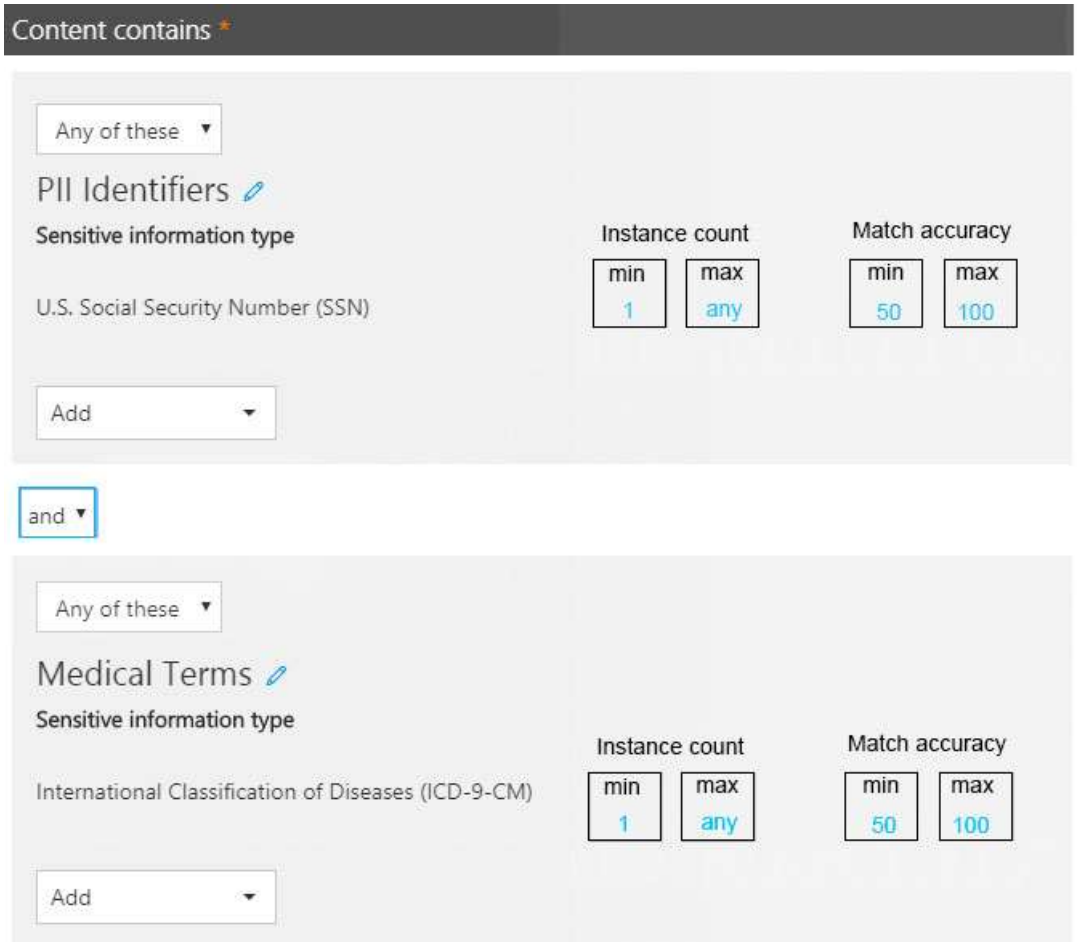
You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM).

The solution must minimize the number of false positives.

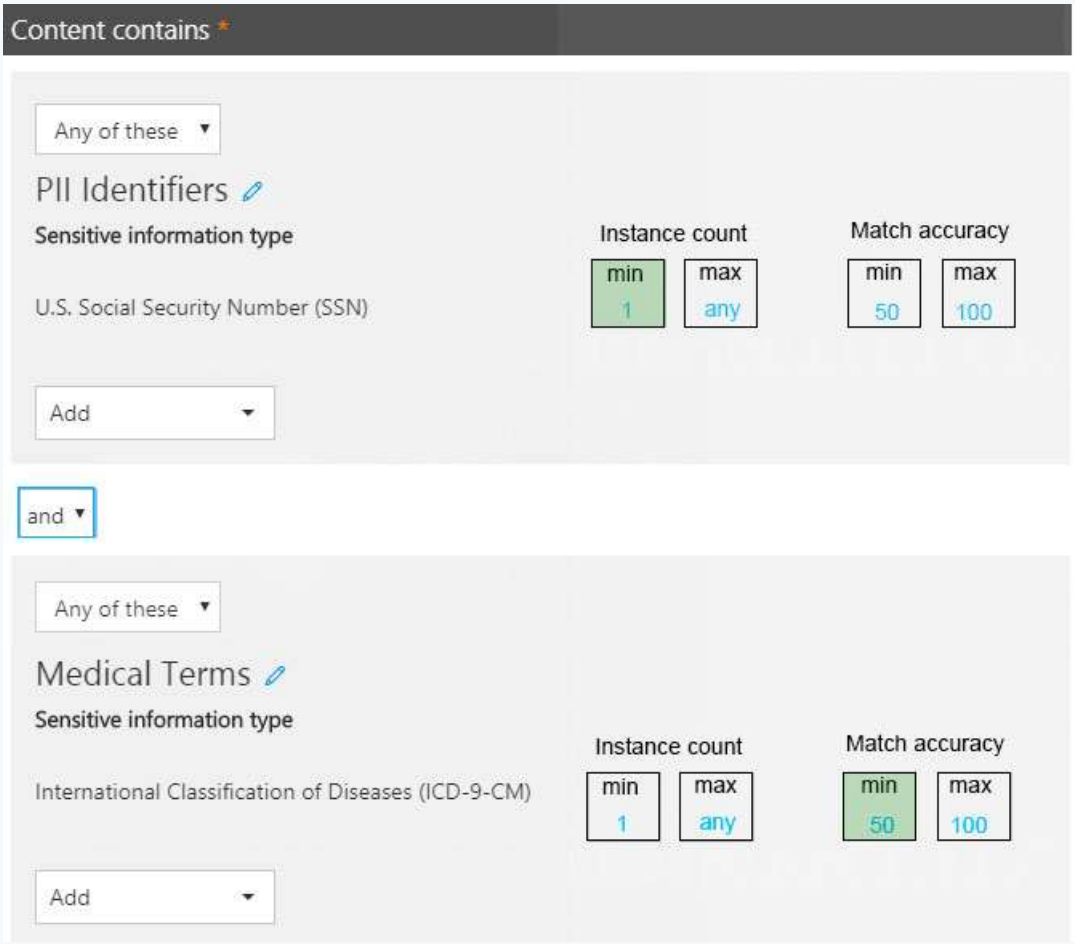
Which two settings should you modify? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



You can tune your rules by adjusting the instance count and match accuracy to make it harder or easier for content to match the rules. Each sensitive information type used in a rule has both an instance count and match accuracy.

To make the rule easier to match, decrease the min count and/or increase the max count. You can also set max to any by deleting the numerical value.

To minimize the number of false positives, we need to increase the minimum match accuracy.

A sensitive information type is defined and detected by using a combination of different types of evidence. Commonly, a sensitive information type is defined by multiple such combinations, called patterns. A pattern that requires less evidence has a lower match accuracy (or confidence level), while a pattern that requires more evidence has a higher match accuracy (or confidence level).

Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm

Aysan Highly Voted 1 year, 4 months ago

MS-101 question

upvoted 5 times

PurpleBreak Most Recent 3 months ago

I would change AND to OR in the policy definition so it would apply on ICD classifications even if didn't have a SSN in the document. Th would make it apply to more documents and then to reduce false positives I'd increase the accuracy.

upvoted 2 times

itmaster 5 months, 4 weeks ago

I would change only the "match accuracy" for both to increase it and avoid false positive. No need t change the "count", because if you increase the "count" the policy likehood to apply will reduce.
The question states that "You need to increase the likelihood that the DLP policy will apply".

upvoted 1 times

joergsi 8 months, 1 week ago

For me the first marking is wrong. We are asked to modify the settings of the International Classification of Diseases (ICD-9-CM) => Adjustment for the SSN is not needed at all!
Min. Instance count and Match accuracy of ICD-9-CM needs to be adjusted!

upvoted 4 times

FatsoGums 11 months, 1 week ago

MS-101 q

upvoted 1 times

jaolbreak 1 year, 4 months ago

Both the minimum instance count and the minimum match accuracy need to be changed on the Medical Terms. If the minimum match accuracy was set to 99%, and the instance count to 1, that means 1 in every 100 could be a false positive. However if the instance count increased to 5 matches, the number of false positives would drop exponentially.
Unless there is specific reference to medical terms in the PII policy changing this would have no impact on reducing the false positives the medical terms policy.

upvoted 4 times

hhaywood 1 year, 4 months ago

I understand the bottom option but why would the SSN min instance help?

upvoted 2 times

gsmith9897 1 year, 4 months ago

It seems both values should change on Medical Terms, increasing the instance count to compensate for lowering the match accurac
Increasing instance count on PII Identifiers might decrease false positives by deceasing the number of matches, but doesn't seem li the right way to go about it.

upvoted 2 times

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
You may now click next to proceed to the lab.

Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
Microsoft 365 Password: xxxxxxxxxx
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab Instance: 111111111 -
Your organization recently implemented a new data retention policy. The policy requires that all files stored in an employee's Microsoft OneDrive folders be retained for 60 days after the employee is terminated from the organization.
The human resources (HR) department of the organization deletes the user accounts of all terminated employees.
You need to ensure that the organization meets the requirements of the data retention policy.

Correct Answer: *See explanation below.*
You need to configure the OneDrive retention period for deleted users.
1. Go to the OneDrive admin center.
2. Select Storage.
3. Set the ג€Days to retain files in OneDrive after a user account is marked for deletionג€ option to 60.
4. Click Save to save the changes.
References:
https://docs.microsoft.com/bs-latn-ba/onedrive/set-retention

chepeerick 3 weeks, 4 days ago
Onedirve settings were moved to Sharepoint
upvoted 1 times

You have a Microsoft 365 subscription.
Your company purchases a new financial application named App1.
From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.
You need to prevent the missing information from affecting the score.
What should you configure from the Cloud Discover settings?

A. App tags

B. Score metrics

C. Organization details

D. Default behavior

Correct Answer: *B*
An app's score in Cloud Discovery is based on categories such as General, Security, Compliance and Legal. Each category has several parameters. For example, the domain registration and consumer popularity parameters are part of the General category. These parameters are known as Score Metrics.
You can modify the default weights given to the Cloud Discovery score configuration. By default, all the various parameters evaluated are given an equal weight. If there are certain parameters that are more or less important to your organization, you can adjust the weight of each score metric.
In this case, we need to lower the weight of the domain registration and consumer popularity score metrics.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/risk-score

MartinSt Highly Voted 2 years, 10 months ago
B - Score Metric
https://docs.microsoft.com/en-us/cloud-app-security/risk-score
upvoted 28 times

Jokke71 2 years, 7 months ago
Correct and even a more specific link is: https://docs.microsoft.com/en-us/cloud-app-security/risk-score#customizing-the-risk-score
upvoted 6 times

IllydeBilly 1 year, 8 months ago
https://docs.microsoft.com/en-us/cloud-app-security/media/score.png
upvoted 1 times

DArnett Most Recent 1 week, 1 day ago
on my exam on 9/27
upvoted 1 times

FatsoGums 11 months, 1 week ago
Ms-101 question . B
upvoted 1 times

Eggsamine 11 months, 2 weeks ago
MS-101?
upvoted 1 times

gsmith9897 1 year, 4 months ago
Anyone know where to find Cloud App Security? Supposedly you go to the Microsoft 365 admin center | Security | More Resources | Cloud App Security. I don't see More Resources anywhere in the Security & Compliance center. I assume Cloud App Security has a new name.
upvoted 1 times

McAlec 1 year, 4 months ago
portal.cloudappsecurity.com
but I assume that you have found it already

upvoted 1 times

atp007 1 year, 6 months ago

Score metrics is 100% correct

upvoted 1 times

estarisbourne 1 year, 8 months ago

if you don't want to read it Matt Soseman on Youtube "App Risk scoring in Microsoft Cloud App Security" explains why its score metric t
allows you to dive in and change the rating on each category of interest of the item selected.

upvoted 1 times

mkoprivnj 1 year, 9 months ago

B for sure!

upvoted 2 times

EllisonLuo 2 years, 4 months ago

B - Score Metric

upvoted 4 times

wyjung 2 years, 7 months ago

correct B or A?
What's correct answer?

upvoted 2 times

Thespy45 2 years, 6 months ago

If you look at the screenshot in the specific link posted by Jokke71, it's obviously Score Metrics, answer B.

upvoted 3 times

HOTSPOT -

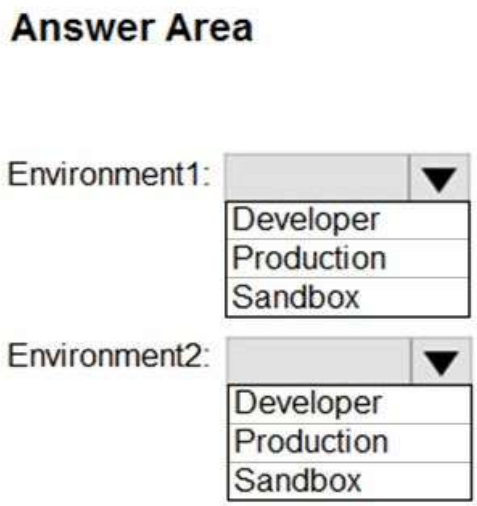
You plan to deploy two Microsoft Power Platform environments as shown in the following table.

Name	Requirement
Environment1	• Supports multiple makers that customize the environment • Supports copying other environments to Environment1 • Minimizes effort to reset the environment
Environment2	• Is a learning environment • Supports the creation of unlimited apps • Does not count against storage allocation for the tenant

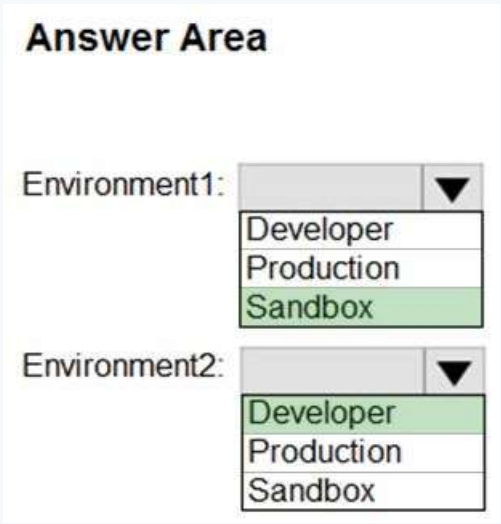
Which environment type should you use for each environment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/power-platform/admin/environments-overview

TimurKazan Highly Voted 1 year ago

sandbox & developer

upvoted 5 times

ChizzyO Most Recent 3 months ago

The provided answers are correct. You can only reset sandbox environment. Just to add this link that shows that the developer environment does not count against storage capacity. https://docs.microsoft.com/en-us/power-platform/admin/capacity-storage

upvoted 1 times

Ammoval 3 months, 2 weeks ago

provided answerer is correct
https://docs.microsoft.com/en-us/power-apps/maker/developer-plan

upvoted 1 times

Ash473 1 year, 1 month ago

in exam today

upvoted 4 times

densyo 1 year, 3 months ago

Answer1: "You can only copy an environment to a sandbox environment."

Answer2: With the developer environment, you can create unlimited apps for development and test purposes."

https://docs.microsoft.com/en-us/power-platform/admin/environments-overview#types-of-environments

upvoted 4 times

PandaTuga 1 year, 3 months ago

You can only reset sandbox environments. https://docs.microsoft.com/en-us/power-platform/admin/sandbox-environments#reset-a-sandbox-environment, https://docs.microsoft.com/en-us/power-platform/admin/reset-environment
"Sandbox These are non-production environments, which offer features like copy and reset"
https://docs.microsoft.com/en-us/power-platform/admin/environments-overview#types-of-environments

"Create and test apps Yes. You can create unlimited apps for development and test purposes"
https://docs.microsoft.com/en-us/powerapps/maker/developer-plan#which-features-are-included-in-the-power-apps-developer-plan

upvoted 2 times

Justin1 1 year, 3 months ago

Sandbox environments still count towards the database storage quota on your tenant so option 2 is developer

upvoted 1 times

itstudy369 1 year, 3 months ago

This should be Developer & Sandbox

upvoted 1 times

itstudy369 1 year, 3 months ago

Looks like the provided answers are correct. You can only reset sandbox environments. https://docs.microsoft.com/en-us/power-platform/admin/sandbox-environments

upvoted 2 times

Chiffa 1 year, 4 months ago

Shouldn't it be vice versa - Developer and Sandbox?

upvoted 4 times

True 1 year, 3 months ago

i feel it should be aswell , have you got any article proving it should be developer and Sandbox ???

upvoted 1 times

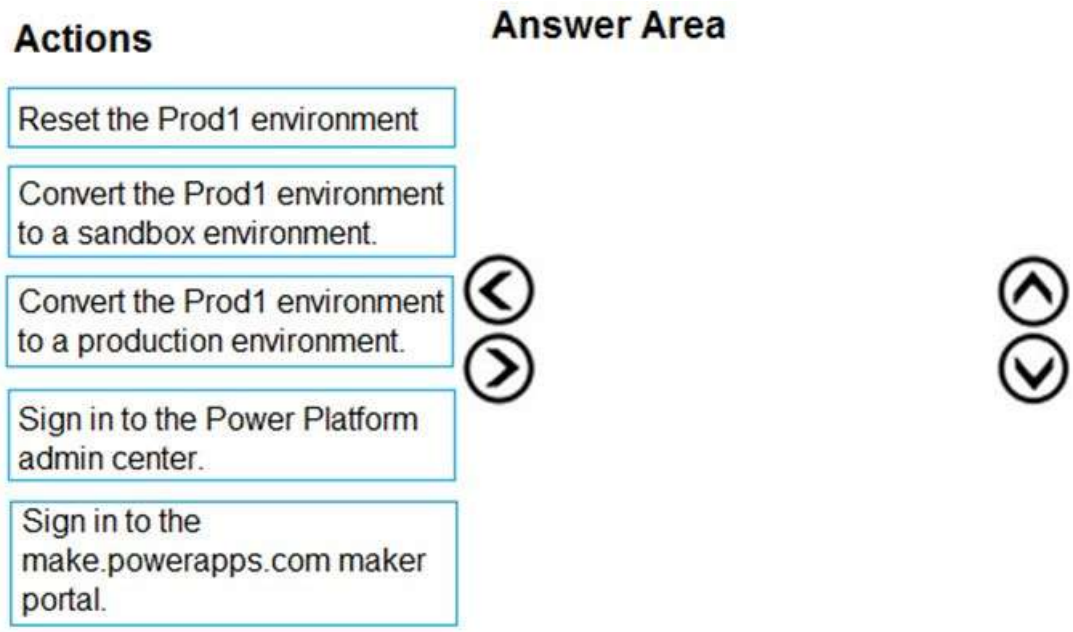
DRAG DROP -

You have a pilot app named App1 deployed to a Microsoft Power Platform production environment named Prod1.

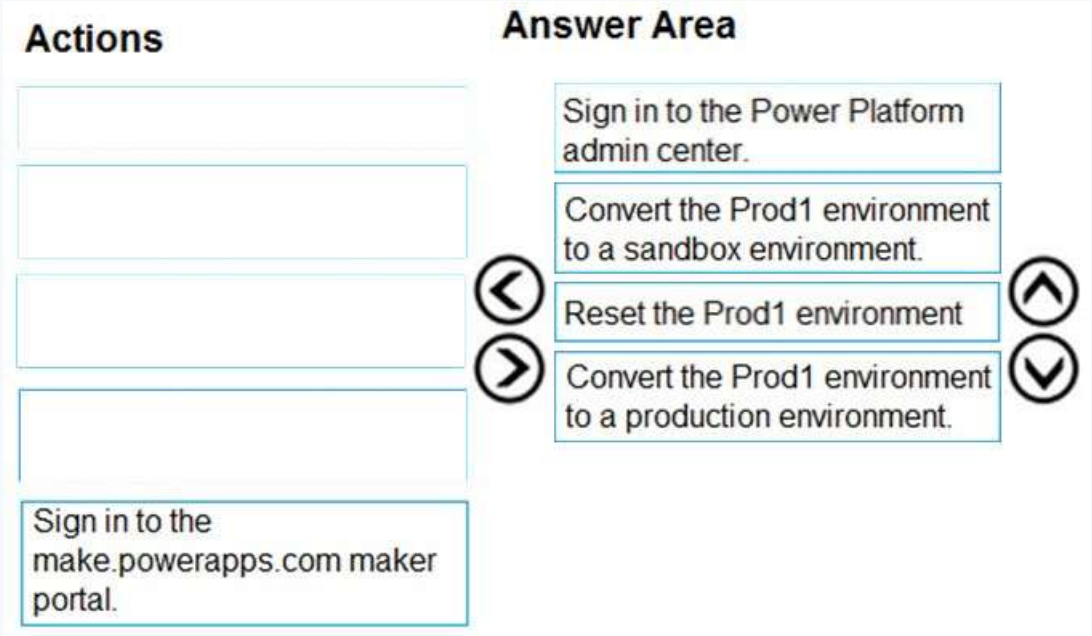
You need to reset the Prod1 environment in preparation for the production deployment of App1.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/power-platform/admin/switch-environment https://docs.microsoft.com/en-us/power-platform/admin/reset-environment

MomoLomo 1 year, 1 month ago

You can only reset sandbox environments.
https://docs.microsoft.com/en-us/power-platform/admin/reset-environment
https://www.azamba.com/2018/01/18/how-to-reset-a-production-instance-in-microsoft-dynamics-365-crm/
Makes sense

upvoted 4 times

Ash473 1 year, 1 month ago

in exam today

upvoted 3 times

Question #54 *Topic 5*

You have a Microsoft 365 tenant that contains a Microsoft Power Platform environment.
You need to ensure that only specific users can create new environments.
What should you do in the Power Platform admin center?

A. From Data policies, create a new data policy.

B. From Data integration, create a new connection set.

C. From Power Platform settings, modify the Governance settings for the environment.

D. From Environments, modify the behaviour settings for the default environment.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/power-platform/admin/control-environment-creation

densyo Highly Voted 1 year, 3 months ago
Answer C is correct
upvoted 5 times

Partylad Most Recent 1 month, 1 week ago
in Admin, cog top right, power platform settings
upvoted 1 times

itstudy369 1 year, 3 months ago
Correct
upvoted 3 times

HOTSPOT -

You have a Microsoft 365 tenant that contains 300 users.

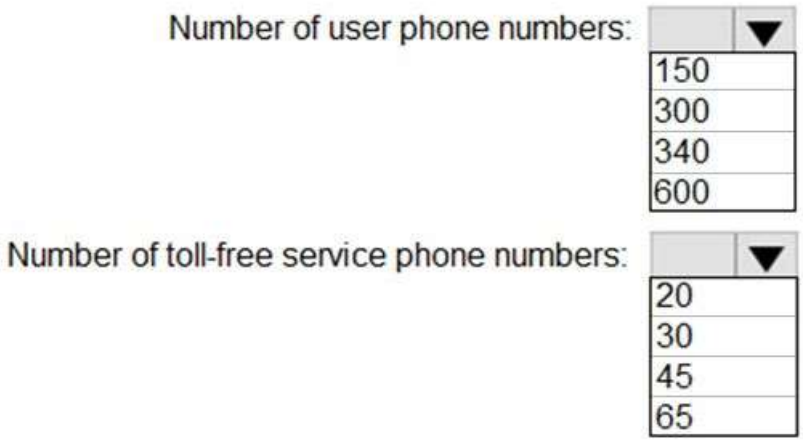
The users have Domestic and International Calling Plan licenses.

What is the maximum user phone numbers and toll-free service phone numbers can you acquire? To answer, select the appropriate options in the answer area.

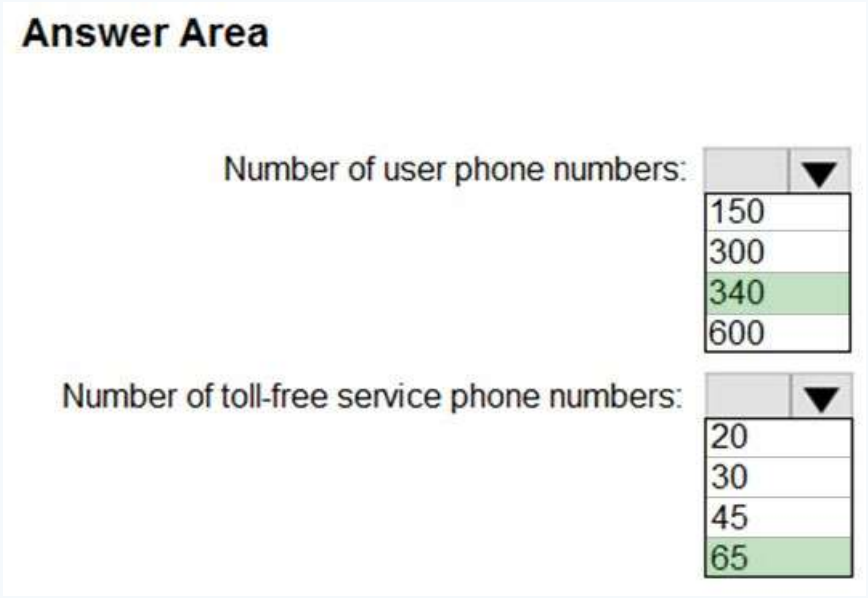
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/microsoftteams/how-many-phone-numbers-can-you-get

jkklim Highly Voted 9 months, 1 week ago

USER PHONE NUMBER = (300 USERS X 1.1) + 10 = 340

TOLL FREE = either you memorise the number or estimate that every 25 users = 5 numbers, so 300 users = 60 numbers (so i will select

upvoted 7 times

joergsi 8 months ago

So, with TOLL FREE = either you memorise the number or estimate that every 25 users = 5 numbers, so 300 users = 60 numbers (so will select 65)

you are saying, to cut it short, every 5 user 0 one number? 300/5 = 60

upvoted 1 times

Turak64 Highly Voted 1 year, 1 month ago

I've passed MS-700 and still didn't know this one. MS really need to bring better focus to their exams!

upvoted 6 times

Turak64 1 year, 1 month ago

These memory type questions also have no place in the exam. In a real world situation, you wouldn't be expected to remember the exact numbers. It's a 2 second Google search and doesn't prove if you have a good understanding of 365 or not

upvoted 21 times

Liradus 1 year ago

I totally agree xD

upvoted 3 times

Eggsamine 11 months, 2 weeks ago

I agree too. Limits can change all the time too, how are we meant to keep up to date with that?

upvoted 2 times

Koetjeboe Most Recent 6 months, 1 week ago

https://docs.microsoft.com/en-us/microsoftteams/how-many-phone-numbers-can-you-get

The number of phone numbers is equal to the total number of Domestic Calling Plan and/or Domestic and International Calling Plan licenses multiplied by 1.1 + 10 additional phone numbers.
Example: If I have 300 users in total with either a Domestic Calling Plan and/or Domestic and International Calling Plan, you can acquir 340 phone number (300 x 1.1 + 10).

The number of phone numbers is equal to the total number of Phone System and Audio Conferencing licenses and uses the following: there are 200-499 licenses then 65 telephone numbers are given.

upvoted 1 times

jjong 1 year ago

this qns came out in exam today

upvoted 3 times

Question #56 *Topic 5*

You have a Microsoft 365 tenant.

You install the Microsoft Power Platform Center of Excellence (CoE) starter kit.

What is required to populate data in the CoE solution?

A. Azure Logic Apps with the prefix Flow

B. Microsoft Power Automate flows with the prefix Sync

C. Azure Functions with the prefix Sync

D. Microsoft Power Automate flows with the prefix Nurture

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/power-platform/guidance/coe/setup

https://www.d365ug.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=0d516a28-db20-4cc9-ba14-3eee2855533f

Question #57 *Topic 5*

You have an on-premises call center and a Microsoft 365 E5 tenant.
You plan to implement Microsoft Phone System Direct Routing and Microsoft Teams.
What should you include in the solution?

A. a Session Border Controller (SBC)

B. a local number port order request

C. Skype for Business Cloud Connector Edition

D. Azure AD Connect

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoftteams/direct-routing-landing-page

Question #58 *Topic 5*

You have a Microsoft 365 E5 tenant.
You plan to create the Microsoft Power Platform environments shown in the following table.

Name	Type	Region	Database
Environment1	Sandbox	United States	No
Environment2	Production	Europe	Yes
Environment3	Production	United States	Yes
Environment4	Trial	Europe	Yes

What is the minimum amount of available database capacity required to create the environments?

A. 1 GB

B. 2 GB

C. 3 GB

D. 4 GB

E. 7 GB

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/power-platform/admin/create-environment#create-an-environment-without-a-database

You have a Microsoft 365 subscription.
From the Microsoft 365 portal, users download and install Microsoft Office apps on their devices.
You need to ensure that Office feature updates are installed by using the Semi-Annual Channel.
What should you configure from the Services page of the Microsoft 365 admin center?

A. Office Scripts

B. User owned apps and services

C. Office installation options

D. Office on the web

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels

Arlecchino 1 month ago

Selected Answer: C

C is the correct answer

upvoted 2 times

Question #60 *Topic 5*

You plan to deploy Microsoft Teams to 2,500 users.

You need to estimate the internet bandwidth required for the deployment.

What should you use?

A. Advisor for Teams

B. Network planner

C. Skype for Business Server Remote Connectivity Test

D. Microsoft Remote Connectivity Analyzer

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/microsoftteams/network-planner

Arlecchino 3 weeks, 2 days ago

In exam today

upvoted 3 times

PmgCosta 5 months, 1 week ago

Selected Answer: B

From: https://docs.microsoft.com/en-us/microsoftteams/network-planner

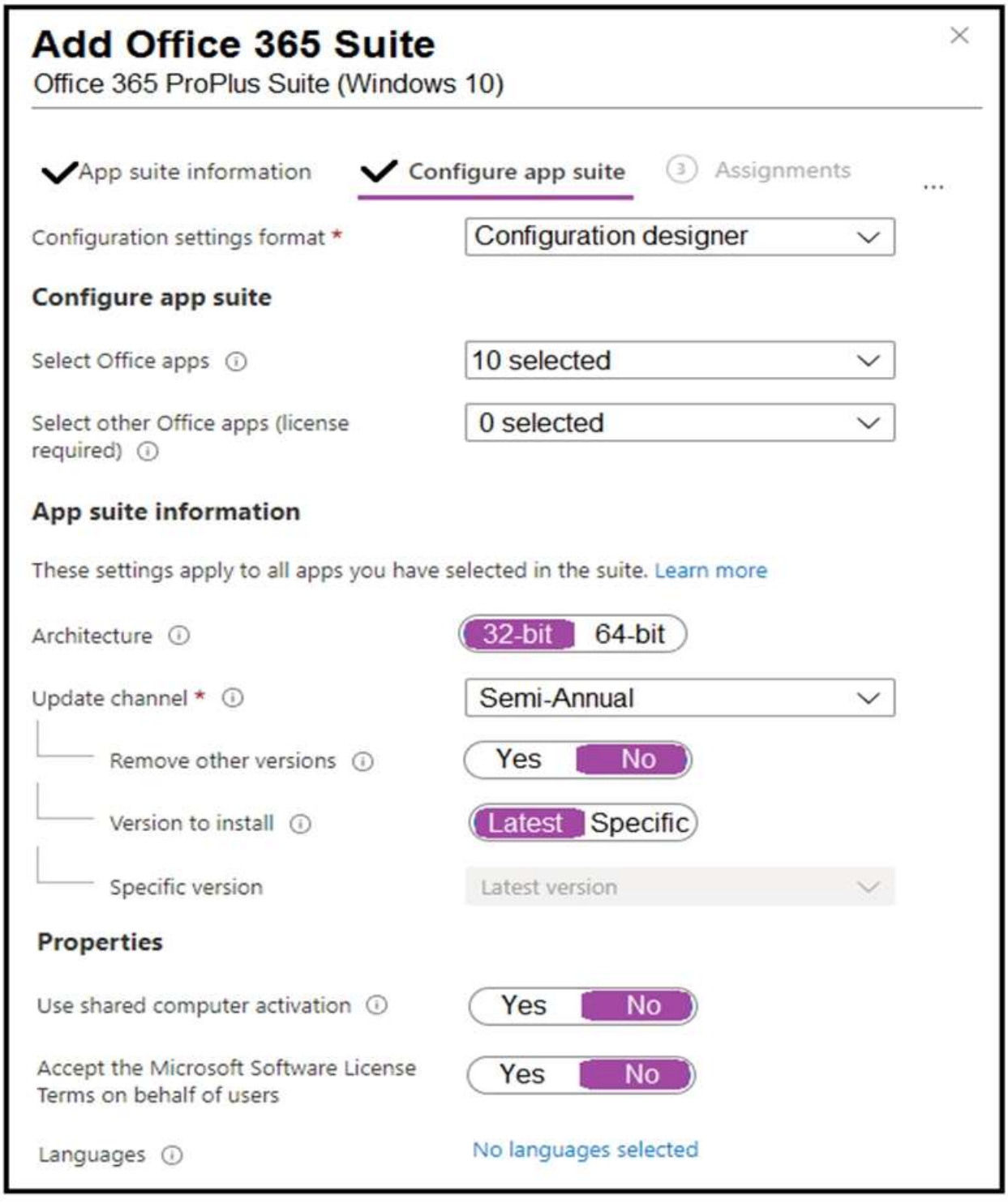
Network Planner is a new tool that is available in the Teams admin center. It can be found by going to Planning > Network planner. In j
a few steps, the Network Planner can help you determine and organize network requirements for connecting Microsoft Teams users
across your organization. When you provide your network details and Teams usage, the Network Planner calculates your network
requirements for deploying Teams and cloud voice across your organization's physical locations.

upvoted 1 times

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager as shown in the following exhibit.

Name	CPU	Member of	Installed apps
Device1	x86	Group1	Microsoft Office 2016
Device2	x86	Group1	**None**
Device3	x64	Group1	Microsoft Office 2019
Device4	x64	Group1	**None**

You create an Office 365 Suite app as shown in the exhibit. (Click the Exhibit tab.) and assign the app to Group1.



On which devices will Office 365 be installed?

A. Device1, Device2, and Device4 only

B. Device1, Device2, Device3, and Device4

C. Device2 and Device4 only

D. Device1 and Device2 only

E. Device2 only

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

chepeerick 2 weeks ago

Remove other versions: Choose Yes to remove other versions of Office (MSI) from user devices. Choose this option when you want to remove pre-existing Office .MSI apps from end-user devices. The installation won't succeed if there are pre-existing .MSI apps on end-u devices. The apps to be uninstalled are not limited to the apps selected for installation in Configure App Suite, as it will remove all Offic (MSI) apps from the end user device. For more information, see Remove existing MSI versions of Office when upgrading to Microsoft 3 Apps. When Intune reinstalls Office on your end user's machines, end users will automatically get the same language packs that they h with previous .MSI Office installations.

RemoveMSI can be used to uninstall 2007, 2010, 2013, or 2016 versions of Office, Visio, or Project that were installed using Windows Installer (MSI).

upvoted 1 times

itsme12p 2 weeks, 5 days ago

Selected Answer: C

is C because other devices already have office and is set to not uninstall other version

upvoted 4 times

Debadatta 3 weeks, 2 days ago

Correct: because, You can install the 32-bit version on both 32-bit and 64-bit devices, but you can install the 64-bit version on 64-bit dev only.
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

upvoted 4 times

Question #62 *Topic 5*

Your company has a single Microsoft 365 E5 subscription.

The company has five departments that each has a dedicated helpdesk operator.

You need to ensure that the helpdesk operators can manage only the users in their respective department.

What should you use?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

B. Custom role based access control (RBAC) roles

C. Administrative units in Azure Active Directory (Azure AD)

D. Privileged access management for Azure Active Directory (Azure AD)

Correct Answer: *B*

Debadatta 1 week, 6 days ago

Selected Answer: C

Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.
Source: https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units

upvoted 1 times

KrisDeb 2 weeks ago

Selected Answer: C

C: Administrative units

upvoted 1 times

simoen 2 weeks ago

Selected Answer: C

C is the correct one

upvoted 1 times

chepeerick 2 weeks ago

Selected Answer: C

https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

upvoted 2 times

KemalM 3 weeks ago

Selected Answer: C

This is what administrative units are for

upvoted 2 times

amitsharma170490 3 weeks, 3 days ago

Answer is C: Administrative units in Azure Active Directory (Azure AD)
Refer: https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

upvoted 1 times

Question #63 *Topic 5*

You have a Microsoft 365 E5 subscription that contains a group named Group1.
You need to ensure that all the members of Group1 are notified when Microsoft 365 outages occur. The solution must minimize administrative effort.
What should you do?

A. From the Microsoft 365 admin center, configure a Service health email notification.

B. From the Microsoft 365 admin center, configure a Message center email notification.

C. From the Microsoft 365 Defender portal, create an alert policy and configure an email notification.

D. From the Exchange admin center, create an alert policy and configure an email notification.

Correct Answer: *C*

KrisDeb 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide

upvoted 1 times

simoen 2 weeks ago

Selected Answer: A

answer: A

upvoted 3 times

ajiejeng 4 weeks ago

Selected Answer: A

answer: A

upvoted 4 times

yukiiw 4 weeks, 1 day ago

it is A
https://office365itpros.com/2019/11/26/email-notifications-when-office-365-services-break/

upvoted 3 times

ariperdis 1 month ago

How come the answer is not A
It's called “Service notifications in email”.
Go to the Microsoft 365 admin center and select “Service Health” or click here.
Select Preferences.
Enter the email address where the notifications need to go (Max of 2 addresses), select the notification issues and the services you war
be notified about.

upvoted 4 times

Question #64 *Topic 5*

You have a Microsoft 365 E5 subscription that uses Endpoint security.

You need to create a group and assign the Endpoint Security Manager role to the group.

Which type of group can you use?

A. security only

B. mail-enabled security, Microsoft 365, and security only

C. distribution, mail-enabled security, Microsoft 365, and security

D. Microsoft 365 only

E. mail-enabled security and security only

Correct Answer: *D*

dth 1 week ago

Selected Answer: B

It's definitely B

"To assign a role to a group, you must create a new security or Microsoft 365 group with the isAssignableToRole property set to true. In the Azure portal, you set the Azure AD roles can be assigned to the group option to Yes. Either way, you can then assign one or more Azure AD roles to the group in the same way as you assign roles to users."

upvoted 2 times

stealthster 2 weeks, 1 day ago

I would go with B
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-role-assignments-to-groups-work

upvoted 3 times

pozzetttt 2 weeks, 6 days ago

Selected Answer: E

E. guys, please test it before voting.

upvoted 1 times

dth 3 days, 23 hours ago

obviously you did not test it ... M365 groups can be used for RBAC as well es (mail-enabled) security groups, so answer B ist correct!

upvoted 1 times

KemalM 3 weeks ago

Selected Answer: E

Both mail-enabled security and security only works. Checked in the tenant

upvoted 1 times

dth 3 days, 23 hours ago

yes, but M365 groups as well!

upvoted 1 times

rajeshrengasamy 3 weeks, 1 day ago

Selected Answer: A

To assign a role to a group, you must create a new security or Microsoft 365 group with the isAssignableToRole property set to true. In the Azure portal, you set the Azure AD roles can be assigned to the group option to Yes.

https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept

upvoted 3 times

amitsharma170490 3 weeks, 3 days ago

Answer is A, Roles can be assigned to a Users(M365 AC) or Groups & Users(Azure AD)

upvoted 1 times

Frederik9190 1 month ago

It is A - just try it

upvoted 1 times

k9_bern_001 1 month ago

I think A is correct

upvoted 3 times

Question #65 *Topic 5*

You have a Microsoft 365 tenant that contains a Microsoft Power Platform production environment named Environment1.

Environment1 contains a database and a Microsoft Dynamics 365 app.

A system backup of Environment1 is performed on June 1.

How many days will the system backup of Environment1 be retained?

A. 5

B. 7

C. 14

D. 28

Correct Answer: *D*

yukiiw 4 weeks, 1 day ago

28 days

Backups of production environments with a database and Dynamics 365 applications deployed are retained for up to 28 days. In contra

backups of production environments that don't have Dynamics 365 applications deployed in them will be retained for 7 days.

upvoted 1 times

You have a Microsoft 365 E5 subscription that uses Microsoft Teams and SharePoint Online.
You create a team and a SharePoint Online site for a new project named Project1.
You need to manage access to the team and the site. The solution must meet the following requirements:
* Members of Project1 must be able to control who has access to the team and the site.
* Only users in the subscription must be able to request access to the team and the site.
* Access to the team and the site must be removed after 12 months.
* Access to the team and the site must be reviewed every month.
What should you create first?

A. a Conditional Access policy

B. a catalog

C. an access package

D. an access review

Correct Answer: *A*

pozzetttt 2 weeks, 6 days ago

Selected Answer: C

https://www.youtube.com/watch?v=zUKoLmel4uA&ab_channel=CloudManagement.Community

upvoted 2 times

rajeshrengasamy 3 weeks ago

Selected Answer: C

https://www.youtube.com/watch?v=zUKoLmel4uA&ab_channel=CloudManagement.Community

upvoted 1 times

KemalM 3 weeks ago

Selected Answer: C

It should be access package
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

upvoted 2 times

rajeshrengasamy 3 weeks, 1 day ago

Selected Answer: A

Conditional Access policy should be created first to meet the conditions mentioned. Access Review comes second.

upvoted 1 times

rajeshrengasamy 3 weeks ago

Ignore this. Correct Answer is Access package. more details https://www.youtube.com/watch?v=zUKoLmel4uA&ab_channel=CloudManagement.Community

upvoted 1 times

amitsharma170490 3 weeks, 3 days ago

Answer is D

upvoted 1 times

ajiejeng 4 weeks ago

Selected Answer: D

i think this is D

upvoted 2 times

Your on-premises network contains a Microsoft Exchange Server 2019 organization.
You purchase a Microsoft 365 E5 subscription.
You need to integrate the on-premises network and Exchange Online.
What should you do first?

A. Implement Azure AD Connect.

B. Add a connector in Exchange Online.

C. Run the Hybrid Configuration wizard.

D. Install an Azure Active Directory (Azure AD) Application Proxy connector.

Correct Answer: *A*

pozzetttt 2 weeks, 3 days ago

Selected Answer: A

https://learn.microsoft.com/en-us/exchange/hybrid-deployment-prerequisites

upvoted 1 times

rajeshrengasamy 3 weeks, 1 day ago

Selected Answer: A

Answer is correct Azure AD connect should be implemented first before running HCW.

upvoted 1 times

Restyle 4 weeks, 1 day ago

Selected Answer: C

Wouldnt it be C?

upvoted 1 times

yukiiw 4 weeks, 1 day ago

it is C
https://www.sherweb.com/blog/office-365/integrate-office-365-onpremises/

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

* Identify when a user's credentials are compromised and shared on the dark web.

* Provide users that have compromised credentials with the ability to self-remediate.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To identify when users have compromised credentials, configure:

- A registration policy
- A sign-in risk policy
- A user risk policy
- Multi-factor authentication (MFA)

To enable self-remediation, select:

- Generate a temporary password
- Require multi-factor authentication
- Require password change

Correct Answer:

Answer Area

To identify when users have compromised credentials, configure:

- A registration policy
- A sign-in risk policy
- A user risk policy
- **Multi-factor authentication (MFA)**

To enable self-remediation, select:

- Generate a temporary password
- Require multi-factor authentication
- **Require password change**

amitsharma170490 3 weeks, 3 days ago

Answer is: User Risk & Change Password

upvoted 2 times

ajiejeng 4 weeks ago

Answer: User Risk & Change Password

upvoted 2 times

JackeD 1 month ago

why pay for this when Microsoft gives you all the answers
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies
user risk and pass change

upvoted 3 times

HOTSPOT -

You have a hybrid Microsoft Exchange Online deployment that contains the users shown in the following table.

Name	Email address	Forwarding address	Location
User1	User1@contoso.com	User6@contoso.com	On-premises
User2	User2@contoso.com	*None*	On-premises
User3	User3@contoso.com	*None*	On-premises
User4	User4@contoso.com	*None*	On-premises
User5	User5@contoso.com	*None*	On-premises
User6	User6@contoso.com	*None*	On-premises

Mailbox permissions are assigned as shown in the following table.

Mailbox	Permission
User2	Send As granted to User4
User4	Full Access granted to User3
User6	Send on Behalf granted to User5

You plan to migrate the mailboxes to Exchange Online by using remote mailbox move requests. The mailboxes will be migrated in batches as shown in the following table.

Batch	Included mailbox
1	User1, User2, User3, User6
2	User4, User5

A cutover migration will be performed for each batch of mailboxes.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The Email forwarding settings for User1 will be preserved after the migration.	○	○
The permissions granted to User4 for the User2 mailbox will be preserved after the migration.	○	○
The permissions granted to User3 for the User4 mailbox will be preserved after the migration.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The Email forwarding settings for User1 will be preserved after the migration.	○	○
The permissions granted to User4 for the User2 mailbox will be preserved after the migration.	○	○
The permissions granted to User3 for the User4 mailbox will be preserved after the migration.	○	○

rajeshrengasamy 3 weeks ago

Full access, Send on Behalf of supported in Hybrid Environments. Send As not supported. So YNY

upvoted 4 times

KemalM 3 weeks ago

Yes & No & Yes
(https://docs.microsoft.com/en-us/exchange/permissions#mailbox-permissions-in-hybrid-environments)

upvoted 2 times

HOTSPOT -

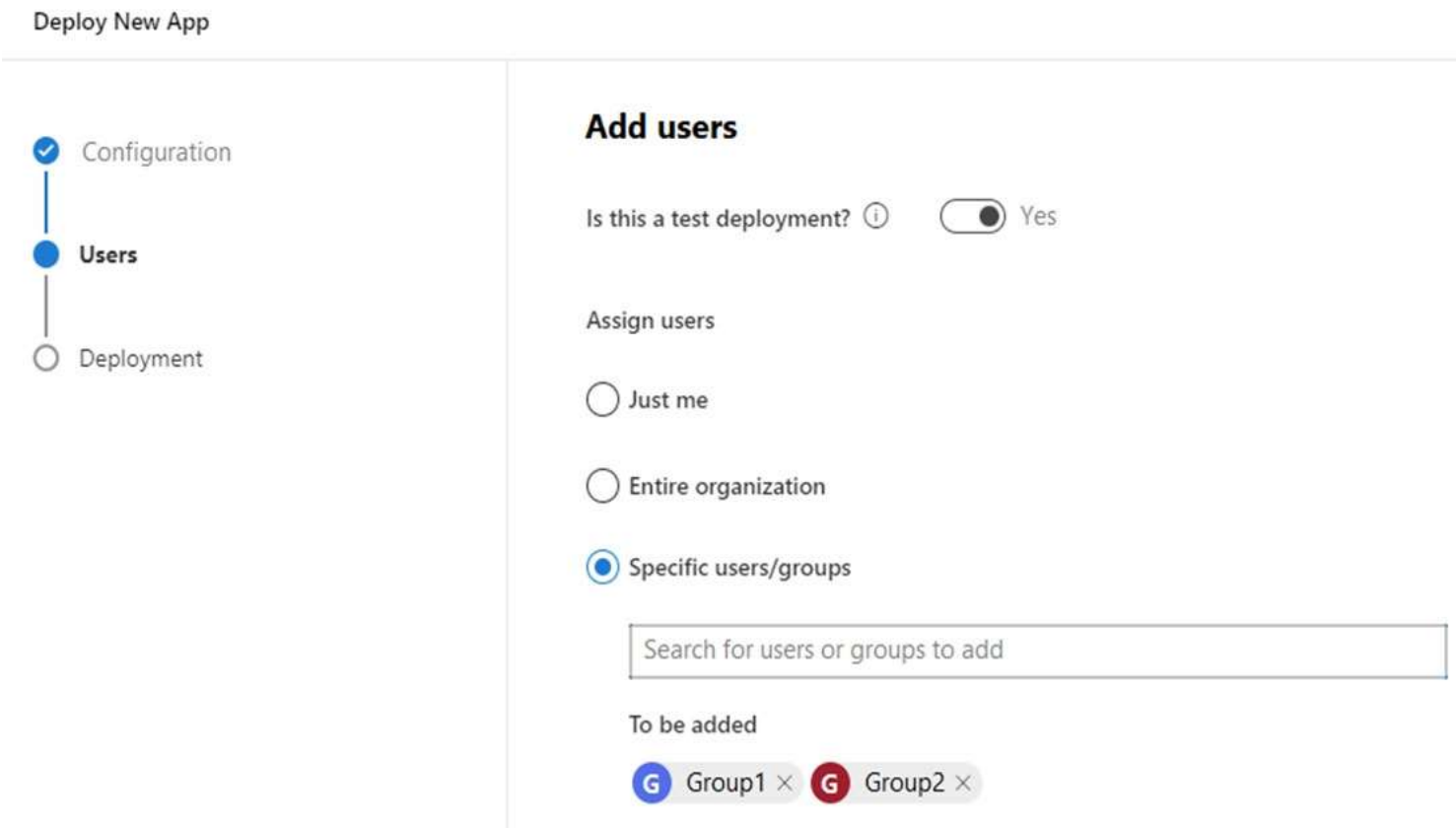
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Helpdesk admin
User2	Global Administrator
User3	*None*
User4	*None*
User5	*None*

The subscription contains the groups shown in the following table.

Name	Type	Members
Group 1	Microsoft 365	User2, User3
Group 2	Mail-enabled security	User1, Group3
Group 3	Distribution list	User4, User5

You deploy an app as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can modify the app deployment.	○	○
User2 will receive the app.	○	○
User4 will receive the app.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can modify the app deployment.	○	○
User2 will receive the app.	○	○
User4 will receive the app.	○	○

xyz213 2 weeks, 1 day ago

N/Y/N Helpdesk can not change the app deployment

upvoted 2 times

yukiiw 4 weeks, 1 day ago

user 1 cannot modify the app deployment

helpdesk admin role :
Assign the Helpdesk admin role to users who need to do the following:
- Reset passwords
- Force users to sign out
- Manage service requests
- Monitor service health

upvoted 4 times

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft 365 usage analytics reports in Microsoft Power BI.

You need to ensure that the Microsoft 365 usage analytics template app can access Microsoft 365 usage data.

Which Authentication method should you select for Power BI?

A. Anonymous

B. OAuth2

C. Key

D. Basic

Correct Answer: *A*

k9_bern_001 Highly Voted 1 month ago

B is the correct answer
https://docs.microsoft.com/en-us/microsoft-365/admin/usage-analytics/enable-usage-analytics?view=o365-worldwide

upvoted 7 times

mh1143 Highly Voted 1 month ago

Should be oauth2
https://docs.microsoft.com/en-us/microsoft-365/admin/usage-analytics/enable-usage-analytics?view=o365-worldwide

upvoted 6 times

ajiejeng Most Recent 4 weeks ago

Selected Answer: B

answer B

upvoted 3 times

Question #72 *Topic 5*

Your on-premises network contains an Active Directory domain that syncs with an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure
AD Connect.
Your company purchases another company that has an on-premises Active Directory domain named litwareinc.com.
You need to sync litwareinc.com with contoso.com.
What should you install in the litwareinc.com domain?

A. an Azure AD application proxy connector

B. an Azure AD Connect instance in staging mode

C. an Azure AD Connect provisioning agent

D. an active instance of Azure AD Connect

Correct Answer: *D*

xyz213 2 weeks, 2 days ago
This makes no sense to me.
If you want to sync a second on-prem AD Domain you need to establish a trust and then modify the existing Azure AD Connect Settings include the second on-prem AD Domain.

you can only have one AD Connect instance per tenant.
https://www.smikar.com/second-domain-using-ad-connect/
upvoted 1 times

dth 6 days, 11 hours ago
Since you cannot add a second AAD-Connect Instance, you have to use AAD Cloud Sync in this scenario - therefore Option C (provisioning agent) is correct
upvoted 1 times

xyz213 2 weeks, 2 days ago
I think C is correct because the Forests/Domains are not connected:
https://learn.microsoft.com/en-us/azure/active-directory/cloud-sync/what-is-cloud-sync
upvoted 2 times

yukiiw 4 weeks, 1 day ago
D is correct
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis
upvoted 1 times

Question #73 *Topic 5*

You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?

A. Windows Hello

B. Microsoft Authenticator app

C. FIDO2 compliant security keys

Correct Answer: *B*

ajiejeng 4 weeks ago

Selected Answer: B

Correct : B

upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory domain. The domain contains a server named Server1. Server1 has a share named Share1 that contains the files shown in the following table.

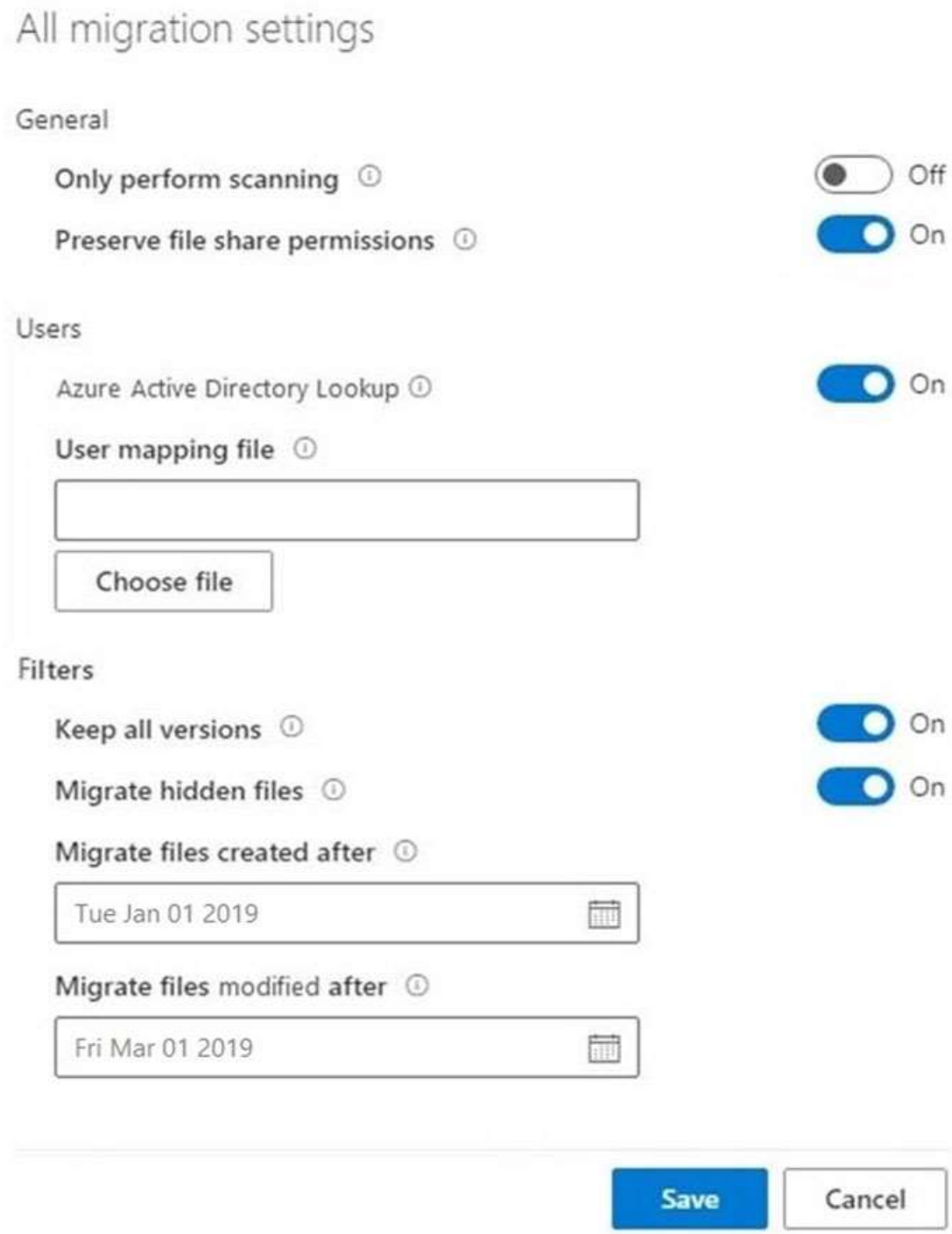
Name	Created	Modified	Permission
File1.txt	12/15/2018	03/15/2019	Domain Users: Allow Read
File2.txt	01/15/2019	03/15/2019	User1: Allow Read
File3.txt	03/05/2019	03/15/2019	Domain Users: Allow Read User1: Deny Read

You have a hybrid deployment of Microsoft 365.

You create a Microsoft SharePoint site collection named Collection1.

You plan to migrate Share1 to a document library in Collection1.

You configure the SharePoint Migration Tool as shown in the exhibit. (Click the Exhibit tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
File1.txt will be migrated to SharePoint.	○	○
File2.txt will be migrated to SharePoint.	○	○
User1 will be denied access to read File3.txt in SharePoint when the migration is complete.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
File1.txt will be migrated to SharePoint.	○	○
File2.txt will be migrated to SharePoint.	○	○
User1 will be denied access to read File3.txt in SharePoint when the migration is complete.	○	○

rajeshrengasamy 2 weeks, 2 days ago

Answer :

NO - File Creation date before Jan 01, 2019. Both the Created after and Modified after conditions should be met. (& logic)

Yes, - Meets both the conditions

No - Special permissions such as DENY are NOT preserved when migrating

upvoted 2 times

renrenren 3 weeks ago

3: No, because there is no user mapping file, the permission will be set to the default permission of the location to which it has been migrated in SPO, am I correct?

upvoted 1 times

rajeshrengasamy 3 weeks ago

Answer :

NO - File Creation date before Jan 01, 2019. Both the Created after and Modified after conditions should be met. (& logic)

Yes, - Meets both the conditions

Yes - Access will be denied as share permissions are preserved.

upvoted 1 times

GodlessCreature 2 weeks, 3 days ago

Special permissions such as DENY are NOT preserved when migrating.

LINK: https://learn.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating
upvoted 1 times

rajeshrengasamy 2 weeks, 2 days ago
Yes, you are correct.
upvoted 1 times

Topic 6 - Testlet 1

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq "Finance")

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
You need to add the custom domain names to Office 365 to support the planned changes as quickly as possible.
What should you create to verify the domain names successfully?

A. three alias (CNAME) records

B. one text (TXT) record

C. one alias (CNAME) record

D. three text (TXT) records

Correct Answer: *D*
Contoso plans to provide email addresses for all the users in the following domains:
- East.adatum.com
- Contoso.adatum.com
- Humongousinsurance.com

To verify three domain names, you need to add three TXT records.
Reference:
https://docs.microsoft.com/en-us/office365/admin/setup/add-domain?view=o365-worldwide

Zardu Highly Voted 11 months, 2 weeks ago
Answer is B See this resource: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-manage
upvoted 13 times

LillyLiver 8 months, 1 week ago
Yes, thank you. I thought the same thing then started questioning myself given the answer here.
upvoted 1 times

ariperdis Most Recent 1 month ago
As the response to the answer is correct and assumes B the correct answer is still D.
The domain is verified due to the parent domain but you are still required to register 3 txt records.
upvoted 1 times

ariperdis 1 month ago
As the question suggests the answer is D. The domain is verified is correct but you are still required to add the TXT records for the subdomains with your provider.
upvoted 1 times

bedny22 7 months, 3 weeks ago
Selected Answer: B
Adatum.com is already verified so you dont need to verify 2 subdomains of Adatum domain... you need to verify only Humongous... domain. So I would go with B.
upvoted 4 times

joergsi 8 months, 1 week ago

Selected Answer: B

Didn't get it at the first reading:

=> The network contains an Active Directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant name
contoso.onmicrosoft.com.
You recently configured the forest to sync to the Azure AD tenant.

=> In other words, contoso.com is already been set up!

-=Planned Changes=-
Contoso plans to provide email addresses for all the users in the following domains:
East.adatum.com
Contoso.adatum.com
Humongousinsurance.com

=> contoso.com is already been set up, no changes are needed for the subdomains!

=> Humongousinsurance.com needs a TXT-Record => (B)

upvoted 2 times

joergsi 8 months ago

OK, need to correct me after reading this a third-time, contoso is not adatum!

upvoted 1 times

STPC 7 months, 3 weeks ago

Keep on reading joergsi ;-)
"You recently configured the forest to sync to the Azure AD tenant." So contoso.com is setup.
"You add and then verify adatum.com as an additional domain name." This means adatum.com is also setup. So the subdomains
adatum.com don't need a TXT record.
humongousinsurrance.com is new and needs a TXT record => answer B

upvoted 1 times

AlexLiourtas 8 months, 1 week ago

Selected Answer: B

B one txt record, the subdomains are been verified from the top level domain

upvoted 1 times

Rickert 1 year, 1 month ago

It is B: https://stackoverflow.com/questions/38555474/do-i-need-to-register-a-domain-name-for-my-subdomain

upvoted 4 times

MessageMeThis 1 year, 1 month ago

The answer is B. From the domain FAQ question "Can I add custom subdomains or multiple domains to Microsoft 365?":
"When you add a subdomain, it is automatically verified based on the parent domain that is being verified."
https://docs.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide

upvoted 4 times

stromnessian 1 year, 2 months ago

The supplied answer is wrong. Adatum.com has already been verified and so subdomains can be added without additional verification
The correct answer is B.

upvoted 4 times

miul84 1 year, 3 months ago

based on the text:
- Adatum.com is already verified
- Humongousinsurance.com is not verified

I just tested and you can add sub-domains from exisiting Domains in Azure AD -> Custom domain names without any additional effort
they apear verified (here) right away. You can also create users with the subdomain.

However, under Settings -> Domains the subdomain apears as incomplete and to need to add a TXT record for that to become healthy.

upvoted 1 times

denmar 1 year, 2 months ago

but in the question, it isn't asked if there are healthy, so like PDB999 wrote "B" is right or ?

upvoted 1 times

michszym 1 year, 2 months ago

If you skip adding dns records you will have "no service selected". So subdomain is verified without txt record. Next you have to add
MX, CNAME and TXT for SPF in order to assign services like mail - then your subdomain status will be "healtly" (but these records are

services to running correctly, not for verifying :)
so just 1 txt record for verifying new domain is needed

upvoted 1 times

PDB999 1 year, 3 months ago

Would it not be 'B': One TXT record?
East.adatum.com - this is a subdomain of adatum.com that would already be verified
Contoso.adatum.com - this is a subdomain of adatum.com that would already be verified
Humongousinsurance.com - this is a new domain that would need verifying via a TXT record

upvoted 4 times

larnyx 1 year, 3 months ago

Correct, D.

You can use a TXT record to verify your domain. Select this and select Next to see instructions for how to add this DNS record to your registrar's website. This can take up to 30 minutes to verify after you've added the record.

upvoted 3 times

Topic 7 - Testlet 10

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.
▪

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
HOTSPOT -
You need to meet the application requirements for the Microsoft 365 Apps for enterprise applications.
You create an XML file that contains the following settings.

```
<Add SourcePath="\\Server1\OfficeSoftware"
     OfficeClientEdition="32"
     Channel="Targeted"
     AllowCdnFallback="True">
  <Product ID="O365ProPlusRetail">
     <Language ID="MatchOS" Fallback="en-us" />
  </Product>
</Add>
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

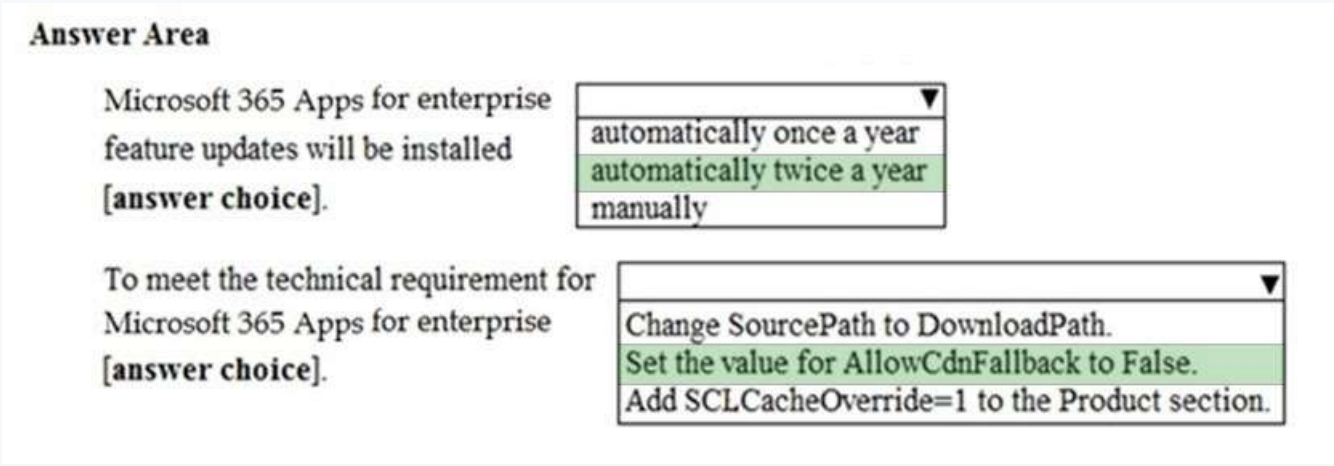
Microsoft 365 Apps for enterprise feature updates will be installed **[answer choice]**.

- automatically once a year
- automatically twice a year
- manually

To meet the technical requirement for Microsoft 365 Apps for enterprise **[answer choice]**.

- Change SourcePath to DownloadPath.
- Set the value for AllowCdnFallback to False.
- Add SCLCacheOverride=1 to the Product section.

Correct Answer:



Box 1:

Microsoft 365 Apps for enterprise feature updates will be installed twice a year in March and September.

The Channel element in the configuration file is set to 'Targeted'. This means Semi-Annual Targeted.

To help your organization prepare for a Semi-Annual Channel release, Microsoft provides Semi-Annual Channel (Targeted). The primary purpose of this update channel is to give pilot users and application compatibility testers in your organization a chance to work with the upcoming Semi-Annual Channel release

Box 2:

⇨ Microsoft 365 Apps for enterprise applications must be installed from a network share only.

The AllowCDNFallback value is currently set to true. The purpose of this setting is to enable Office 365 to be downloaded from Microsoft's Content Delivery

Network if the network share is unavailable. The AllowCDNFallback value should be set to false to meet the technical requirement.

Reference:

https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool#updates-element

https://docs.microsoft.com/en-us/deployoffice/overview-of-update-channels-for-office-365-proplus

Moderator 2 months, 1 week ago

Correct answers given. Setting the AllowCdnFallback toFalse makes sure the (language) files/packages won't be downloaded over the Office Content Delivery Network (CDN).

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.
▪

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
Which migration solution should you recommend for Project1?

A. From Exchange Online PowerShell, run the New-MailboxImportRequest cmdlet.

B. From Exchange Online PowerShell, run the New-MailboxExportRequest cmdlet.

C. From Exchange admin center, start the migration and select Remote move migration.

D. From the Exchange admin center, start the migration and select Cutover migration.

Correct Answer: *C*
⇨ Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
⇨ Fabrikam does NOT plan to implement identity federation.
⇨ All users must be able to exchange email messages successfully during Project1 by using their current email address.
During Project1, some users will have mailboxes in Microsoft 365 and some users will have mailboxes in Exchange on-premises. To enable users to be able to exchange email messages successfully during Project1 by using their current email address, we'll need to configure hybrid Exchange.
To migrate mailboxes in a hybrid Exchange configuration, you use the Exchange admin center to perform Remote move migrations.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
⇨ From Exchange admin center, start the migration and select Remote move migration.
From the Microsoft 365 admin center, start a data migration and click Exchange as the data service.
▪
Other incorrect answer options you may see on the exam include the following:
⇨ From the Exchange admin center, start a migration and select Staged migration.
⇨ From the Microsoft 365 admin center, start a data migration and click Upload PST as the data service.
⇨ From the Microsoft 365 admin center, start a data migration and click Outlook as the data service.
⇨ From the Exchange admin center, start a migration and select Cutover migration.
Reference:
https://docs.microsoft.com/en-us/exchange/hybrid-deployment/move-mailboxes

itmaster 5 months, 4 weeks ago

Selected Answer: C
Anser C is correct.
This is a hybrid setup senario where sales department will be moved to exchange online and ohter departments will stay on-prem. For Hybrid setup, the correct answer is "remove move migration". Reference:
https://docs.microsoft.com/en-us/previous-versions/exchange-server/exchange-150/jj945412(v=exchg.150)?

redirectedfrom=MSDN#:~:text=A%20remote%20move%20migration%20is%20used%20to%20migrate%20on%2Dpremises%20Exchang
20mailboxes%20to%20Exchange%20Online%20in%20an%20Exchange%20hybrid%20deployment.%20You%20must%20have%20an%20
hange%20hybrid%20deployment%20to%20use%20a%20remote%20move%20migration

upvoted 3 times

trexar 6 months ago

Selected Answer: D

A. From Exchange Online PowerShell, run the New-MailboxImportRequest cmdlet.
NO.This cmdlet is available only in on-premises Exchange. (THE SAME QUESTION)
B. From Exchange Online PowerShell, run the New-MailboxExportRequest cmdlet.
NO.This cmdlet is available only in on-premises Exchange. (THE SAME QUESTION)

C. From Exchange admin center, start the migration and select Remote move migration.
NO.The Mailbox Replication Service (MRS) has a proxy endpoint that's required for cross-forest mailbox moves and remote move migrations between your on-premises
D. From the Exchange admin center, start the migration and select Cutover migration.

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.
▪

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
Which migration solution should you recommend for Project1?

A. From the Microsoft 365 admin center, start a data migration and click Exchange as the data service.

B. From the Exchange admin center, start a migration and select Cutover migration.

C. From the Exchange admin center, start a migration and select Staged migration.

D. From the Microsoft 365 admin center, start a data migration and click Upload PST as the data service.

Correct Answer: *A*
⇨ Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
⇨ Fabrikam does NOT plan to implement identity federation.
⇨ All users must be able to exchange email messages successfully during Project1 by using their current email address.
During Project1, some users will have mailboxes in Microsoft 365 and some users will have mailboxes in Exchange on-premises. To enable users to be able to exchange email messages successfully during Project1 by using their current email address, we'll need to configure hybrid Exchange.
A new way to migrate mailboxes in a hybrid Exchange configuration is to use the Microsoft 365 data migration service. The data migration service can migrate
Exchange, SharePoint and OneDrive. Therefore, we need to start a data migration and click Exchange as the service to be migrated.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
⇨ From Exchange admin center, start the migration and select Remote move migration.
⇨ From the Microsoft 365 admin center, start a data migration and click Exchange as the data service.
Other incorrect answer options you may see on the exam include the following:
⇨ From Exchange Online PowerShell, run the New-MailboxImportRequest cmdlet.
⇨ From Exchange Online PowerShell, run the New-MailboxExportRequest cmdlet
⇨ From the Microsoft 365 admin center, start a data migration and click Outlook as the data service.
⇨ From the Exchange admin center, start a migration and select Cutover migration.
Reference:
https://docs.microsoft.com/en-us/fasttrack/O365-data-migration https://docs.microsoft.com/en-us/exchange/hybrid-deployment/move-mailboxes

rajeshrengasamy 3 weeks ago
Selected Answer: A

Exchange as Data Service is the correct answer as the On-premises Exchange is exchange 2016.
https://www.nucleustechnologies.com/blog/exchange-server-2016-hybrid-migration-to-office-365/
upvoted 1 times

rajeshrengasamy 3 weeks ago

Selected Answer: D

Export and import PST is the correct solution in this scenario.
upvoted 1 times

rajeshrengasamy 3 weeks ago

Sorry, Exchange as Data Service is the correct answer as the On-premises Exchange is exchange 2016
upvoted 1 times

Rsm2906 5 months, 1 week ago

I dont think cutover will sove the problem. Becouse we are only migrateing 1 Department and the otherones nees to stay onprem
upvoted 1 times

trexar 6 months ago

Selected Answer: B

A. From the Microsoft 365 admin center, start a data migration and click Exchange as the data service.
Yes, then apply option B
B. From the Exchange admin center, start a migration and select Cutover migration.
Yes, Choosing a cutover migration is suggested when: Your current on-premises Exchange organization is Microsoft Exchange Server 2
or later. Your on-premises Exchange organization has fewer than 2,000 mailboxes
C. From the Exchange admin center, start a migration and select Staged migration.
No,A staged migration is recommended when: Your source email system is Microsoft Exchange Server 2003 or Microsoft Exchange Ser
2007, or you have more than 2,000 mailboxes
D. From the Microsoft 365 ad
upvoted 2 times

Davidchercm 9 months, 1 week ago

In the EAC, go to Office 365 > Recipients > Migration.

Click Add Add Icon., and then select Migrate to Exchange Online.

On the Select a migration type page, select Remote move migration and then click Next.

On the Select the users page, click Add Add Icon. and select the on-premises users to move to Microsoft 365 or Office 365 and click Add
and then click OK. Click Next.
upvoted 2 times

Davidchercm 9 months, 1 week ago

https://docs.microsoft.com/en-us/exchange/hybrid-deployment/move-mailboxes
upvoted 1 times

Cybersecgirl 1 year, 2 months ago

BTW when you go to M365 and Set up and migration there is an option to select exchange as a data service
upvoted 1 times

miul84 1 year, 3 months ago

So Remote Move ist the way to go but I dont find this:
From the Microsoft 365 admin center, start a data migration and click Exchange as the data service.
upvoted 1 times

adaniel89 1 year, 3 months ago

From the Microsoft 365 admin center, start a data migration and click Exchange as the data service - This doesnt exists!

Microsoft 365 Admin Centre > Setup > Migrations > Email> Get Started > Import my PST files - this should be the Answer
upvoted 2 times

phvogel 1 year, 6 months ago

I misread the question: It's not selecting the Cutover answer but Remote Move (as indicated by picking a migration source -- that's part
a remote move because you have to indicate whether you're going from cloud to on-prem or on-prem to cloud). That's a good choice a
you can select the users to migrate using a remote move. Staged migration is only available on 2007 and 2010. My bad.
upvoted 2 times

phvogel 1 year, 6 months ago

The discussion in the "Show Solution" is great but the provided answer (Cutover) is wrong. You should use Cutover only when moving a
the mailboxes (up to 2000 but 150 is the recommended target): https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutove
migration-to-office-365.
If you're moving some (not all) of your mailboxes, which is what this question asks, you want to do a staged migration by providing a lis

users to migrate in a CSV file: https://docs.microsoft.com/en-us/exchange/mailbox-migration/perform-a-staged-migration/perform-a-staged-migration

upvoted 3 times

adaniel89 1 year, 3 months ago

Staged Migration is only application for Windows Server 2003 and 2007 https://docs.microsoft.com/en-us/exchange/mailbox-migration/what-to-know-about-a-staged-migration#:~:text=As%20part%20of%20a%20Microsoft,it's%20called%20a%20staged%20migration.&text=Consider%20using%20a%20cutover%20migration%20or%20a%20hybrid%20email%20migration%20instead.

Answer A doesnt make sense as the solution doesnt exist, so it has to be D!

upvoted 2 times

Topic 8 - Testlet 11

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

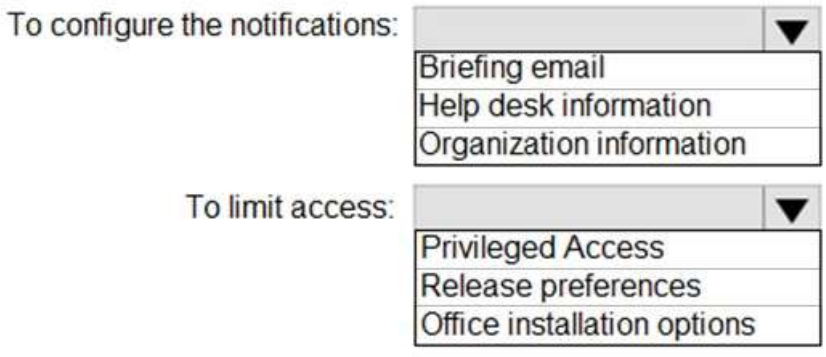
Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

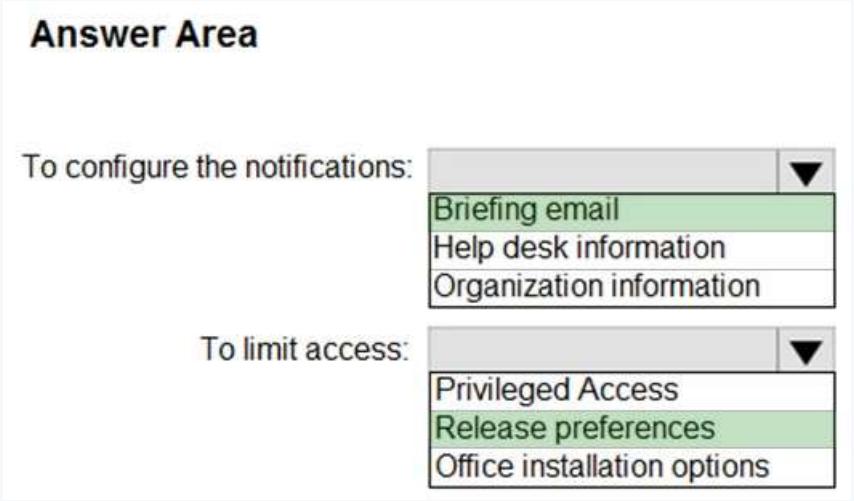
Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
HOTSPOT -
You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements.
What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/briefing/be-admin

https://docs.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide

DArnett 1 week, 1 day ago

I also believe it's Org Settings & Release Prefs

upvoted 1 times

pozzetttt 2 weeks, 5 days ago

The first answer is wrong:
1. Organization information: https://admin.microsoft.com/ --> Settings --> Org Settings --> Organization information --> Techincal conta
2. Release preferences

upvoted 2 times

rajeshrengasamy 2 weeks, 2 days ago

Correct.

upvoted 2 times

rajeshrengasamy 2 weeks, 2 days ago

https://learn.microsoft.com/en-us/microsoft-365/admin/manage/change-address-contact-and-more?view=o365-worldwide

upvoted 1 times

KemalM 4 weeks ago

Briefing emails do not provide information with service status notifications. It should be service health.

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
You need to select the update channel for Microsoft 365 Apps. The solution must meet the technical requirements.
What should you select?

A. Current Channel

B. Semi-Annual Enterprise Channel

C. Monthly Enterprise Channel

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#current-channel-overview

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

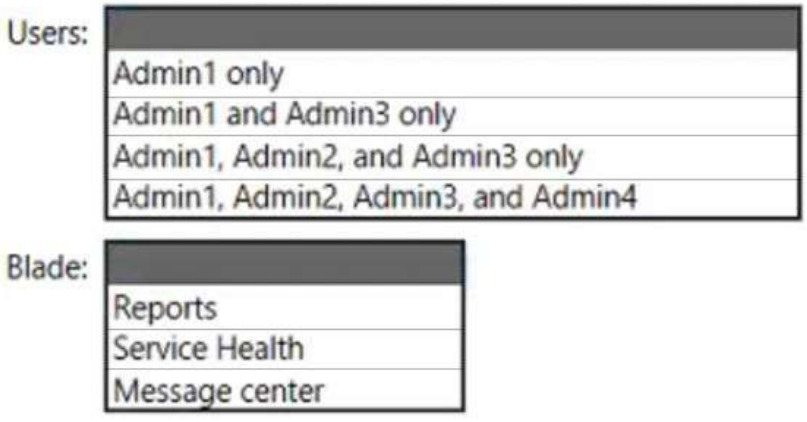
Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

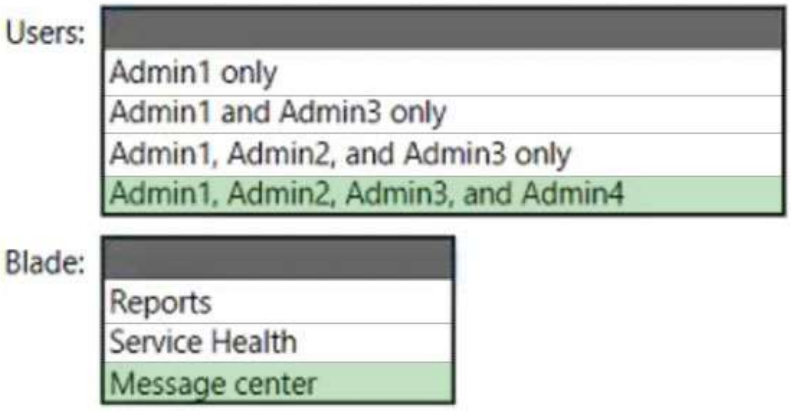
Question
HOTSPOT -
You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.
Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:

Answer Area



rajeshrengasamy 3 weeks ago

Answers : Admin 1 only and Service Health

https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide

upvoted 4 times

KemalM 4 weeks ago

Answer is NOT correct.

It should be Service Health blade. "The All services tab (the default view) shows all services, their current health state, and any active incidents or advisories. An icon and status in the Health column indicate the state of each service". https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide

For the first part, people who are assigned the global admin or service support admin role can view service health.

upvoted 3 times

renrenren 3 weeks ago

Yes, should be Service Health blade. But all users can view service health.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

upvoted 2 times

JerryZy 2 weeks, 1 day ago

People who are assigned the global admin or service support admin role can view service health
https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide

upvoted 2 times

Topic 9 - Testlet 2

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

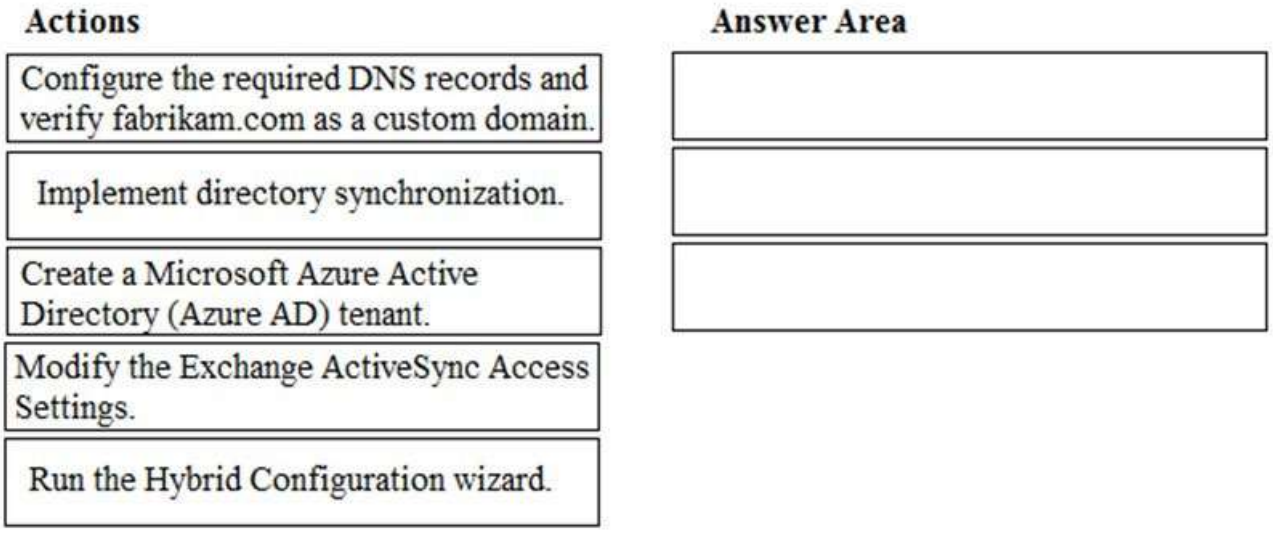
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

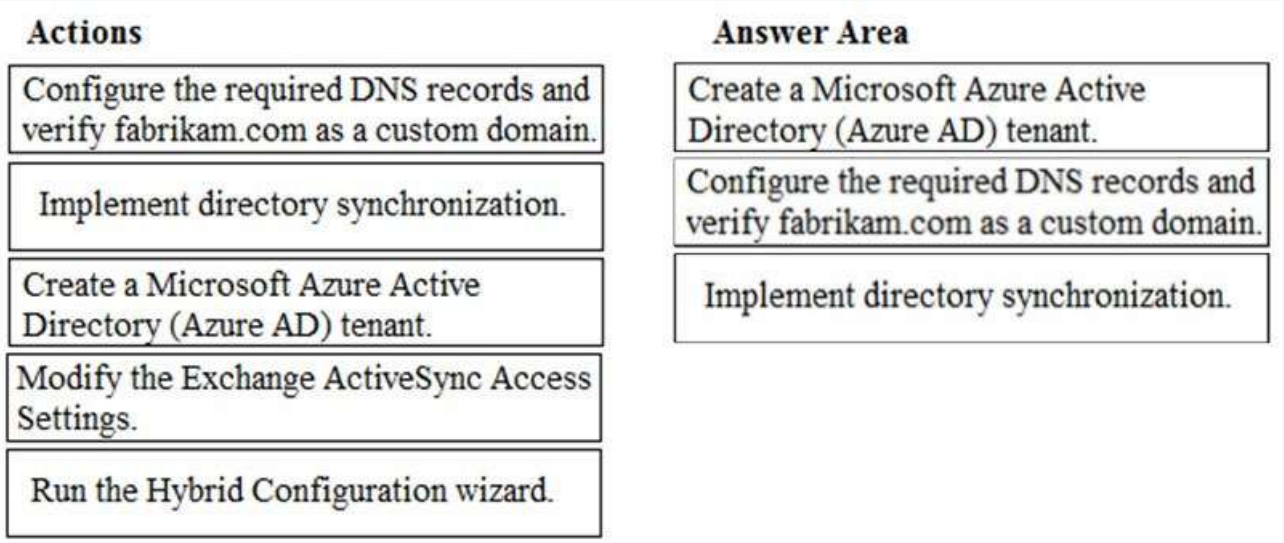
Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
DRAG DROP -
You need to prepare the environment for Project1.
You create the Microsoft 365 tenant.
Which three actions should you perform in sequence next? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Correct Answer:



Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
All users must be able to exchange email messages successfully during Project1 by using their current email address.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
This configuration requires a hybrid Exchange configuration during the pilot phase. This means that you will have mailboxes hosted in Exchange Online and mailboxes hosted in Exchange on-premise.
The first steps to configure Exchange hybrid are to Create the Azure AD tenant, add the Fabrikam.com domain as a custom domain, then configure directory synchronization to replicate the on-prem Active Directory user accounts to Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/exchange/exchange-hybrid

tejb Highly Voted 1 year ago
It says that you create the M365 tenant..what you do next? when you create the tenant, by default the Azure AD tenant is create.
The correct answer should be: configure domains, implement directory sync & run hybrid wizard
upvoted 16 times

bLINDmONKEY 1 year ago
This is the correct answer. Have done this IRL.
Azure AD is setup when you create the 365 tenant in the first place. So you add the custom domain. Setup the dirsync (ADConnect).
Then run the hybrid wiz to move the mailboxes seamlessly.
upvoted 7 times

joergsi 8 months, 1 week ago
You are 100% correct. The text is saying:
You create the Microsoft 365 tenant.
Which three actions should you perform in sequence next? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

To start with the tenant again is wrong! Missed this at first reading!
upvoted 2 times

larnyx Highly Voted 1 year, 3 months ago
Create - Configure - Implement
upvoted 6 times

michszym 1 year, 2 months ago
Agree - Implementing directory synchronization is on the "Hybrid deployment prerequisites" list:
https://docs.microsoft.com/en-us/exchange/hybrid-deployment-prerequisites
upvoted 1 times

Nilz76 Most Recent 6 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 1 times

kanag1 8 months, 2 weeks ago
What is the purpose of giving wrong answers? To make people to learn by themselves ?? Good initiative ! Thank you community for posting sensible comments and details along with answers !!
My answer choice is same as "tejb"
upvoted 5 times

Domza 1 year, 2 months ago
Little hint there, "user accounts needs to be moved over to the cloud from on-prem first".
(by using Azure Ad connect) Then, you'd migrate emails and files over to the cloud.

Users UPN's has to be in both places to be able to authenticate. (on-prem and Azure AD)

Life is good~
upvoted 1 times

Mamluk 1 year, 3 months ago
The answer is incorrect. 1,2,4 is correct
upvoted 2 times

vasyab 1 year, 3 months ago
Disagree with answer.
In task we have next requerements:

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using

their UPN.

Before you are able to move mailbox you must configure Hybrid configuration
https://docs.microsoft.com/en-us/exchange/hybrid-deployment/move-mailboxes#what-do-you-need-to-know-before-you-begin

directory synchronization is part of Hybrid configuration wizzard so we don't need to run it separetely.
My answer is:
Create a Microsoft Azure AD tenant
Configure the requered DNS records
Run the Hybrid Configuration Wizzard

upvoted 3 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
You are evaluating the required processes for Project1.
You need to recommend which DNS record must be created before adding a domain name for the project.
Which DNS record should you recommend?

A. alias (CNAME)

B. host information (HINFO)

C. host (AAA)

D. mail exchanger (MX)

Correct Answer: *D*
When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the
DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Text (TXT)
2. Mail exchanger (MX)
Other incorrect answer options you may see on the exam include the following:
1. Host (AAAA)
2. Pointer (PTR)
3. Name Server (NS)
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide

joergsi 8 months, 1 week ago
https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide

Step 1: Add a TXT or MX record to verify you own the domain
upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
You are evaluating the required processes for Project1.
You need to recommend which DNS record must be created while adding a domain name for the project.
Which DNS record should you recommend?

A. name server (NS)

B. text (TXT)

C. host (AAAA)

D. pointer (PTR)

Correct Answer: *B*
When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the
DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Text (TXT)
2. Mail exchanger (MX)
Other incorrect answer options you may see on the exam include the following:
1. Host Information (HINFO)
2. Host (A)
3. Name Server (NS)
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
Which migration solution should you recommend for Project1?

A. From the Microsoft 365 admin center, start a data migration and click Outlook as the data service.

B. From the Microsoft 365 admin center, start a data migration and click Exchange as the data service.

C. From Exchange Online PowerShell run the New-MailboxImportRequest cmdlet.

D. From Exchange Online PowerShell run the New-MailboxExportRequest cmdlet.

Correct Answer: *B*
Note:
* All users connect to an on-premises Microsoft Exchange Server 2016 organization.
* Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
* All users must be able to exchange email messages successfully during Project1 by using their current email address.
Use Minimal Hybrid to quickly migrate Exchange mailboxes to Microsoft 365 or Office 365.
Start migrating user mailbox data
After you assign licences to your users you can go to the Data migration page to start migrating their mailboxes.
1. Go to Setup > Data migration, and on the Migration page choose Exchange for your data service.
2. On the Data migration page, select the users whose mailboxes you want to migrate and then choose Start migration.
Note: Potential delay in email routing: Email sent to on-premises users whose mailboxes were migrated to Microsoft 365 or Office 365 are routed to their on- premises Exchange mailboxes until the MX record is changed.
Reference:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/use-minimal-hybrid-to-quickly-migrate

Topic 10 - Testlet 3

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
You need to ensure that Litware has the appropriate license to support the planned changes. The solution must minimize costs.
Which license type should you use?

A. Microsoft 365 Enterprise E5

B. Office 365 Enterprise F3

C. Microsoft 365 Enterprise E3

D. Office 365 Enterprise E5

Correct Answer: *A*
Reference:
https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-apps-for-enterprise-product

Topic 11 - Testlet 4

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to assign User2 the required roles to meet the security requirements.
Solution: From the Office 365 admin center, you assign User2 the Security Reader role. From the Exchange admin center, you assign User2 the Compliance
Management role.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
☞ User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The Security Reader role can view reports.
The Compliance Management role can schedule the email delivery of security and compliance reports.
Reference:
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to assign User2 the required roles to meet the security requirements.
Solution: From the Office 365 admin center, you assign User2 the Security Administrator role. From the Exchange admin center, you add User2 to the View-Only
Organization Management role.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
☞ User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The Security Administrator role can view reports but not schedule the email delivery of security and compliance reports.
The View-Only Organization Management role cannot schedule the email delivery of security and compliance reports.
Reference:
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to assign User2 the required roles to meet the security requirements.
Solution: From the Office 365 admin center, you assign User2 the Security Reader role. From the Exchange admin center, you assign User2 the Help Desk role.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
☞ User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The Security Reader role can view reports but not schedule the email delivery of security and compliance reports.
The Help Desk role cannot schedule the email delivery of security and compliance reports.
Reference:
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to assign User2 the required roles to meet the security requirements.
Solution: From the Office 365 admin center, you assign User2 the Records Management role. From the Exchange admin center, you assign User2 the Help Desk role.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The Records Management role cannot view reports or schedule the email delivery of security and compliance reports.
The Help Desk role cannot schedule the email delivery of security and compliance reports.
Reference:
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

Wojer 8 months ago
I think Security Operator would be better choice
upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

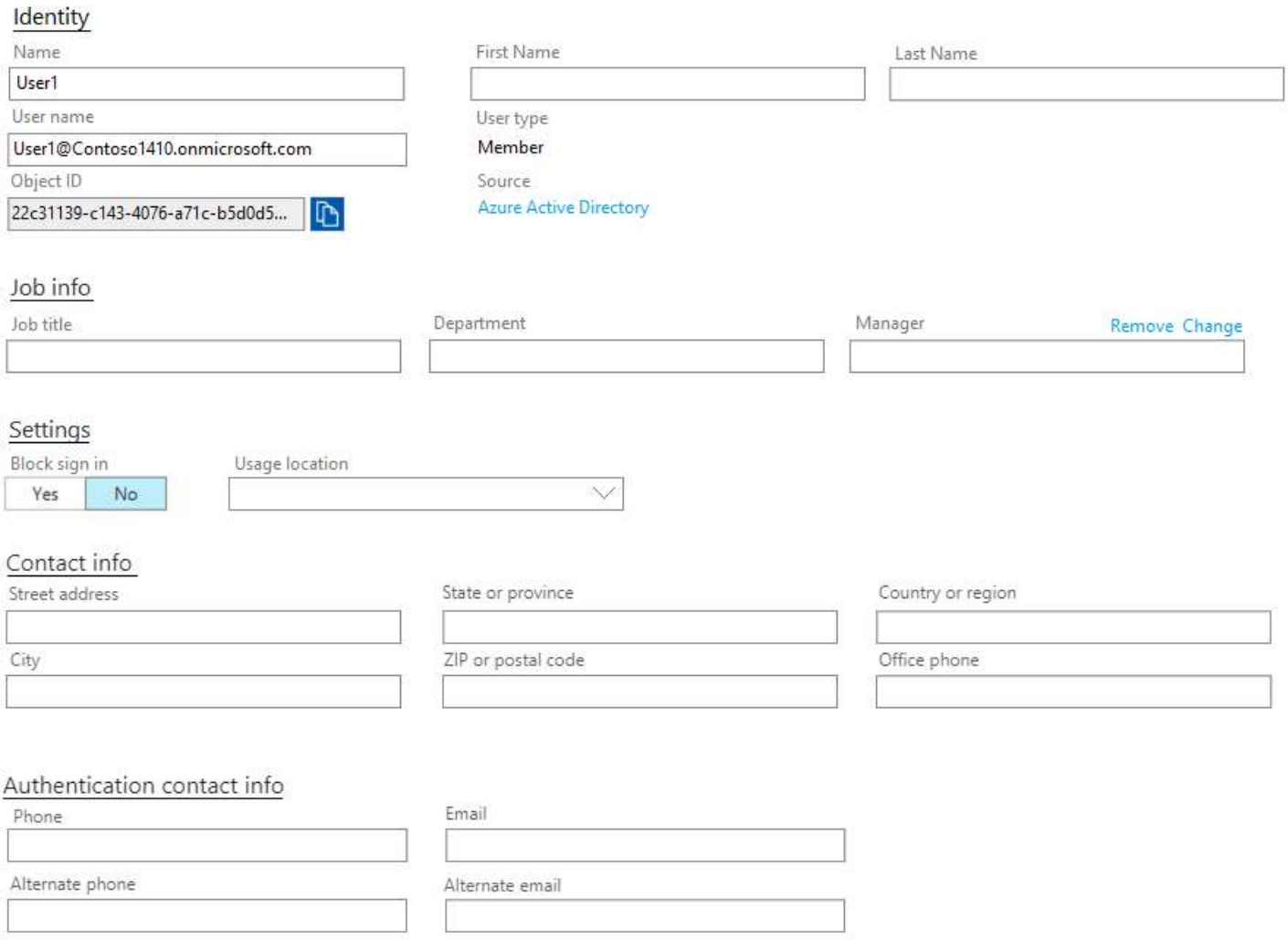
Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

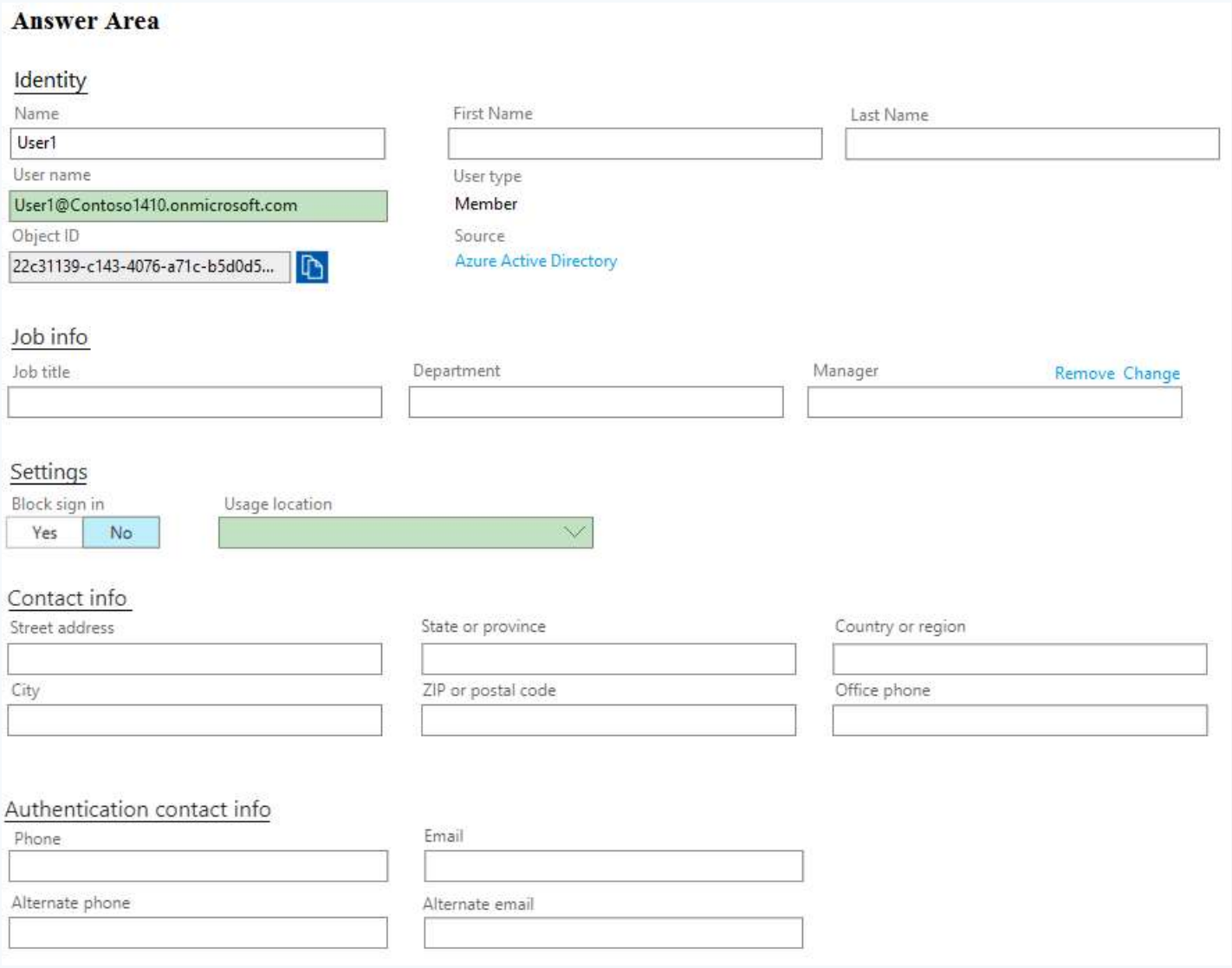
Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
HOTSPOT -
You need to meet the technical requirements for the user licenses.
Which two properties should you configure for each user? To answer, select the appropriate properties in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:



All new users must be assigned Office 365 licenses automatically.

To enable Microsoft 365 license assignment, the users must have a username. This is also the UPN. The users must also have a Usage Location.

vasyab Highly Voted 1 year, 3 months ago

Statements:
Microsoft Office 365 licenses are assigned only to Group2.
Group2 is dynamyc with filter user.Department -eq "Finance"

Question:
"Which two properties should you configure for each user? To answer, select the appropriate properties in the answer area."

My answer:
1. We have to modify Department (type Finance there)
2. Set user location US (licence won't assign without it and we don't have information about tenant initial location)

upvoted 30 times

michszym 1 year, 2 months ago

Question is about "technical requirments" and see this section: All new users must be assigned Office 365 licenses automatically.
So in my opinion answer is correct.

upvoted 1 times

ubt 1 year, 3 months ago

I agree with vasyab

upvoted 2 times

MomoLomo 1 year, 1 month ago

Agree with you

upvoted 2 times

kanag1 8 months, 2 weeks ago

Thats a great point about the department. Thank you Vasyab!!
The answers are :
1. Usage location
2. Department.

upvoted 2 times

emilianogalati Highly Voted 1 year, 1 month ago

The text states:
"Microsoft Office 365 licenses are assigned only to Group2."

I think we should modify the Department field and the location.
I would also modify the domain on which the user are assigned, but this is not in the question.

If I am wrong, please correct me!

upvoted 7 times

stoneface 9 months ago

The location for each user is inherited from the parent group. So in this case I do not consider that we must set a location.

For my answer I will consider changing the UPN and also setting the Department field with "Finance"

upvoted 2 times

amitsharma170490 Most Recent 3 weeks, 2 days ago

Usage Location and Department is the correct answer.

upvoted 2 times

Wojer 8 months ago

UPN and Department need to be adjust

upvoted 3 times

joergsi 8 months, 1 week ago

https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts?view=o365-worldwide

For the cloud-only identity model, you can assign Microsoft 365 licenses to user accounts as they are created, depending on how you create them.

For the hybrid identity model, when Active Directory Domain Services (AD DS) user accounts are synchronized for the first time, they ar not automatically assigned a location or a Microsoft 365 license. You must configure each user account with a user location prior to or along with assigning a license.

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
To which Azure AD role should you add User4 to meet the security requirement?

A. Password administrator

B. Global administrator

C. Security administrator

D. Privileged role administrator

Correct Answer: *B*
⇨ User4 must be able to reset User3 password.
User3 is assigned the Customer Lockbox Access Approver role. Only global admins can reset the passwords of people assigned to this role as it's considered a privileged role.
Reference:
https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Customer-Lockbox-Approver-Role-Now-Available/ba-p/223393

vasyab Highly Voted 1 year, 3 months ago
Just copy from link's answer from FAQ section:

Q: Can a regular user admins reset the password for members of Customer Lockbox access approver role?

A: Only global admins can reset the passwords of people assigned to this role as it's considered a privileged role.

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/customer-lockbox-approver-role-now-available/ba-p/223393
upvoted 6 times

spg987 Highly Voted 1 year, 1 month ago
In exam toay
upvoted 5 times

Wojer Most Recent 8 months ago
My question is how manage office 365 connectors have to do with Customer Lockbox Access Approver role. one is managing connecto
exchange another is managing access requests.
upvoted 1 times

Wojer 8 months ago
By the way, it's true only Global admin can reset password for that role.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#customer-lockbox-access-approver
upvoted 1 times

joergsi 8 months, 1 week ago
This question is a real bitch:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#customer-lockbox-access-approver

Customer LockBox Access Approver
Manages Customer Lockbox requests in your organization. They receive email notifications for Customer Lockbox requests and can approve and deny requests from the Microsoft 365 admin center. They can also turn the Customer Lockbox feature on or off. => Only Global Administrators can reset the passwords of people assigned to this role.

upvoted 1 times

ubt 1 year, 3 months ago

I can confirm this was in my MS-100 Exam

upvoted 4 times

Cybersecgirl 1 year, 3 months ago

Did you get any labs/simulations in your exam? asking as your comment seems to be very recent. thanks

upvoted 1 times

venwaik 1 year, 2 months ago

Took the exam today and i didn't got any labs in my exam.

upvoted 9 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

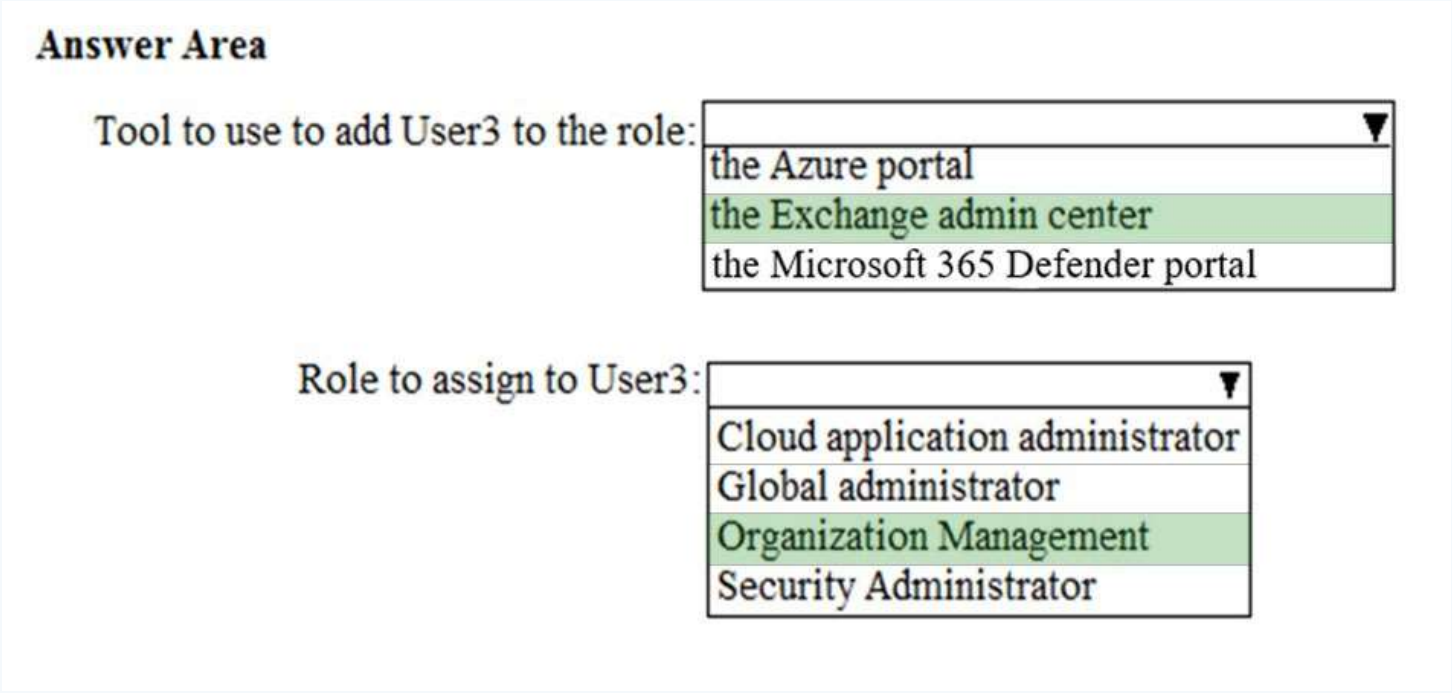
Question
HOTSPOT -
You need to meet the security requirements for User3. The solution must meet the technical requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Tool to use to add User3 to the role:
- the Azure portal
- the Exchange admin center
- the Microsoft 365 Defender portal

Role to assign to User3:
- Cloud application administrator
- Global administrator
- Organization Management
- Security Administrator

Correct Answer:



User3 must be able to manage Office 365 connectors.

The principle of least privilege must be used whenever possible.

Office 365 connectors are configured in the Exchange Admin Center.

You need to assign User3 the Organization Management role to enable User3 to manage Office 365 connectors.

A Global Admin could manage Office 365 connectors but the Organization Management role has less privilege.

Reference:

https://docs.microsoft.com/en-us/office365/SecurityCompliance/eop/feature-permissions-in-eop

spg987 Highly Voted 1 year, 1 month ago

In exam today

upvoted 5 times

kanag1 Most Recent 8 months, 2 weeks ago

The given asnwers are correct
The question says: You need to meet the "security requirements for User3" which is "User3 must be able to manage Office 365 connectors" .
The role is “Organisation Management” to manage the connectors.
The role could be assigned from Exchange management Console.

upvoted 2 times

AlexLiourtas 8 months, 3 weeks ago

Box 2: Global Administrator.
It is not stated in the question: "The principle of least privilege must be used whenever possible" so i m not really sure why not global admin would cut it.

upvoted 1 times

DK_edu 7 months, 3 weeks ago

It is stated under Technical Requirements.

upvoted 1 times

L33D 10 months, 3 weeks ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide

upvoted 1 times

ubt 1 year, 3 months ago

I can confirm this was in my MS-100 exam

upvoted 3 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com
Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
You need to assign User2 the required roles to meet the security requirements and the technical requirements.
To which two roles should you assign User2? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Exchange View-only Organization Management role

B. the Microsoft 365 Records Management role

C. the Exchange Online Help Desk role

D. the Microsoft 365 Security Reader role

E. the Exchange Online Compliance Management role

Correct Answer: *DE*
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The Security Reader role can view reports but not schedule the email delivery of security and compliance reports.
The Exchange Online Compliance Management role can schedule the email delivery of security and compliance reports.
Reference:
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

RiTh73 7 months, 2 weeks ago
Selected Answer: DE
Answer are correct.
upvoted 2 times

kanag1 8 months, 2 weeks ago
Selected Answer: DE
D and E are correct answers
upvoted 3 times

Topic 12 - Testlet 5

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

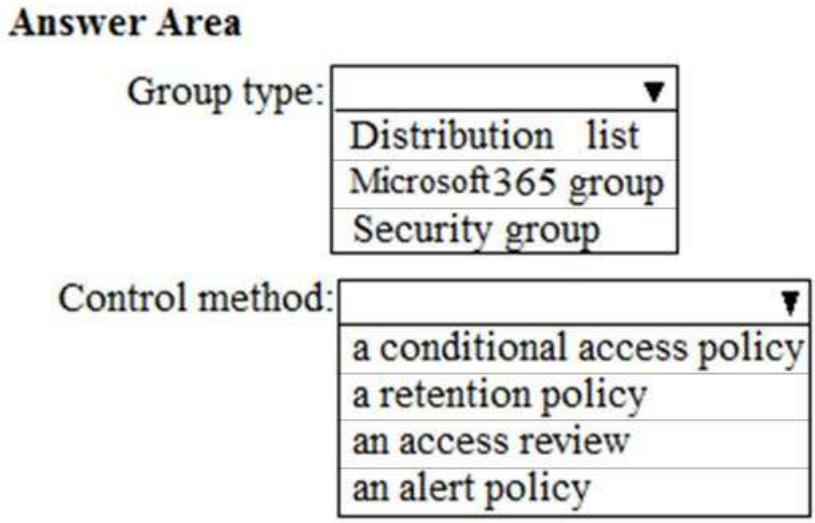
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

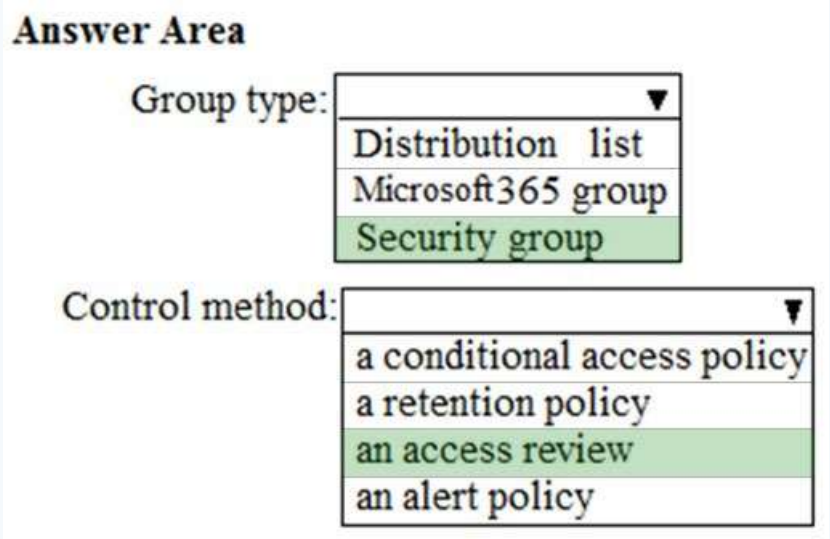
Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
HOTSPOT -
You need to create the UserLicenses group. The solution must meet the security requirements.
Which group type and control method should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
The group needs to be a Security group.
Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise

applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

TashaGirl 8 months, 3 weeks ago

This is very interesting, M365 Group with dynamic membership allows to add a license. However, nowhere it states that the group will have dynamic membership, so I will go with security + access reviews. Both group types would be supported though, with the assumpt of dynamic membership for M365 group.

upvoted 1 times

TEEEEEEEEEE 1 year, 1 month ago

"Licenses can be assigned to any security group in Azure AD." https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-licensing-whatis-azure-portal#features

upvoted 4 times

RML_Wyvern 1 year, 1 month ago

If you look in Azure Ad Groups, only Security Group has the licence option.

upvoted 4 times

dminerva94 1 year, 1 month ago

Couldn't this be done with either a M365 or security group?

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
Which role should you assign to User1?

A. Security Administrator

B. Records Management

C. Security Reader

D. Hygiene Management

Correct Answer: *C*
☞ A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure
Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in
Office 365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

BDuff 8 months, 3 weeks ago
C is correct
upvoted 2 times

vasyab 1 year, 3 months ago
this explanation link is more correct https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide#permissions-for-dlp-reports
upvoted 3 times

Topic 13 - Testlet 6

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

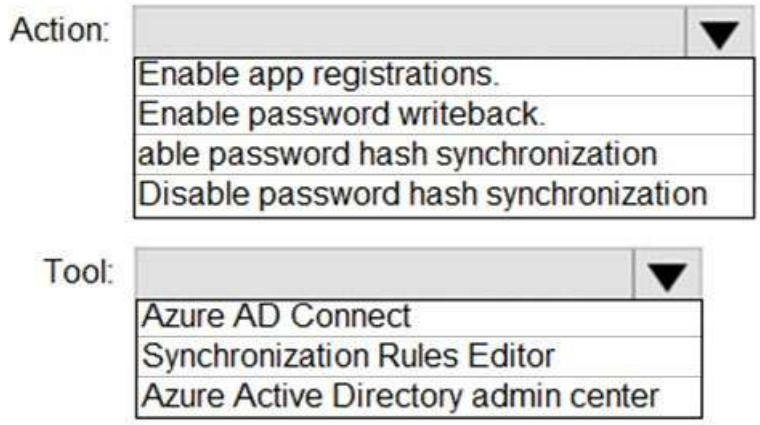
Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

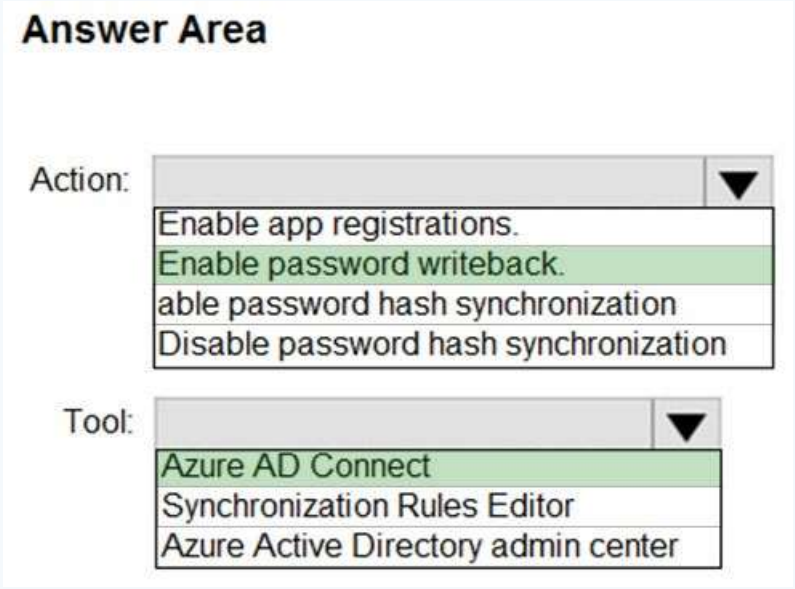
Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
HOTSPOT -
You need to ensure that Admin4 can use SSPR.
Which tool should you use, and which action should you perform? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.
What should you do?

A. From PowerShell, run the Start-ADSyncCycle cmdlet.

B. From the Microsoft Azure Active Directory Connect wizard, select Manage federation.

C. From PowerShell, run the Add-ADSyncConnectorAttributeInclusion cmdlet.

D. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#organizational-unitbased-filtering

Topic 14 - Testlet 7

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Office 365 E5 licenses are assigned only to Group2.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com

Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
You need to meet the security requirement for Group1.
What should you do?

A. Configure all users to sign in by using multi-factor authentication.

B. Modify the properties of Group1.

C. Assign Group1 a management role.

D. Modify the Password reset properties of the Azure AD tenant.

Correct Answer: *D*
The members of Group1 must be required to answer a security question before changing their password.
If SSPR (Self Service Password Reset) is enabled, you must select at least one of the following options for the authentication methods.
Sometimes you hear these options referred to as "gates."

Mobile app notification -

Mobile app code -

Email -

Mobile phone -

Office phone -

Security questions -
You can specify the required authentication methods in the Password reset properties of the Azure AD tenant. In this case, you should set the required authentication method to be 'Security questions'.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

Wearsy Highly Voted 1 year, 5 months ago
Poor explination but this is correct, at least give us some indication you can specify a group in the answer overview... - https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#:~:text=Sign%20in%20to%20the%20Azure%20portal.,the%20SSPR%20change%2C%20select%20Save.
upvoted 5 times

AlexLiourtas 8 months, 3 weeks ago
garbage questions and wording, typical microsoft.
upvoted 1 times

RiTh73 Most Recent 7 months, 2 weeks ago

Selected Answer: D

I would prefer for D

upvoted 2 times

L33D 10 months, 3 weeks ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

upvoted 1 times

spg987 1 year, 1 month ago

In exam today

upvoted 3 times

TimNov 1 year, 4 months ago

D - these options are configured in the SSPR (Self Service Password Reset)

upvoted 3 times

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Office 365 E5 licenses are assigned only to Group2.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com

Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
You need to meet the security requirement for the vendors.
What should you do?

A. From the Azure portal, add an identity provider.

B. From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the λ€"UserPrincipalName parameter.

C. From Azure Cloud Shell, run the Set-AzureADUserExtension cmdlet.

D. From the Azure portal, create guest accounts.

Correct Answer: *D*
☞ Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user's account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest user must then redeem their invitation to access resources. An invitation of a user does not expire.
The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question, the vendors already have Microsoft accounts so they can authenticate using them.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator

Currently there are no comments in this discussion, be the first to comment!

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment -

The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You recently configured the forest to sync to the Azure AD tenant.

You add and then verify adatum.com as an additional domain name.

All servers run Windows Server 2016.

All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.

All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Office 365 E5 licenses are assigned only to Group2.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq “Finance”)

Office 365 E5 licenses are assigned only to Group2.

The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements -

Planned Changes -

Contoso plans to provide email addresses for all the users in the following domains:

East.adatum.com

Contoso.adatum.com

Humongousinsurance.com

Technical Requirements -
Contoso identifies the following technical requirements:
All new users must be assigned Office 365 E5 licenses automatically.
The principle of least privilege must be used whenever possible.

Security Requirements -
Contoso identifies the following security requirements:
Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The members of Group1 must be required to answer a security question before changing their password.
User3 must be able to manage Office 365 connectors.
User4 must be able to reset User3 password.

Question
You need to meet the security requirement for the vendors.
What should you do?

A. From Azure Cloud Shell, run the Set-MsolUserPrincipalName and specify the ג€"tenantID parameter.

B. From Azure Cloud Shell, run the Set-AzureADUserExtension cmdlet.

C. Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the ג€"UserPrincipalName parameter.

D. From Azure Cloud Shell, run the New-AzureADMSInvitation cmdlet and specify the ג€"InvitedUserEmailAddress parameter.

Correct Answer: *D*
☞ Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user's account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest user must then redeem their invitation to access resources. An invitation of a user does not expire.
The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question, the vendors already have Microsoft accounts so they can authenticate using them.
In this solution, we are creating guest account invitations by using the New-AzureADMSInvitation cmdlet and specifying the ג€"InvitedUserEmailAddress parameter.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From the Azure portal, create guest accounts.
2. From Azure Cloud Shell, run the New-AzureADMSInvitation cmdlet and specify the ג€"InvitedUserEmailAddress parameter.
Other incorrect answer options you may see on the exam include the following:
1. From the Azure portal, modify the authentication methods.
2. From the Azure portal, add an identity provider.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

mkoprivnj Highly Voted 1 year, 9 months ago
D for sure!
upvoted 8 times

BDuff Most Recent 8 months, 3 weeks ago
D all the way!
upvoted 1 times

PattiD 1 year, 9 months ago

New-AzureADMSInvitation
[-InvitedUserDisplayName <String>]
-InvitedUserEmailAddress <String>
[-SendInvitationMessage <Boolean>]
-InviteRedirectUrl <String>
[-InvitedUserMessageInfo <InvitedUserMessageInfo>]
[-InvitedUserType <String>]
[<CommonParameters>]

upvoted 2 times

Alvaroll 2 years ago

12-50 https://www.examtopics.com/exams/microsoft/ms-100/view/43/

upvoted 3 times

Topic 15 - Testlet 8

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

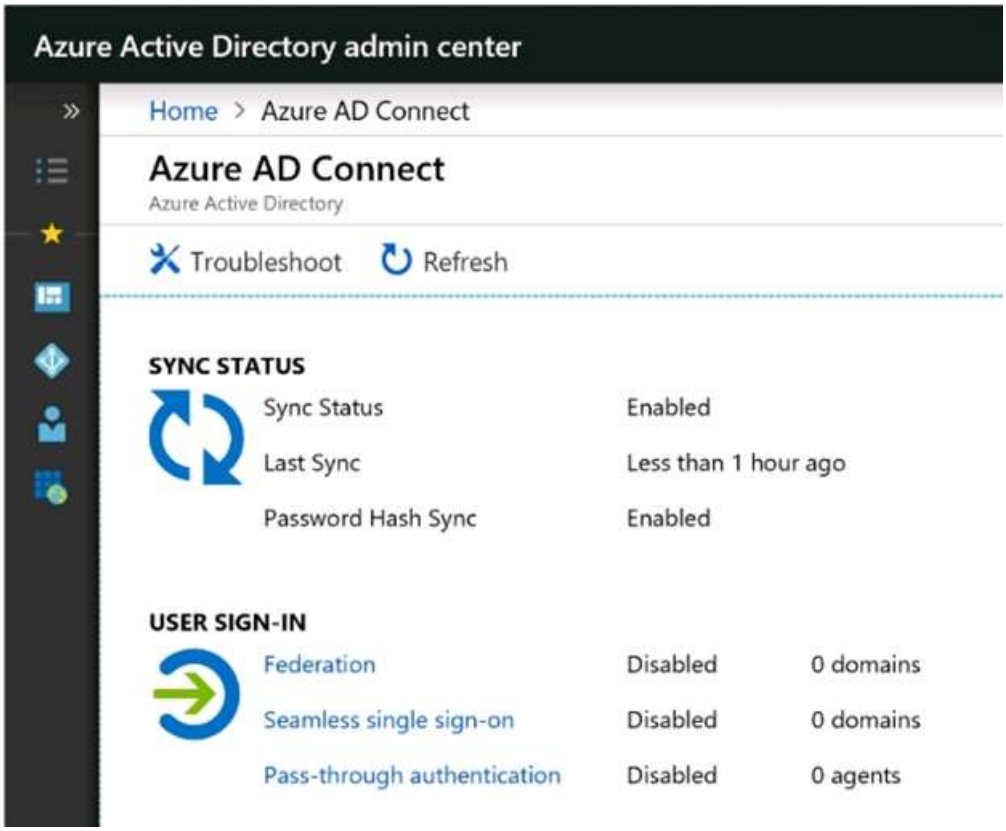
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
▪
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

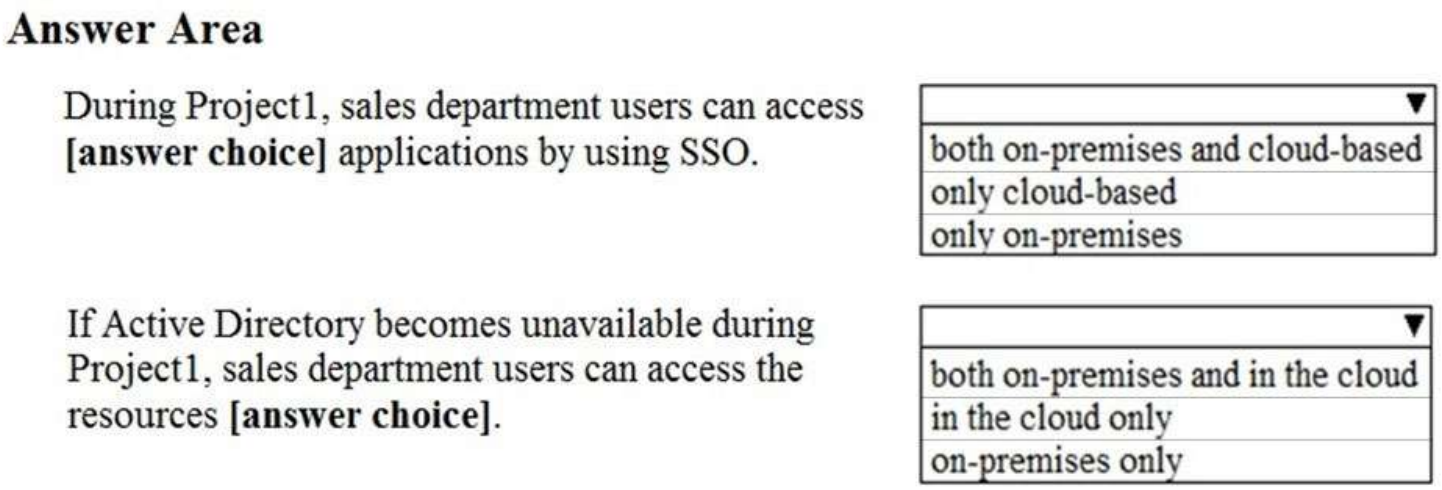
Question
HOTSPOT -
You create the Microsoft 365 tenant.
You implement Azure AD Connect as shown in the following exhibit.



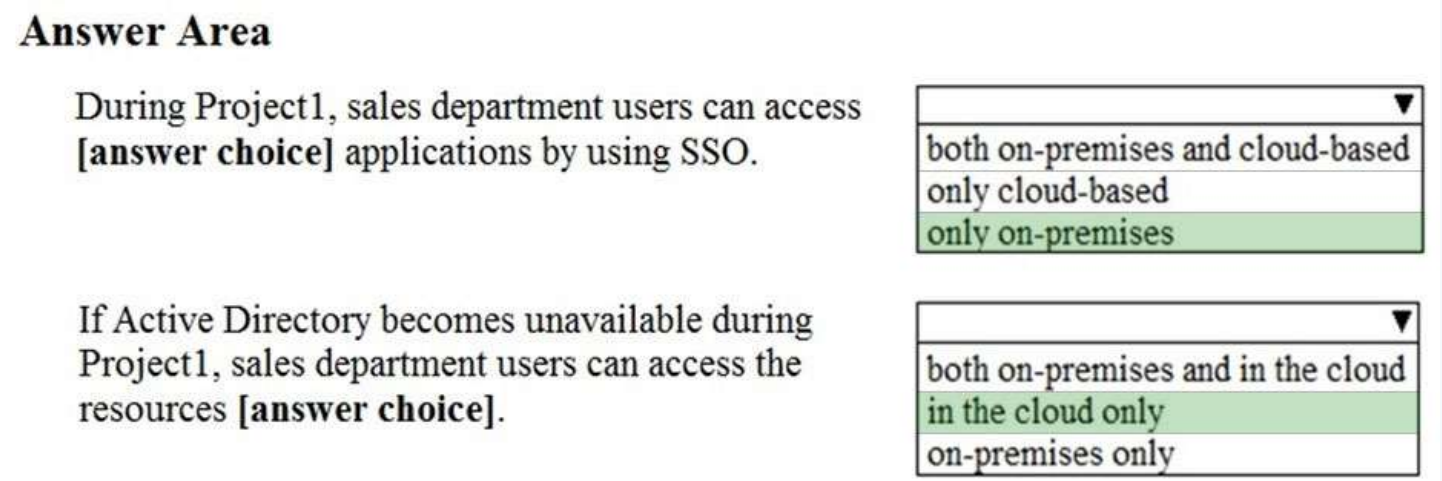
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.

In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Azure Active

Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active

Directory. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.

Davidchercm 8 months, 2 weeks ago

what is the correct answer ? it should be using PHS right ?

upvoted 1 times

junior6995 1 year ago

Kind of funny, you Turn on PSH but you disable SSO. wft?

upvoted 3 times

jkklim 9 months, 2 weeks ago

why cannot ?

upvoted 1 times

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
▪
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
You need to meet the application requirement for App1.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From the Azure Active Directory admin center, configure the application URL settings.

B. From the Azure Active Directory admin center, add an enterprise application.

C. On an on-premises server, download and install the Microsoft AAD Application Proxy connector.

D. On an on-premises server, install the Hybrid Configuration wizard.

E. From the Microsoft 365 admin center, configure the Software download settings.

Correct Answer: *ABC*
☞ An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the
Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. Azure AD, the Application Proxy service, and the Application Proxy connector work together to securely pass the user sign-on token from Azure AD to the web application.
In this question, we need to add an enterprise application in Azure and configure a Microsoft AAD Application Proxy connector to connect to the on-premises web application (App1).
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy#how-application-proxy-works

RiTh73 7 months, 2 weeks ago

Selected Answer: ABC
I don't think why we need to add Enterprise Application and not Application Proxy in AAD since we actually install App proxy connector on-prem network.

But since there is no application proxy, so only Enterprise app is the last choice.

Answer: A,B,C
upvoted 2 times

PDR 9 months, 2 weeks ago

looks correct to me
the steps are correct and also easy enough to eliminate D and E as Hybrid Config Wizard is for Exchange Hybrid config so not in scope this and E would simply be for controlling the Office Apps downloads

upvoted 2 times

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication.

Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as a DNS server.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
▪
The memberships of UserLicenses must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

Question
You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

A. password hash synchronization and seamless SSO

B. pass-through authentication

C. password hash synchronization

D. pass-through authentication and seamless SSO

Correct Answer: *A*
⇨ Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
⇨ Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
⇨ After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
⇨ Fabrikam does NOT plan to implement identity federation.
⇨ After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

VTHAR Highly Voted 1 year, 11 months ago
"Users must be able to authenticate to cloud services if Active Directory becomes unavailable." => That means PTA doesn't meet the requirement. PHS left.

"After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically." That means PHS alone is not the solution and must implement together with Seamless SSO.

Therefore the answer is correct.
upvoted 22 times

DArnett Most Recent 1 week, 1 day ago
This was on my exam on 9/27/22.
upvoted 1 times

MichaelJS 1 year, 9 months ago

I agree, the answer is correct. What I don't get is the statement "Fabrikam does NOT plan to implement identity federation.". Aren't PTA and maybe PHS a sort of "identity federation"?

upvoted 2 times

Turak64 1 year, 1 month ago

I'd take that as not using AD FS

upvoted 1 times

mkoprivnj 1 year, 9 months ago

A for sure!

upvoted 2 times

mkoprivnj 1 year, 9 months ago

VTHAR, well done!

upvoted 1 times

pkudude99 2 years ago

Corrected link -- https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 1 times

moh15 2 years ago

Ans is correct

upvoted 1 times

ExamStudy68 2 years, 8 months ago

Why would this require the Seamless SSO element? Is not PHS enough?

upvoted 2 times

TFou0076 2 years, 8 months ago

They said "After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically."

upvoted 11 times

Sisko 2 years, 8 months ago

This requirement indicates you need the seamless SSO. "After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically."

upvoted 9 times

donathon 1 year, 11 months ago

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses. >> This a make pass-through authentication unsuitable.

upvoted 1 times

juliuscsir 2 years, 6 months ago

Kind of agree--the question states "Which authentication strategy should you implement FOR THE PILOT PROJECTS?" This leads me t think that 'password hash synchronization' (C) is the answer.

upvoted 1 times

JaBe 2 years, 3 months ago

That's debatable as using a different configuration for the pilot would defeat the purpose of a pilot altogether. Therefore I lean towards SSO here (although reluctantly)

upvoted 2 times

Topic 16 - Testlet 9

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
HOTSPOT -
You are evaluating the use of multi-factor authentication (MFA).
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	○	○
Users must use the Microsoft Authenticator app to complete MFA.	○	○
After registering, users must use MFA for every sign-in.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	○	○
Users must use the Microsoft Authenticator app to complete MFA.	○	○
After registering, users must use MFA for every sign-in.	○	○

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy
https://blog.admindroid.com/configuring-and-managing-mfa-in-office-365/

DArnett 1 week, 1 day ago
This was on my exam on 9/27/22.
upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
You need to configure just in time access to meet the technical requirements.
What should you use?

A. access reviews

B. entitlement management

C. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

D. Azure Active Directory (Azure AD) Identity Protection

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

DArnett 1 week, 1 day ago
This was on my exam on 9/27/22.
upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

General Overview -

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named ADatum Corporation.

Environment -

On-Premises Environment -

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins,

Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud environment -

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure Active Directory Premium Plan 2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

Password hash synchronization is enabled.

Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk admin
Admin3	Security admin
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Azure Active Directory (Azure AD) tenant has Security defaults enabled.

Problem Statements -
Litware identifies the following issues:
Admin1 cannot create conditional access policies.
Admin4 receives an error when attempting to use SSPR.
Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Implement Microsoft Intune.
Implement Microsoft Teams.
Implement Microsoft Defender for Office 365.
Ensure that users can install Office 365 apps on their device.
Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -
Litware identifies the following technical requirements:
Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
Litware users must be able to invite. ADatum users to participate in the following activities:
- Join Microsoft Teams channels.
- Join Microsoft Teams chats.
- Access shared files.
Just in time access to critical administrative roles must be required.
Microsoft 365 incidents and advisories must be reviewed monthly.
Office 365 service status notifications must be sent to Admin2.
The principle of least privilege must be used.

Question
You need to configure Microsoft Teams to support the technical requirements for collaborating with ADatum.
What should you configure in the Microsoft Teams admin center?

A. meeting policies

B. messaging policies

C. guest access

D. external access

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoftteams/manage-external-access

dth 4 days, 9 hours ago

Selected Answer: C

Requirements are join Teams channels and access shared files > So we need guest users. Therefore we need to configure C. guest acce

upvoted 1 times

KemalM 2 weeks, 4 days ago

Most of all, if you need to give access to shared files, you should configure guest access (https://learn.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations#things-your-users-can-do)

upvoted 1 times

Debadatta 3 weeks, 1 day ago

Correct answer: C
"If you want people from other organizations to have access to your teams and channels, use guest access instead. "
https://docs.microsoft.com/en-us/microsoftteams/manage-external-access

upvoted 3 times

renrenren 2 weeks, 5 days ago

Agree.
More info, the difference between external access and guest
https://learn.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations#compare-external-and-gues
access
https://learn.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations#compare-external-and-gues
access

upvoted 1 times