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.

Suggested 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 3 years, 2 months ago
IT = E5
Mangers = E3
upvoted 38 times

EG_Jack 3 years, 2 months ago
Correct
upvoted 3 times

ElimGarak Highly Voted 3 years, 3 months 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

Adebimpeidiat Most Recent 1 year, 8 months ago
A&D is the answer
upvoted 1 times

BobDobolina 1 year, 10 months ago
https://m365maps.com/matrix.htm
upvoted 1 times

Don123 1 year, 11 months ago
A&D is correct

Microsoft 365 E3 license includes Azure Active Directory (Azure AD) Conditional Access, which is required for both the IT and Managers group members. Additionally, Azure AD Privileged Identity Management, which is required for the IT group members, is included in the Microsoft 365 E5 license but the cost is higher than the E3 license. Therefore, to keep the licensing costs to a minimum, you should recommend acquiring the Microsoft 365 E3 license for both the IT and Managers group members.
upvoted 2 times

egsalvadori 2 years ago
Selected Answer: AD
PIM is only available for E5

upvoted 1 times

Startkabels 2 years ago

Selected Answer: AD

AD it is

upvoted 1 times

conorward96 2 years, 1 month ago

Correct

upvoted 1 times

NikolasFj98 2 years, 2 months ago

Selected Answer: AD

A D are correct

upvoted 1 times

NASH77 2 years, 3 months 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 2 years, 8 months 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 2 years, 10 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 2 years, 10 months ago

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

upvoted 1 times

joergsi 2 years, 11 months ago

Where is the difference between answers B and D?

upvoted 2 times

joergsi 2 years, 10 months ago

Passed the Exam with 830 Points!

upvoted 1 times

Zethembiso 2 years, 11 months 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 2 years, 12 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 3 years ago

IT needs : Microsoft 365 E5 = Azure P2 = Privileged Identity Management

Managers needs : Microsoft 365 E3 = Azure P1 = Conditional Access

upvoted 8 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.

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

Community vote distribution
B (67%) C (33%)

zul_n Highly Voted 3 years, 3 months ago
B is correct.

Exchange admin centre | organization | new organization sharing
upvoted 9 times

Adebimpeidiat Most Recent 1 year, 8 months ago
B is the answer
It is because you are sharing with an external organization, this would allow them to access calendar of every user in your organization.
upvoted 1 times

vanr2000 1 year, 9 months ago
Selected Answer: B
The right answer is "B"

Set up an organization relationship to share calendar information with an external business partner. Microsoft 365 or Office 365 admins can set up an organization relationship with another Microsoft 365 and Office 365 organization or with an Exchange on-premises organization. If you want to share calendars with an on-premises Exchange organization, the on-premises Exchange administrator has to set up an authentication relationship with the cloud (also known as "federation") and must meet minimum software requirements.

Links that supports the right answer:
https://learn.microsoft.com/en-us/exchange/sharing/organization-relationships/organization-relationships

https://learn.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship
upvoted 1 times

Don123 1 year, 11 months ago
B. Configure a new organization relationship via Exchange admin center.

To enable calendar sharing with a partner organization that also has a Microsoft 365 tenant, you should configure a new organization relationship via the Exchange admin center. This will allow users in the partner organization to have access to the calendar of every user in your organization instantly.
You would have to go to Exchange admin center > sharing > + new > organization and add the partner organization details and configure the appropriate sharing settings such as calendar sharing, mailboxes sharing etc.
Conditional access policy, sharing settings and running cmdlet are not related to calendar sharing with partner organization.
upvoted 2 times

soosha 1 year, 12 months ago
Selected Answer: B

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

upvoted 1 times

Gillactus 2 years ago

Selected Answer: C

Exchange Admin center --> Organization -->Sharing

upvoted 2 times

Razuli 2 years ago

thanks

upvoted 1 times

Startkabels 2 years ago

Selected Answer: B

Nobrainer B

upvoted 1 times

NikolasFj98 2 years, 2 months ago

Selected Answer: B

B is correct

upvoted 1 times

Balvosko 2 years, 9 months 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 2 years, 9 months ago

The answer is C

Exchange admin centre | organization | Sharing and add a the policy with the desired domain. No relationship involved

upvoted 4 times

Oceanide 3 years, 1 month ago

Correct answer is B.

upvoted 2 times

JakeH 3 years, 1 month 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

Suggested Answer: *B*

Community vote distribution

B (100%)

[Removed] Highly Voted 3 years ago

B. No, you need to change the maximum concurrent migration to decrease the connection to the source server.

upvoted 8 times

Adebimpeidiat Most Recent 1 year, 8 months ago

b is the answer. Labels are meant to prove how confidential the document or email is, it has nothing to do with migration.

upvoted 1 times

Don123 1 year, 11 months ago

B. No

Creating a label policy will not help to decrease the effect the mailbox migration has on users.
This solution does not address the root cause of the issue (slow performance during migration) and it is not related to the migration process.
Label policies are used to classify and protect sensitive data in Exchange Online and Microsoft 365 environments.
To decrease the effect of the migration on users, you should review the migration batch settings and ensure that the migration is properly configured and optimized.

upvoted 3 times

Startkabels 2 years ago

Selected Answer: B

Labels are for documents, emails and stuff to classify and apply compliance policies etc.
They have nothing to do with the migration performance.

upvoted 1 times

waterlego 2 years, 8 months ago

Still valid, April 2022

upvoted 1 times

Moderator 2 years, 9 months ago

Selected Answer: B

No, a label policy definitely wouldn't help here.

upvoted 1 times

Oceanide 3 years, 1 month ago

No, because you need to modify the migration endpoint settings.

upvoted 2 times

cseg 3 years, 2 months 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

Question #4 *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 mail flow rule.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

myloking Highly Voted 3 years, 1 month 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 issue, modify the migration endpoint settings.

upvoted 10 times

Adebimpeidiat Most Recent 1 year, 8 months ago

B is the answer, mail flow has nothing to do with the messages already sent.

upvoted 1 times

vanr2000 1 year, 9 months ago

Selected Answer: B

Mail flow rules (transport rules) in Exchange Online are for different purposes
https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

upvoted 1 times

Don123 1 year, 11 months ago

B. No

Creating a label policy will not help to decrease the effect the mailbox migration has on users.
This solution does not address the root cause of the issue (slow performance during migration) and it is not related to the migration process.
Label policies are used to classify and protect sensitive data in Exchange Online and Microsoft 365 environments.
To decrease the effect of the migration on users, you should review the migration batch settings and ensure that the migration is properly configured and optimized.

upvoted 1 times

Startkabels 2 years ago

Selected Answer: B

Nope, surely not

upvoted 1 times

waterlego 2 years, 8 months ago

Still valid, April 2022

upvoted 1 times

Moderator 2 years, 9 months ago

Selected Answer: B

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

upvoted 1 times

Question #5 *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 modify the migration endpoint settings.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Community vote distribution

A (100%)

FumerLaMoquette Highly Voted 3 years, 5 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 20 times

Tonio77s 3 years, 2 months ago
Thanks for the link
upvoted 2 times

Adebimpeidiat Most Recent 1 year, 8 months ago
A is the answer.
upvoted 1 times

Don123 1 year, 11 months ago
A. Yes
You may consider implementing a migration throttling policy to limit the number of mailboxes that are migrated simultaneously and stagger the migration of large mailboxes. Additionally, you can also consider using migration tools that are designed to minimize the impact on users during the migration process.
upvoted 1 times

Startkabels 2 years ago
Selected Answer: A
Nobrainer A
upvoted 1 times

waterlego 2 years, 8 months ago
Still valid, April 2022
upvoted 1 times

Moderator 2 years, 9 months ago
Selected Answer: A
This is the correct answer indeed.
upvoted 3 times

mikl 2 years, 11 months 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 4 times

Question #6 *Topic 1*

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.

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

Community vote distribution
C (100%)

gxsh Highly Voted 3 years, 3 months ago
C is the right answer.
upvoted 6 times

Adebimpeidiat Most Recent 1 year, 8 months ago
C is the answer. This is because this policy is used to protect the organization from any malicious/threat email.
upvoted 1 times

Irism 1 year, 9 months ago
domme vraag
upvoted 1 times

Don123 1 year, 11 months ago
C. Threat management policy

To prevent your company from receiving phishing email messages, you should create a new mail flow rule as part of a threat management policy in Microsoft 365.
A threat management policy allows you to configure rules and settings to help protect your organization from spam, phishing, and other types of malicious email. This includes creating mail flow rules to identify and block suspicious messages based on specific criteria, such as sender, recipient, subject, or message content.
Label policy, spam filter policy are not related to phishing email protection.
upvoted 2 times

Startkabels 2 years ago
Selected Answer: C
C for sure
upvoted 1 times

[Removed] 3 years ago
C. You can modify Anti-phishing settings there.
upvoted 4 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

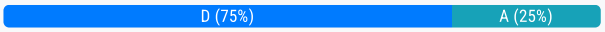
B. Update-OfflineAddressBook

C. Set-AddressBookPolicy

D. Set-EmailAddressPolicy

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

Community vote distribution



JakeH Highly Voted 3 years, 1 month ago
In exam today. Answer is correct
upvoted 9 times

Jcbrow27 3 years, 1 month ago
¿you cleared?
upvoted 3 times

Adebimpeidiat Most Recent 1 year, 8 months ago
D is the answer. You need to the Set-EmailAddressPolicy first before updating.
upvoted 1 times

st2023 1 year, 8 months ago
What does the command look like:
Set-EmailAddressPolicy -Identity "Office 365 Groups" -EnabledEmailAddressTemplates "SMTP:@contoso.com","smtp:@contoso.onmicrosoft.com","smtp:@contoso.microsoftonline.com"
https://learn.microsoft.com/en-us/powershell/module/exchange/set-emailaddresspolicy?view=exchange-ps#example-3
Command:
https://learn.microsoft.com/en-us/powershell/module/exchange/set-emailaddresspolicy?view=exchange-ps#-enabledemailaddresstemplates
upvoted 2 times

vanr2000 1 year, 9 months ago
Selected Answer: D
You first need to apply the Set-EmailAddressPolicy. This will apply to any new account you create.
If you want to apply the policy to the existing accounts, after you use the Set-EmailAddressPolicy cmdlet to modify an email address policy in an on-premises Exchange organization, you need to use the Update-EmailAddressPolicy cmdlet to apply the updated policy to recipients.

https://learn.microsoft.com/en-us/powershell/module/exchange/set-emailaddresspolicy?view=exchange-ps
upvoted 2 times

Feyenoord 1 year, 10 months ago
Selected Answer: A
After you use the Set-EmailAddressPolicy cmdlet to modify an email address policy in an on-premises Exchange organization, you need to use the Update-EmailAddressPolicy cmdlet to apply the updated policy to recipients.
upvoted 1 times

Feyenoord 1 year, 10 months ago
I am wrong, please delete my comment, answer given is correct, update emailadres policy is not available in EOL
upvoted 2 times

Don123 1 year, 11 months ago

D. Set-EmailAddressPolicy

To make sure that the primary email address of all new mailboxes uses the new domain in Exchange Online, you should run the Set-EmailAddressPolicy cmdlet. This cmdlet is used to modify the email address policies in your Exchange Online organization.

upvoted 1 times

Startkabels 2 years ago

Selected Answer: D

Correction D

upvoted 1 times

Cisco 2 years, 3 months ago

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

upvoted 3 times

Tibo49100 2 years, 8 months ago

Wrong answer, command only available for O365 groups

upvoted 2 times

Wojer 3 years ago

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

upvoted 4 times

Wojer 3 years, 1 month ago

in EOL is available only for groups

upvoted 2 times

marcomartinez 3 years, 1 month 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 2 times

sabin001 3 years, 1 month 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 UpdateEmailAddressPolicy cmdlet is used to apply an email address policy to users.

upvoted 3 times

Abdoulaz 3 years, 2 months 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 3 years, 2 months ago

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

upvoted 2 times

EG_Jack 3 years, 2 months 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 3 years, 2 months ago

They are available for Exchange Online but only for groups.

upvoted 2 times

zul_n 3 years, 3 months 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 for Microsoft 365 Groups.

Set-EmailAddressPolicy
[-EnabledPrimarySMTPAddressTemplate <String>]
upvoted 4 times

Eggsamine 3 years, 2 months 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 3 years, 4 months ago
This question is totally off

You can't use that command in EXO it's only for group mailbox !!
upvoted 4 times

stoneface 2 years, 12 months ago
So what would you consider to be the answer to this question then?
upvoted 2 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

Suggested Answer: *C*

zyir Highly Voted 3 years, 2 months ago
C
It can be both Monthly and Weekly but the question says "as often you can" So its Weekly
upvoted 10 times

Adebimpeidiat Most Recent 1 year, 8 months ago
B is the answer. But it depends on how often the request comes, can come before the months ends.
upvoted 1 times

Don123 1 year, 11 months ago
Answer: C

When configuring the automatic delivery of DLP incident reports in Microsoft 365, you can set a variety of delivery schedules. Some options include:

Real-time: Reports are delivered as soon as a DLP violation occurs.

Scheduled: Reports are delivered at a specific time or on a specific schedule, such as daily or weekly.

Batched: Reports are delivered in batches, such as every hour or every six hours.

On-demand: Reports can be delivered on request, typically by a user or administrator with the necessary privileges.
upvoted 1 times

Shun80 2 years, 11 months 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 2 years, 12 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#schedule-report
upvoted 4 times

JakeH 3 years, 1 month ago
In exam today.
upvoted 4 times

Don123 3 years, 2 months ago
why is there no "Custom" in the answer.....
upvoted 1 times

zul_n 3 years, 3 months ago
C - weekly is correct
upvoted 2 times

Davidchercm 3 years, 4 months 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.

Suggested Answer: *A*

Community vote distribution

A (100%)

zul_n Highly Voted 3 years, 3 months ago

A is correct

Azure AD } Licenses | select he licenses | Licensed group

upvoted 11 times

Adebimpeidiat Most Recent 1 year, 8 months ago

A is the answer,. This is where the licenses assigned can be viewed or managed.

upvoted 1 times

Meebler 1 year, 9 months ago

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

In the Azure portal, you can view and manage licenses assigned to users and groups. By accessing the Licenses blade, you can see which users have licenses assigned through group membership and ensure that the group you are interested in is included in your results. The Microsoft 365 admin center and Products blade are not relevant for this task, and the Monitor blade in the Azure portal is focused on monitoring and analytics, rather than license management.

upvoted 1 times

Don123 1 year, 10 months ago

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

To detect all users in a Microsoft 365 subscription who have a Microsoft Office 365 license as a result of belonging to a group, you can use the Microsoft 365 admin center and navigate to the Users blade. From there, you can filter the list of users by license type and group membership to identify the users who have been assigned licenses through the specified group.

Option A (accessing the Azure portal and navigating to the Licenses blade) is not the best choice, as this blade does not provide information on group membership.

Option B (accessing the Microsoft 365 admin center and navigating to the Products blade) is also not the best choice, as this blade provides information on the available products and services, but not on group membership or license assignment.

Option C (accessing the Azure portal and navigating to the Monitor blade) is not relevant to this task, as the Monitor blade is focused on monitoring and analyzing usage and performance data for Azure services.

upvoted 1 times

ColmTheMeanie 1 year, 10 months ago

It's not D

It is in fact A, there is no guidance that i could find anywhere that says the Azure portal is not the best place to do this.

I've found several articles that indicate that the best place to manage them is in Azure.

You CAN see the group membership but you CANNOT see the members or what the group even does.

I've tested this and i can confirm it is the Azure portal.

Billing>Licenses>the license in question (E3)>licensed groups

upvoted 1 times

Don123 1 year, 11 months ago

Correct Answer: A

upvoted 1 times

pozzetttt 2 years, 4 months ago

Selected Answer: A

A. for sure

upvoted 2 times

Mthaher 2 years, 8 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 2 years, 10 months ago

Selected Answer: A

A Correct

upvoted 2 times

mikl 2 years, 11 months ago

Selected Answer: A

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

upvoted 3 times

joergsi 2 years, 11 months ago

The question is, why not users, creation of a dynamic group with all users without a license?

upvoted 1 times

Parzival 2 years, 11 months ago

Azure Portal or Azure AD Portal? There's a difference.

upvoted 1 times

Contactfornitish 2 years, 8 months 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 3 years, 1 month ago

In exam today.

upvoted 2 times

myloking 3 years, 1 month ago

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

upvoted 1 times

juuvvy 3 years, 2 months ago

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

upvoted 2 times

Contactfornitish 2 years, 8 months 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.

Suggested Answer: *B*
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/faqimporting-pst-files-to-office-365

zul_n Highly Voted 3 years, 3 months 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 completed 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 11 times

Adebimpeidiat Most Recent 1 year, 8 months ago
B is the answer. It has a 30 days maximum.
upvoted 1 times

Don123 1 year, 11 months ago
B is correct
upvoted 1 times

QuanN7 2 years, 1 month ago
Just a question out of context, why would we want to import PST to Azure and have them deleted after 30 days? What's the point of doing all this?
upvoted 1 times

waterlego 2 years, 8 months ago
Still valid, April 2022
upvoted 2 times

mikl 2 years, 11 months 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 2 years, 12 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

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

Community vote distribution
A (100%)

MikeMatt2020 Highly Voted 3 years, 2 months 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 onboard them to Intune and use Autopilot to wipe/image "existing" devices. If our devices existed in Intune, we could create a deployment profile 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 using this method...
3) An in-place upgrade will do exactly what we want
upvoted 14 times

Razuli 2 years ago
Great response thanks
upvoted 1 times

L33D Highly Voted 3 years, 1 month 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 5 times

Adebimpeidiat Most Recent 1 year, 8 months ago
A is the answer.
upvoted 1 times

amiarobot 1 year, 9 months ago
Please add <u> </u> to the underlined text for these questions
upvoted 2 times

juras 2 years ago
Answer is A
This is explained in the MS-100 exams but I believe upgrading OS versions cannot be done with the other methods it has to be an in place upgrade
upvoted 1 times

Startkabels 2 years ago
Selected Answer: A
Affirmative
upvoted 1 times

Moderator 2 years, 8 months ago

Selected Answer: A

The most logical option is an in-place upgrade, so I'd go for that. A.

upvoted 2 times

trexar 2 years, 10 months 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

Jcbrow27 3 years, 1 month 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 2 times

Marcelmikael 3 years, 1 month 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 3 years, 1 month 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 3 years, 2 months 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 3 years, 2 months ago

A is correct
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

upvoted 2 times

zul_n 3 years, 3 months ago

A is correct.

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

upvoted 1 times

HappyMudd 3 years, 3 months ago

The question states you are "deploying a Windows 10 Enterprise *image*..." an in place upgrade does not deploy an image. None of the supplied answers meet that requirment?

upvoted 1 times

rfox321 3 years, 3 months 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 "None of these meet the requirement?" - You sound unsure yourself, so why even comment to confuse people?

upvoted 7 times

xofowi5140 3 years, 2 months ago

https://docs.microsoft.com/en-us/mem/autopilot/existing-devices

upvoted 2 times

Question #12 *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.
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

Suggested Answer: *B*

Community vote distribution

B (100%)

Ronger Highly Voted 3 years, 6 months ago
federation, Smart card is the key word.
upvoted 21 times

RiTh73 Highly Voted 2 years, 10 months ago
Selected Answer: B
Federation with Active Directory federation service is the solution
upvoted 5 times

tommy_tommy09 Most Recent 2 years ago
Selected Answer: B
B
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 1 times

zul_n 3 years, 3 months ago
B is correct.

the keyword is smart card
upvoted 4 times

MartiFC 3 years, 4 months ago
We need Federation Services
upvoted 4 times

Question #13 *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.
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

Suggested Answer: *B*

zul_n Highly Voted 3 years, 3 months ago
B is correct.

the keyword is smart card
upvoted 7 times

Adebimpeidiat Most Recent 1 year, 8 months ago
B is the answer.
upvoted 1 times

MartiFC 3 years, 4 months ago
we nned Federation Services for Smart Card
upvoted 4 times

Question #14 *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.
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

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

Community vote distribution
A (100%)

BobDobolina Highly Voted 3 years, 3 months ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 7 times

Tonio77s 3 years, 2 months ago
Thanks for the correct link
upvoted 2 times

Don123 Most Recent 1 year, 11 months ago
A. Yes

Pass-through authentication and seamless SSO with password hash synchronization is a solution that enables users to authenticate to on-premises resources using the same credentials they use for cloud resources. This solution can be used to authenticate users with smart card-based certificates and also permits the use of SSO to connect to on-premises and Microsoft 365 services.
Pass-through authentication allows users to authenticate directly against on-premises Active Directory and Seamless SSO automatically signs in users when they are on their corporate devices connected to the corporate network.
Password hash synchronization syncs a hash of the users' on-premises AD password with Azure AD, enabling SSO experience for cloud services.

So overall the solution meets the goal by allowing sign in via smart card-based certificates and also permitting the use of SSO to connect to on-premises and Microsoft 365 services.
upvoted 1 times

RiTh73 2 years, 10 months ago
Selected Answer: A
Correct
upvoted 1 times

Davidchercm 3 years, 4 months ago
answer is correct
upvoted 3 times

Question #15 *Topic 1*

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.

Suggested 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 3 years, 3 months 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 32 times

rfox321 3 years, 3 months ago
Good information and resources.. Thank you
upvoted 3 times

xofowi5140 3 years, 2 months ago
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
upvoted 2 times

Itokawa Most Recent 2 years, 1 month ago

Shouldn't it be A and B, because they both have user admin roles?

upvoted 1 times

trexar 2 years, 9 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 no 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 2 years, 9 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 3 years, 1 month ago

In exam today.

upvoted 2 times

DaBummer 3 years, 3 months 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

Suggested Answer: *A*

Community vote distribution

A (100%)

MartiFC Highly Voted 3 years, 4 months ago

One active mode. A lot of in stagin mode

upvoted 15 times

emilianogalati 3 years, 4 months ago

Correct!

upvoted 4 times

Navi1411 Most Recent 1 year, 10 months ago

According to Microsoft documentation, the maximum number of Azure AD Connect servers that can be installed in an environment is two. This is because Azure AD Connect does not support load balancing or clustering, and having more than two servers can cause synchronization issues.

Therefore, the maximum amount of servers that can run Azure AD Connect in this scenario is two. It is important to note that Azure AD Connect can be installed on virtual machines to achieve redundancy and high availability.

upvoted 1 times

Don123 1 year, 11 months ago

A. 1

Azure AD Connect can only be installed on one server at a time. This is because it is responsible for synchronizing your on-premises Active Directory with Azure Active Directory, and having multiple servers running the service could cause conflicts and errors. If you need redundancy, you can set up a secondary server as a backup, but only one server can be actively running Azure AD Connect at a time.

upvoted 2 times

One111 2 years ago

Actually, Microsoft supports one active and one sarge AADC server. Technically you can install more stage servers, but it's unsupported.
>Azure AD Connect supports installing a second server in staging mode.
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#staging-server

upvoted 1 times

petersonal 1 year, 11 months ago

For your source: "It's possible to have more than one staging server when you want to have multiple backups in different datacenters." I do not seeing where it sates that multiple sate servers are unsupported.

upvoted 1 times

petersonal 1 year, 11 months ago

From* - can not edit my own post...

upvoted 1 times

trexar 2 years, 9 months ago

Selected Answer: A

correct

upvoted 2 times

Tonio77s 3 years, 2 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

Suggested Answer: *C*

Community vote distribution

D (100%)

fofo1960 Highly Voted 3 years, 2 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 Authentication Agents per tenant.
So its 40
upvoted 22 times

Turd_Reynolds Highly Voted 3 years, 6 months ago
I thought the maximum number of Agents was 40?
upvoted 12 times

Rickert 3 years, 6 months ago
Yes! Minimum of 3 and a maximun of 40
upvoted 9 times

Turd_Reynolds 3 years, 6 months ago
So then this answer should be 13 (D) shouldn't it?
upvoted 17 times

AH Most Recent 1 year, 4 months ago
The question says "which of the following is the most amount of servers that can run standalone Authentication Agents?, didn't say maximum
upvoted 1 times

markymark01977 1 year, 9 months ago
Selected Answer: D
Same as rest, D is the most in the list but max is 40
upvoted 1 times

Feyenoord 1 year, 10 months ago
Selected Answer: D
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 systems (see reference).
upvoted 1 times

st2023 1 year, 10 months ago
Selected Answer: D
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start - recommend minimum is 3 authenticating agents, and the system limit is 40 authentication agents per tenant. option D- 13 is the highest out of the four options.
upvoted 1 times

Don123 1 year, 11 months ago
A. 7

Azure AD Pass-through Authentication and Seamless SSO can be installed on a maximum of 7 servers in your environment. These servers are known as Standalone Authentication Agents and are used to authenticate your on-premises users to Azure AD. These servers are installed on-premises and communicates with the Azure AD Pass-through Authentication service to authenticate the users to Azure AD.
It is important to note that Azure AD Pass-through Authentication and Seamless SSO are different from Azure AD Connect, which is responsible for synchronizing your on-premises Active Directory with Azure Active Directory.
upvoted 2 times

PeterAth 2 years, 1 month ago
definitely 40
upvoted 1 times

NikolasFj98 2 years, 2 months ago
Selected Answer: D
D is correct - Admin pls update this answer for this question
upvoted 4 times

SkullRage 2 years, 2 months ago
Selected Answer: D
Answer is D
upvoted 5 times

RiTh73 2 years, 10 months ago
Selected Answer: D
Recommended server is 3 and the maximum is 40
upvoted 2 times

sliix 2 years, 10 months ago
Selected Answer: D
Highest possible is 40.
upvoted 2 times

Musa007 2 years, 10 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 2 times

mfaisal786 2 years, 11 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 2 years, 11 months ago
Selected Answer: D
Answer is D
upvoted 2 times

Pr9 2 years, 11 months ago
Selected Answer: D
Max limit 40
Min is 3
upvoted 2 times

Zethembiso 2 years, 11 months ago
Selected Answer: D
The most number is 13 as you can run up the maximum of 40
upvoted 2 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.

Suggested 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 3 years, 4 months 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 8 times

Olamilekinsin 3 years ago
Thank you for the link
upvoted 1 times

MartiFC Highly Voted 3 years, 4 months ago
The ask say CREATE. Not say INVITE. This is the keywork
upvoted 6 times

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

rfox321 3 years, 3 months ago
1000% correct my dude
upvoted 1 times

Nussi1108 Most Recent 1 year, 10 months ago
Nur die Rolle "Benutzeradministrator" oder "Privilegierter Administrator" kann verwendet werden, um ein Gastbenutzerkonto zu erstellen.
upvoted 1 times

Don123 1 year, 11 months ago
B. The User administrator role.

The User administrator role in Azure AD is responsible for managing user accounts, including creating, modifying, and deleting user accounts. This includes the ability to create guest user accounts, which are used to give external users access to certain resources within your tenant.
upvoted 1 times

mllerena 2 years, 3 months ago
B
https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-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 2 years, 11 months ago

Selected Answer: B

Is correct

upvoted 1 times

xyzfra 3 years 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 under Azure AD admin, and CREATE a guest user. So, INVITE and CREATE are different operations. Who knows what Microsoft is asking for in this kind of questions....

upvoted 1 times

tf444 3 years ago

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

Invite or create.

upvoted 1 times

Grudo 2 years, 11 months ago

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

upvoted 1 times

Grudo 2 years, 11 months 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 3 years, 2 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 3 years, 3 months 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 3 years, 4 months 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 2 times

Madball 3 years, 4 months 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 may have changed the default settings.

upvoted 1 times

Davidchercm 3 years, 4 months ago

is the answer correct ?

upvoted 1 times

dminerva94 3 years, 4 months 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.

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

Community vote distribution
B (64%) A (36%)

zul_n Highly Voted 3 years, 3 months 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 3 years, 3 months ago
This is correct. Read the doc people
upvoted 5 times

mfaisal786 Highly Voted 2 years, 11 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 7 times

Leo1905tti Most Recent 1 year, 5 months ago
Selected Answer: A
Somente o administrador de função privilegiada pode tornar um grupo atribuível a funções administrativas
upvoted 1 times

JFFRY 1 year, 8 months ago
Selected Answer: B
B is correct
upvoted 1 times

Meebler 1 year, 9 months ago
Checked and tested: (B)
Source : https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator
upvoted 1 times

Feyenoord 1 year, 10 months ago
Selected Answer: A
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.
upvoted 1 times

Feyenoord 1 year, 10 months ago
I think I am switching to B. If you read carefully it's a security group which is used to managing accounts with privileges. Nowhere they are mentioning something about managing a role assignable group.
upvoted 1 times

hubran 1 year, 11 months ago
Selected Answer: A
Right answer is A. The question says about the group as "... purpose of managing administrative accounts". This clearly indicates that we are talking about a roles assigned group. If you read about that in https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept, they say that "Only Global Administrators and Privileged Role Administrators can create a role-assignable group"
upvoted 1 times

Don123 1 year, 11 months ago
A. The Privileged role administrator role.

The Privileged role administrator role in Azure AD is the highest level of administrative access, and it has the ability to manage all aspects of an Azure AD tenant, including managing other administrators.
This role can be used to add a user with the Security administrator role to the security group.
The User administrator, Security administrator, and Billing administrator roles do not have the necessary permissions to manage other administrators and add them to the security group.
It is important to note that, depending on the organization's security policies, adding users to the security group with the role of Security administrator may require approval from more than one privileged role administrator.
upvoted 2 times

MicrosoftBTN 2 years, 1 month ago
Using this link
https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task
by section Users there is Create guest users Guest inviter and User administrator
upvoted 1 times

JakeLi 2 years, 1 month ago
Tested it just now. B is correct.
upvoted 2 times

richardgnz 2 years, 1 month ago
I think the answer here is A
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."
B - would be correct if they had been added to the group owners but this is not the default.
We need to assume that the default settings are in place - therefore the answer must be A
upvoted 1 times

reastman66 2 years, 1 month ago
Correct answer is B User Administrator. Seems that there is a new feature where you can do a Run As for the different roles.

For Priviledged Role , Security Administrator and Billing Administrator this is displayed when trying to add any user to a security group.

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 1 times

mllerena 2 years, 3 months 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 2 years, 4 months 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 of 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 2 years, 4 months ago

Forgot one more point as per documentation: 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 2 times

Paolo2022 2 years, 1 month ago

This is not about assigning a role to a group (which is what only the priviledged role admin and global admin can do) - but about adding an admin user to a group. That is definitely possible for a user admin.
So no further experiments - choose B!

upvoted 2 times

cluocal 2 years, 8 months ago

Selected Answer: B

B is correct.

upvoted 2 times

sandi412 2 years, 9 months ago

Tested.B is correct

upvoted 2 times

dudus999 2 years, 9 months 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 2 years, 9 months ago

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

upvoted 1 times

Question #20 *Topic 1*

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

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

Community vote distribution
C (100%)

Davidchercm Highly Voted 3 years, 4 months 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 13 times

zul_n 3 years, 3 months ago
agreed, C is correct
upvoted 5 times

devilcried Most Recent 1 year, 9 months ago
Selected Answer: C
Start-ADSyncSyncCycle
upvoted 1 times

Don123 1 year, 11 months ago
C. Start-ADSyncSyncCycle

The command you should use to make sure that the new user accounts synchronize to Azure AD in the shortest time required is "Start-ADSyncSyncCycle". This command will start a new synchronization cycle immediately, which will synchronize all changes made in Active Directory to Azure AD, including the newly created user accounts.
upvoted 1 times

k9_bern_001 2 years, 9 months ago
Correct
upvoted 2 times

joergsi 2 years, 11 months 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.

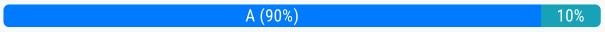
B. The user with the Password administrator role.

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

D. The user with no roles.

Suggested Answer: *A*

Community vote distribution



stromnessian Highly Voted 3 years, 5 months ago
The supplied answer is wrong. Both the global administrator and security administrator can change the password protection policy.
upvoted 13 times

rfox321 3 years, 3 months ago
Stop providing input without proof or links please.
upvoted 5 times

michszym 3 years, 5 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-protection
Prerequisites: An account with global administrator privileges.
upvoted 16 times

MomoLomo 3 years, 4 months 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 3 years, 2 months 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 3 years, 1 month ago
in both cases you must be a global admin.
upvoted 1 times

vofka Highly Voted 3 years 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 - user C has the ability to manage password protection.
upvoted 9 times

NotKnown Most Recent 1 year, 6 months ago
Selected Answer: C
Tested on my tenant, i can change the password protection policy with a account with the role security administrator
upvoted 1 times

NotKnown 1 year, 6 months ago

correct answer: A and C
upvoted 1 times

markymark01977 1 year, 9 months ago

Selected Answer: A

This question needs to be amended to allow more than one choice.
The third user has both the Security administrator and the Guest inviter roles configured. The fact they have the guest inviter role is irrelevant in this case. The question indicates the answer could be multiple "(choose all that apply)".

The answer is A and C.
Global admin has permission
Security admin has permission

The user with Password admin doesn't have permission
The user with no role assigned doesn't have permission
upvoted 1 times

Don123 1 year, 11 months ago

A. The user with the Global administrator role.
B. The user with the Password administrator role.

The Global administrator role in Azure AD has the highest level of administrative access and can manage all aspects of an Azure AD tenant, including managing password protection policies.
The Password administrator role has the ability to manage password policies such as resetting passwords, creating password policies, and more.
The Security administrator and Guest inviter roles are not related to password management and do not have the necessary permissions to alter the password protection policy.
A user with no roles configured will not have any permissions to manage or access the Azure AD tenant.
It is important to note that, depending on the organization's security policies, altering the password protection policy may require approval from more than one administrator with the Global administrator or Password administrator roles.
upvoted 2 times

One111 2 years ago

This is multiple choices question and both global admin and security admin can modify password protection policy.
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#global-administrator
upvoted 2 times

Helper2022 2 years ago

I think it is all users. It does not specifically specify that the External collaboration settings>>Guest invite settings are configured:
https://learn.microsoft.com/en-us/microsoft-365/solutions/limit-who-can-invite-guests?view=o365-worldwide

I tested this and everyone can invite (ie. create) guest accounts!
upvoted 1 times

Helper2022 2 years ago

This is WRONG! I meant it for the guest user question
upvoted 2 times

JakeLi 2 years, 1 month ago

Tested in my tenant just now. A is correct.
upvoted 2 times

Mthaher 2 years, 8 months ago

any user can send the invite if the external collaboration option is enabled
upvoted 2 times

trexar 2 years, 9 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 5 times

k9_bern_001 2 years, 9 months ago

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

upvoted 2 times

salla 2 years, 10 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 2 years, 11 months ago

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

upvoted 3 times

Wojer 2 years, 12 months ago

Checked in my azure portal and its A and C

upvoted 1 times

PDR 3 years ago

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

upvoted 4 times

tf444 3 years 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 3 years, 1 month ago

A-C for sure

upvoted 2 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.

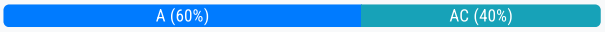
B. The user with the Password administrator role.

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

D. The user with no roles.

Suggested Answer: *AC*

Community vote distribution



examjustin Highly Voted 2 years, 8 months 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 user is enabled. Answer is only A folks.

upvoted 14 times

Paolo2022 2 years, 1 month ago

I refuse to believe that what you say is correct - that MS would not consider sending a invitation (which, when it is accepted, creates a Guest user) as a way of creating a Guest user. I know these exams are often about semantics. But this would be taking it too far, even for MS standards...

upvoted 4 times

DaDaDave 1 year, 5 months ago

Liked document confirms this interpretation, that for these purposes invite is as good as create and that the inviter role allows what is considered "create"

https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#:~:text=User%20Administrator-,Create%20guest%20user,-Guest%20Inviter

upvoted 1 times

MEG Highly Voted 2 years, 11 months 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 guest user]

upvoted 10 times

yawb 2 years, 3 months ago

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

upvoted 2 times

osxzvkwpfcfxobqjby Most Recent 1 year, 4 months ago

Selected Answer: AC

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

upvoted 1 times

kailashsahoo39 1 year, 9 months ago

Both AC are correct.
https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

upvoted 1 times

SITM 1 year, 8 months ago

But Secruity admin can´t create guest user

upvoted 1 times

Feyenoord 1 year, 10 months ago

I just tested guys, it's ABC!
https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal
upvoted 1 times

fessebook 1 year, 8 months ago
You're right if you consider that inviting a user is the same as creating a user.
Security and Password administrators can invite guest so it will create the account at the end of the process but the menu to create a guest user is greyed out for these two.
So it depends what Microsoft means by "necessary permissions to create guest users".
So i think it could be A,B,C if invite equals create or just A if invite doesn't equals create...
upvoted 1 times

st2023 1 year, 10 months ago
Selected Answer: AC
MEG's link is convincing. https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#users [Create guest user]
upvoted 2 times

suvittech 1 year, 11 months ago
https://learn.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, such as the Global Administrator role or a limited administrator directory role (for example, Guest inviter or User administrator).
upvoted 1 times

Don123 1 year, 11 months ago
A. The user with the Global administrator role.
C. The user with the Security administrator and Guest inviter roles. (This answer should only have Guest inviter roles) part of the answer.

The Guest inviter role in Azure AD has the ability to create and manage guest user accounts, which are used to give external users access to certain resources within the tenant.
The Global administrator and the Password administrator roles have the highest level of administrative access and can manage all aspects of an Azure AD tenant, but they are not specifically related to guest user management.
The Security administrator role is not related to guest user management and does not have the necessary permissions to create guest users.
A user with no roles configured will not have any permissions to manage or access the Azure AD tenant.
It is important to note that, depending on the organization's security policies, creating guest user accounts may require approval from more than one administrator with the Global administrator or Security administrator roles.
upvoted 2 times

Don123 1 year, 11 months ago
Tested in the lab and only A is the answer
upvoted 1 times

Baset100 1 year, 11 months ago
i just asked chatGPT and that is the Answer:
The user that has the necessary permissions to create guest users is the one that has the "Guest inviter" role configured.

Option C is the correct answer. The "Guest inviter" role is specifically designed to allow a user to create and manage guest accounts in Azure AD.

Option A and B are incorrect. The "Global administrator" and "Password administrator" roles do not include permissions to create guest users.

Option D is also incorrect, as the user with no roles configured does not have any permissions to create guest users.
upvoted 1 times

petersonal 1 year, 11 months ago
I refuse Option A (global admin) is incorrect. As Global admin open Azure AD, under manage > users > new user > invite external user.
According to this: https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#users
guest invite role is equal to guest creation. So in my opinion A is correct (and also C).
upvoted 1 times

One111 2 years ago
When you have invite user, account to s created (pending activation). You can list s ch account, delete it.
Both inviter and global admin can create guest users.
On top is f this also synchronization user can do it and normal user when tenant policy has no restrictions on b2b inviting.
upvoted 1 times

Helper2022 2 years ago

I think it is all users. It does not specifically specify that the External collaboration settings>>Guest invite settings are configured:
https://learn.microsoft.com/en-us/microsoft-365/solutions/limit-who-can-invite-guests?view=o365-worldwide

I tested this, where the Guest invite settings were not configure, and everyone can invite (ie. create) guest accounts!

upvoted 1 times

Zemansky 2 years, 1 month ago

Selected Answer: A

Guest Inviter's cannot create users.

upvoted 1 times

Pietras123 2 years, 1 month ago

Selected Answer: A

Guest inviter's can invite but not create.

upvoted 1 times

SIFISO2021 2 years, 2 months ago

A is correct

upvoted 1 times

mllerena 2 years, 3 months 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 2 times

LuisAitor 2 years, 2 months ago

Creo que te confundes. La opción buena es solo la A. En el enunciado dice "A third user has both the Security administrator and the Guest inviter roles configured" En tu link se especifica que un usuario invitado puede crear un usuario mientras tenga las funciones adicionales de "Administrador de usuarios". En el enunciado tiene permisos de Administrador de Seguridad.

upvoted 1 times

F1B3R 2 years, 3 months 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" button as a Guest inviter.
Pretty sure this is a Microsoft certified trick question

upvoted 2 times

Question #23 *Topic 1*

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.

Suggested 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_111 Highly Voted 3 years, 1 month ago
It's Set-AipServiceOnboardingControlPolicy now
upvoted 35 times

gdunlop Highly Voted 2 years, 4 months ago
Unlikely to see on exam - 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 5 times

AsthaAshik Most Recent 1 year, 10 months ago
https://learn.microsoft.com/en-us/azure/information-protection/activate-service
upvoted 2 times

NBemfica 1 year, 10 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

Don123 1 year, 11 months ago
Set-AIPAuthentication -Users Group1
upvoted 2 times

Don123 1 year, 11 months ago
The Add-AadrmRoleBaseAdministrator cmdlet is used to assign roles to users or groups in Azure Information Protection. This cmdlet can be used to assign the role of "Information Protection Administrator" to the Group1. This role allows members of the group to protect content using Azure Information Protection.

The Set-AadrmDoNotTrackUserGroup cmdlet sets the user groups that are not tracked by Azure Information Protection.
upvoted 2 times

Mthaher 2 years, 8 months ago
- Set-AipServiceOnboardingControlPolicy
https://docs.microsoft.com/en-us/azure/information-protection/activate-service#configuring-onboarding-controls-for-a-phased-deployment
upvoted 2 times

Question #24 *Topic 1*

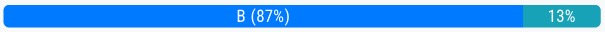
Your company has acquired Microsoft 365 for their Active Directory domain, which includes five domain controllers.
Prior to implementing a number of Microsoft 365 services, you are tasked with making use of an authentication solution that allows users to access Microsoft 365 by using their on-premises 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 password hash synchronization only.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution



MartiFC Highly Voted 3 years, 4 months ago
Correct! Password hash synchronization store password on Azure Active Directory
upvoted 9 times

lafcow 3 years, 3 months ago
Is the question asking if the password hashes are stored in Azure or the passwords ? Does it change the answer ?
upvoted 3 times

BenimAdim 3 years, 2 months ago
Passwords are never stored in Cloud, just hashes are. Security ;).
upvoted 6 times

dumpmaster 3 years, 1 month ago
Yes, but the point is use the on-premises environment, for me it is B.
upvoted 1 times

rfox321 3 years, 3 months ago
Correct - question clearly states “Must be stored on-premise”
upvoted 4 times

zul_n Highly Voted 3 years, 3 months 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 8 times

marek_jazz Most Recent 1 year, 6 months ago
AAD does not store password in the cloud - it stored password Hashes in the cloud
upvoted 1 times

DeLoc 1 year, 10 months ago
Selected Answer: B
The solution of using password hash synchronization only can allow users to sign in to Microsoft 365 with their on-premises password and only uses the current server infrastructure. However, it does not meet the requirement of storing all user passwords on-premises and providing high availability. Password hash synchronization does not store actual passwords on-premises but rather a hash of the password, and it does not provide high availability for authentication. To meet these requirements, additional measures such as AD FS or pass-through authentication would be needed.
upvoted 2 times

blaghund 1 year, 10 months ago

Password hash doesn't store passwords in Azure AD, just the hashes of them.
And it's highly available (MS 365 Sing in works, when there is an occur with on-prem.)

upvoted 1 times

Don123 1 year, 11 months ago

A. Yes

Password hash synchronization is a feature of Azure AD Connect that allows for on-premises Active Directory user account passwords to be synchronized with the corresponding Azure AD user account passwords. By configuring password hash synchronization, users will be able to use their on-premises credentials to access Microsoft 365 services and their passwords will be stored on-premises.
Additionally, by making use of the current server infrastructure and configuring five domain controllers, you can ensure high availability.

upvoted 1 times

Don123 1 year, 11 months ago

The answer is A
Reason:
Yes, you should configure the use of password hash synchronization (PHS) only in order to meet the requirements stated in your task.

PHS is a feature of Azure Active Directory (Azure AD) Connect that allows you to synchronize a hashed version of your on-premises Active Directory (AD) users' passwords to Azure AD. This enables your users to authenticate to Microsoft 365 services using the same username and password they use to log on to their on-premises resources.

By configuring PHS, you can meet the requirement of allowing users to access Microsoft 365 services using their on-premises credentials and storing all user passwords on-premises. Additionally, PHS can be highly available by using multiple servers in your on-premises infrastructure, and allows you to leverage your existing server infrastructure without the need for additional hardware or software.

upvoted 1 times

One111 2 years ago

Selected Answer: B

ADDS something store hashes of password, nota plain text passwords. But in this description they use "password stored onprem only". We can assume that in this case password equals hash. So syncing hashes of hashes is not acceptable.
This would require PtA installed on all DCs.

upvoted 1 times

KakTak 2 years ago

Selected Answer: A

This could be A because Password Hash sync is not storing passwords in cloud. It is storing just hash which is not a real password. You cannot convert hash to password. Users would still use on-prem for authentication and they have 5 DC's which will provide HA. So I will go for A

upvoted 1 times

[Removed] 2 years, 3 months ago

answer is NO means B.

upvoted 2 times

trexar 2 years, 9 months ago

Selected Answer: B

the password is onpremise and the password hash is on the cloud.

upvoted 2 times

joergsi 2 years, 11 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 try 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

joergsi 2 years, 11 months 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 2 years, 10 months 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 2 years, 11 months ago
Selected Answer: B
Stored ONLY on premises, so there shouldn't be any password syncronisation with AAD
upvoted 2 times

tf444 3 years ago
the answer is PTA , not PHS.
upvoted 2 times

natazar 3 years 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 4 times

Stiobhan 3 years, 1 month 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 rainbow table to get the decrypted password. The only solution to this question would be to use pass-through authentication or federated services.
upvoted 2 times

Question #25 *Topic 1*

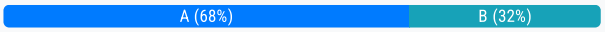
Your company has acquired Microsoft 365 for their Active Directory domain, which includes five domain controllers.
Prior to implementing a number of Microsoft 365 services, you are tasked with making use of an authentication solution that allows users to access Microsoft 365 by using their on-premises 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

Suggested Answer: *B*

Community vote distribution



Stiobhan Highly Voted 3 years, 1 month 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 13 times

Durden871 2 years, 10 months 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 still need to install two more authentication agents which I don't see anywhere else in this question. The question is asking, how do you do this and provide HA. The solution specifically says, "only enable PTA".

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

upvoted 3 times

fofo1960 Highly Voted 3 years, 2 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 2 years, 12 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 2 years, 12 months ago

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

upvoted 1 times

Paolo2022 2 years, 1 month ago

Well, the suggested answer doesn't mention agents - so how do you know that any agents are installed? ;-) It might be 1 or 2 or 3, it doesn't say... So I think your argument doesn't hold here.

upvoted 2 times

DaDaDave Most Recent 1 year, 5 months ago

Selected Answer: B

Pass Through is PART of the solution, but HA is needed to achieve goal but not states as implemented

upvoted 1 times

BigStan82 1 year, 9 months ago

Selected Answer: A

100% A

upvoted 1 times

Feyenoord 1 year, 10 months ago

Selected Answer: B

100% B while PTA is indeed correct you still need to install at least 2 agents. Since they talk about enabling PTA only it is not enough!

upvoted 1 times

DeLoc 1 year, 10 months ago

Selected Answer: A

Yes, the solution of using pass-through authentication only meets all the requirements of the task, including allowing users to access Microsoft 365 with their on-premises credentials, storing all user passwords on-premises, and providing high availability for authentication.

upvoted 1 times

Nussi1108 1 year, 10 months ago

Selected Answer: A

Ja, die Verwendung der Pass-Through-Authentifizierung kann die Ziele erfüllen. Die Pass-Through-Authentifizierung ermöglicht es Benutzern, sich mit ihren lokalen Anmeldeinformationen bei Microsoft 365 anzumelden, indem sie ihre Anmeldeinformationen an den lokalen Domänencontroller weiterleiten. Die Kennwörter werden nur lokal gespeichert und die aktuelle Serverinfrastruktur wird genutzt, um eine hohe Verfügbarkeit zu gewährleisten.

upvoted 1 times

Don123 1 year, 11 months ago

A. Yes, the solution of configuring pass-through authentication meets the goal of allowing users to access Microsoft 365 by using their on-premises credentials, utilizing the current server infrastructure, and ensuring that all user passwords are stored on-premises and highly available. Pass-through authentication allows for on-premises Active Directory credentials to be verified directly against the on-premises Active Directory, rather than syncing the credentials to Azure Active Directory. This way, it meets the requirement of storing the passwords on-premises and being highly available.

upvoted 1 times

hubran 1 year, 11 months ago

Selected Answer: B

Consider the wording here. They say: "You configure PTA ONLY". This means by just enabling PTA without doing anything else, high availability won't be reached

upvoted 2 times

gbartumeu 1 year, 11 months ago

Selected Answer: B

Not only PTA but PTA with password hash

upvoted 2 times

urbanmonk 2 years, 2 months ago

If we consider high availability which the question emphazises, PTA only does not meet this requirement. So the answer is correct - NO
"If you plan to deploy Pass-through Authentication in a production environment, you should install additional standalone Authentication Agents. Install these Authentication Agent(s) on server(s) other than the one running Azure AD Connect. This setup provides you with high availability for user sign-in requests."
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start#step-4-ensure-high-availability

upvoted 1 times

gdunlop 2 years, 4 months ago

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

upvoted 2 times

Mea988 2 years, 10 months ago

Selected Answer: A

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

upvoted 1 times

joergsi 2 years, 11 months ago

Selected Answer: B

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

upvoted 2 times

alex_p 2 years, 10 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 2 years, 11 months 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 2 times

joergsi 2 years, 11 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 forest try 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 2 years, 12 months ago
You configure the use of pass-through authentication only?
Needs SSO!
B is correct.
upvoted 1 times

Davidchercm 2 years, 12 months ago
i would choose no as no sso
upvoted 1 times

Question #26 *Topic 1*

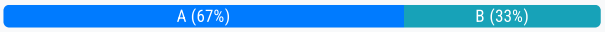
Your company has acquired Microsoft 365 for their Active Directory domain, which includes five domain controllers.
Prior to implementing a number of Microsoft 365 services, you are tasked with making use of an authentication solution that allows users to access Microsoft 365 by using their on-premises 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

Suggested Answer: *A*

Community vote distribution



MikeMatt2020 Highly Voted 3 years, 2 months 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 9 times

TimurKazan Highly Voted 3 years, 3 months ago

correct, PTA is also considered as highly available by Microsoft

upvoted 6 times

bake73 2 years, 12 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 4 times

Mea988 2 years, 10 months 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 in this case

upvoted 8 times

osxzvkwpfcfxobqjby Most Recent 1 year, 4 months ago

Selected Answer: A

PTA is de correct answer, do not over complicate your answers. It does not state "you configure PTA half-way". If you configure PTA you install at least one agent, so you can also install more agents. "only" can also refer to SSO or something else.

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

upvoted 1 times

proxyma93 1 year, 7 months ago

Selected Answer: A

It's PTA vs PHS, so it's PTA

upvoted 2 times

ijarosova 1 year, 9 months ago

I vote B. By configuring PTA and SSO, users will be able to access Microsoft 365 services using their on-premises credentials without having to enter their credentials again.

upvoted 1 times

Meebler 1 year, 9 months ago

Pass-through authentication and seamless single sign-on (SSO) provide a comprehensive solution for enabling users to access Microsoft 365 services using their on-premises credentials. With pass-through authentication, user sign-in credentials are verified against the on-premises Active Directory, providing a secure and highly available authentication method. User passwords are not stored in the cloud, ensuring that they remain on-premises.

Seamless SSO further simplifies the user experience by allowing users to access Microsoft 365 services without having to enter their credentials again. This is accomplished through the use of Kerberos authentication, which enables the user's on-premises credentials to be used for authentication to Microsoft 365 services.

Both pass-through authentication and seamless SSO can be implemented using the current server infrastructure, without the need for additional hardware or software. This makes it a cost-effective solution for enabling secure and seamless access to Microsoft 365 services.

Therefore, this is the best answer.
upvoted 2 times

Meebler 1 year, 9 months ago

While Pass-through Authentication (PTA) provides a secure authentication method, users must still enter their credentials each time they sign in to Microsoft 365 services. This can be inconvenient for users and may increase the risk of credential phishing attacks.

In contrast, seamless Single Sign-On (SSO) provides a more user-friendly experience by allowing users to access Microsoft 365 services without having to re-enter their credentials. This is achieved through the use of Kerberos authentication, which allows users to authenticate to Microsoft 365 services using their on-premises credentials without being prompted to enter their username and password.

Implementing PTA with seamless SSO provides the best of both worlds by providing a secure authentication method and a convenient user experience. It also eliminates the need for users to remember multiple sets of credentials for on-premises and cloud-based services.

Therefore, PTA with seamless SSO is better than just PTA because it provides a better user experience, while maintaining security and reducing the risk of credential phishing attacks.
upvoted 1 times

Feyenoord 1 year, 10 months ago

Selected Answer: B

100% B while PTA is indeed correct you still need to install at least 2 agents. Since they talk about enabling PTA only it is not enough!
upvoted 1 times

ColmTheMeanie 1 year, 10 months ago

When you enable password-based SSO for an application, Azure AD collects and securely stores usernames and passwords for the application. User credentials are stored in an encrypted state in the directory. Password-based SSO is supported for any cloud-based application that has an HTML-based sign-in page

Although the above does relate to app passwords, it would open up the possibility for credential storage in Azure so i would say no
upvoted 2 times

Don123 1 year, 11 months ago

A. Yes
The solution of configuring pass-through authentication and seamless SSO meets the goal of allowing users to access Microsoft 365 by using their on-premises credentials, utilizing the current server infrastructure, and ensuring that all user passwords are stored on-premises and highly available. Pass-through authentication allows for on-premises Active Directory credentials to be verified directly against the on-premises Active Directory, rather than syncing the credentials to Azure Active Directory. Seamless SSO provides a way for users who are already signed in to their on-premises network to be automatically signed in to their cloud-based resources without having to enter their password again. This way, it meets the requirement of storing the passwords on-premises, being highly available and providing a seamless experience for the end user.
upvoted 1 times

Baset100 1 year, 11 months ago

B. No, the solution does not meet the goal.

Pass-through Authentication (PTA) and Seamless Single Sign-On (SSO) are features of Azure AD Connect that allows users to authenticate against on-premises Active Directory using their on-premises credentials when accessing cloud-based resources and also allow for a Single Sign-On (SSO) experience for the users.

While PTA does allow for on-premises credentials to be used and passwords to be stored on-premises, the use of Seamless SSO would allow for users to be authenticated automatically when signing in to Azure AD, without having to enter their credentials again. This would require the user's password hash to be stored in Azure AD which violates the requirement of having the passwords stored only on-premises.

It's important to note that, it's possible to achieve SSO experience without storing the password hash in Azure AD, but that would require additional components, such as ADFS or another third-party identity provider.

upvoted 3 times

Don123 1 year, 11 months ago

It is possible that the solution of using pass-through authentication and seamless SSO meets the goal, as it allows users to access Microsoft 365 by using their on-premises credentials, without the need for additional servers or infrastructure. Pass-through Authentication (PTA) is a feature of Azure Active Directory Connect that allows users to authenticate to Azure AD by validating their credentials against on-premises Active Directory. Seamless SSO is a feature of Azure AD Connect that provides a single sign-on experience to users that are signed in to their on-premises domain-joined devices. With this solution, user's passwords are only stored on-premises and users can access to Microsoft 365 services with the same password they use to sign in to their on-premise domain. However, it is important to note that this solution is not the only one and other factors such as environment and security considerations may play a role in determining if the solution truly meets the goal.

upvoted 1 times

One111 2 years ago

Selected Answer: A

They have 5 DCs. This is HA for onprem authentication and password storing. They must have at least 1 AADC server. We can enable PtA and install agents on all DC. All requirements fulfilled.
Seamless SSO does not change anything.

upvoted 1 times

areis 2 years, 1 month ago

If configuring PTA only doesn't meet the goal, configuring PTA w/ SSO will definitely not either.
I'll go to No for both coz both solutions don't meet the requirement of being highly available, install more than 1 PTA agent is missing.

upvoted 2 times

Contactfornitish 2 years, 8 months 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't change a thing so A is right

upvoted 3 times

trexar 2 years, 9 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 2 years, 11 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 3 times

Durden871 2 years, 10 months ago

The previous question said enabling the feature of PTA only. This is talking of configuring PTA with SSO, but doesn't use the delimiter of "Only". These questions are awful. Even with these study aides I'm incredibly confused.

upvoted 3 times

Bulldozzer 2 years, 11 months ago

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

upvoted 2 times

tf444 3 years 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

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

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

Community vote distribution
B (100%)

hussain2000 Highly Voted 2 years, 8 months ago
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert
upvoted 6 times

BigStan82 Most Recent 1 year, 9 months ago
Selected Answer: B
90 days
upvoted 1 times

Don123 1 year, 11 months ago
B. 90 days.
Once a tenant user submits a fraud alert for their account, the Block user when fraud is reported setting will automatically block their account for a default period of 90 days, this is to prevent any unauthorized access or activities on the account. This setting is intended to provide additional security for the tenant by automatically blocking an account when suspicious or fraudulent activity is reported.
upvoted 1 times

Question #28 *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. 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

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

Community vote distribution
A (100%)

Davidchercm Highly Voted 3 years, 4 months ago
Code to report fraud during initial greeting: When users receive a phone call to perform multi-factor authentication, 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.
upvoted 16 times

st2023 Most Recent 1 year, 10 months ago
Selected Answer: A
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert
you can scroll down to Custom voice message defaults or crtl + f "zero" or "zero pound" to find the relevant information.
upvoted 2 times

Don123 1 year, 11 months ago
A. 0
When a tenant user submits a fraud alert for their account and multi-factor authentication is enabled, the default special code that the user needs to enter when prompted in the alert call is 0 (zero) followed by #. This is a default code used as a way to verify that the user submitting the fraud alert is the actual user of the account. The user will be prompted to enter the code when receiving the alert call and the code will be used to validate the user's identity before unblocking the account.
upvoted 1 times

Suxi22 2 years, 2 months ago
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert
upvoted 2 times

simoen 2 years, 3 months ago
such a useless question...
upvoted 4 times

invaderzim48 2 years, 3 months ago
Really though, what is this designed to test other than the ability to memorize niche features.
upvoted 4 times

Razuli 1 year, 11 months ago
this is a horrible exam. At no point at all does any training give you any knowledge on this, just like most of the exam quesitons.
upvoted 1 times

Nilz76 2 years, 10 months 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

Question #29 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

FleurJ Highly Voted 3 years, 3 months ago

https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

upvoted 8 times

osxzvkwpfcfxobqjby Most Recent 1 year, 4 months ago

Selected Answer: D

D for now, but should be B & D.

Set-SPOSite -Identity https://contoso.sharepoint.com/sites/site1 -SharingCapability ExternalUserSharingOnly

https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps#-sharingcapability

upvoted 1 times

Don123 1 year, 11 months ago

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

To ensure that users are only able to invite authenticated guest users to the SharePoint sites, you should modify the sharing settings in the SharePoint admin center. Specifically, you should set the "External sharing" option to "Authenticated guests only." This will restrict external users from accessing the SharePoint sites unless they have been authenticated as a guest user. You can find this setting in the SharePoint admin center under the "Settings" menu, in the "Sharing" section.

upvoted 1 times

francklinmg 3 years, 3 months 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.

Suggested 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
D (100%)

Don123 1 year, 11 months ago
D. You should make sure that the Admins and users in the guest inviter role can invite setting is set to Yes.

To make sure that authorized users are able to create guest users in the tenant, you should ensure that the "Admins and users in the guest inviter role can invite" setting is set to "Yes."
This setting is found in the Azure AD external collaboration settings, and when it's set to "Yes," it allows users who are members of the guest inviter role or are global administrators to invite guest users to the tenant.
upvoted 1 times

MEG 2 years, 10 months 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 2 years, 10 months 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 3 years 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 3 years ago
I had in mind c need to be set to NO
upvoted 1 times

Don123 3 years, 2 months 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 3 years, 4 months 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 3 years, 3 months 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

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

Community vote distribution
B (100%)

ItsMax Highly Voted 3 years, 6 months ago
sure
complete command is:
Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods -ne $null -and $_.BlockCredential -eq $False} | Select-Object -Property UserPrincipalName
upvoted 28 times

extrankie 2 years, 12 months ago
great explanation
upvoted 2 times

emilianogalati 3 years, 4 months ago
Thank you.
I will test it later on my tenant!
upvoted 1 times

Ademar 3 years, 3 months ago
Thanks
upvoted 2 times

st2023 Most Recent 1 year, 10 months ago
Selected Answer: B
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting
upvoted 1 times

Don123 1 year, 11 months ago
B. Get-MsolUser
upvoted 1 times

Rick_James 2 years ago
Microsoft has pushed out the retirement of the Azure AD and MSOL license management cmdlets to 31 March 2023.
upvoted 1 times

Mthaher 2 years, 8 months ago
B. Get-MsolUser
upvoted 2 times

Tibo49100 2 years, 8 months ago
MSOL commands are not available in Cloud Shell so I think this question is not valid any more
upvoted 3 times

trexar 2 years, 9 months ago

Selected Answer: B

Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods -ne $null -and $_.BlockCredential -eq $False} | Select-Object -Property UserPrincipalName

upvoted 2 times

bakkus 3 years, 1 month 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 Active Directory PowerShell for Graph. We advise customers who are creating new PowerShell scripts to use the newer module instead of this module."

upvoted 3 times

Razgrad 3 years, 3 months 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 3 times

FumerLaMoquette 3 years, 3 months 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

PDR 3 years 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 particular domain in the UPN with Get-AzureADUser but the MSOL command allows you to specify with -Domain switch. Yes you can use 'Where-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 properties now only exposable via Graph API. You can use MGGraph powershell module and the Get-MgUserAuthenticationPhoneMethod to get the info via powershell also, or just graph API rest calls

upvoted 3 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

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

Community vote distribution
B (100%)

PDR Highly Voted 3 years ago
B is correct because Sign-Ins allow you to add custom filters to show access to sharepoint, using conditional access and MFA . Using other MFA reports doesnt give this kind of targeting
upvoted 6 times

Don123 Most Recent 1 year, 11 months ago
A. No adjustment required.

The underlined segment is accurate. You can view the usage reports from Azure Active Directory admin center to check who used multi-factor authentication to authenticate when accessing SharePoint after configuring a conditional access policy to force mobile device users to use MFA. Usage reports can give you information about successful and failed sign-in attempts, and you can also filter by MFA, sharepoint and mobile device.
upvoted 1 times

ColmTheMeanie 1 year, 10 months ago
That's not true
Like Henrik said
A will show you which users are required to use MFA, but
B will show you which users gained access by using MFA.
upvoted 1 times

HenriksDisciple 2 years, 9 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 3 times

Wojer 2 years, 12 months ago
Truly speaking A and B is the proper answer
upvoted 1 times

Stiobhan 3 years, 1 month 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 3 years, 1 month 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 3 years ago
agree with Khaldunazar
upvoted 1 times

sliix 2 years, 11 months 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 3 years, 3 months ago
Answer is correct
upvoted 2 times

emilianogalati 3 years, 4 months ago
Correct!
upvoted 2 times

Question #33 *Topic 1*

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.

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

Community vote distribution

YClaveria Highly Voted 3 years, 2 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 14 times

Storm 2 years, 10 months ago
Why would you assume that our sales personnel has done anything to be recognized by MS as risky users ???
upvoted 10 times

TimurKazan Highly Voted 3 years, 2 months ago
actually this is implemented in conditional access policies. I don think it has something to do with sign in risk policies regarding cloud apps
upvoted 9 times

extrankie 2 years, 12 months ago
Conditional access should be best be approach but risky policy also force MFA
upvoted 2 times

osxzvkwpfcfxobqjby Most Recent 1 year, 4 months ago
Selected Answer: D
Conditional access with session option is only working with "supported apps". So, at the moment your only option is D. To make sure it applies to all users in the group you select all options High to noRisk.

https://learn.microsoft.com/nl-nl/azure/active-directory/conditional-access/concept-conditional-access-session#application-enforced-restrictions
upvoted 2 times

Rednevi 1 year, 7 months ago
Selected Answer: C
C. You should create a session policy.

By creating a session policy, you can define and enforce specific settings for user sessions. In this case, you can configure the session policy to require multi-factor authentication for all cloud-based applications accessed by sales department users. This policy will ensure that users are prompted for an additional authentication factor when accessing these applications, enhancing security.

Creating a DLP (Data Loss Prevention) policy is not directly related to enforcing multi-factor authentication.

Creating a new app registration or a sign-in risk policy does not directly address the requirement of compelling sales department users to use multi-factor authentication for all cloud-based applications.

Therefore, the most appropriate action to achieve the specified goal is to create a session policy.
upvoted 2 times

Don123 1 year, 11 months ago
D. You should create a sign-in risk policy

To make sure that sales department users are compelled to make use of multi-factor authentication for all cloud-based applications, you should create a sign-in risk policy. A sign-in risk policy can be used to require multi-factor authentication for users based on certain conditions or risk level, such as location, device, IP address, and more. This can be done using Azure Active Directory Conditional Access in the Azure portal and you can use the cloud based subscription to apply this policy.
upvoted 2 times

Startkabels 2 years, 1 month ago
Selected Answer: B
Id vote D: Force sales uses to do MFA. Risk-policy doesnt do that cause risk is determined automatically and if there is no risk there is no MFA. I would use Conditional Access to achieve that but first you need to register those cloud apps in AzureAD to use as a condition for the policy. So apply to Sales users and apply to the registered app and always force MFA. Makes sense to me..
upvoted 1 times

Startkabels 2 years, 1 month ago
Id vote B: We need to force sales uses to do MFA for cloud apps. Risk-policy doesnt do that cause risk is determined automatically and if there is no risk there is no MFA. I would use Conditional Access to achieve it but first you need to register those cloud apps in AzureAD to use as a condition for the policy. So apply to Sales users and apply to the registered app and always force MFA. Makes sense to me..
upvoted 1 times

Monk16 2 years, 2 months ago
Answer is D

It would be conditional access policy if that was an option for sure. But as its not. You create a Sign in risk policy which which forces MFA on the user when there is no risk. Obviously this is silly as you normally use a risk policy with a risk level of medium or high and block the connection for example. But this fits best
upvoted 1 times

Pha0691 2 years, 3 months ago
Risk-based policies
If your organization uses Azure AD Identity Protection to detect risk signals, consider using risk-based policies instead of named locations. 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 2 years, 8 months 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 3 times

Storm 2 years, 10 months 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 level... I think we can assume that the people we have hired in out sales department are not doing impossible travel, logging in from unknown Ip's or other stuff that would make them risky...
The correct answer should be conditional access policy...
upvoted 7 times

HenriksDisciple 2 years, 9 months ago
This is the truth.
upvoted 1 times

Frede 2 years, 9 months ago
You are correct Sir!
upvoted 1 times

joergsi 2 years, 11 months 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 locations. 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 3 years, 3 months 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 the 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 3 years, 3 months 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 2 years, 11 months 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

NrdAlrt 1 year, 5 months ago
Actually, yes we do. Even E3 includes Azure AD Premium P1. E5 includes AADP P2. After researching all the arguments here, "Session based" is the best way to narrowly push MFA on a group for use of a specific application along a specific access vector... which is the nature of this question when you consider how much effort they went to list specifics all the way down to the specific license.
upvoted 1 times

fofo1960 3 years, 3 months ago
I am not sure that this is correct answer
upvoted 1 times

Noie 3 years, 5 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.

Suggested Answer: *C*

Community vote distribution

C (53%) D (47%)

vasyab Highly Voted 3 years, 6 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-connect-health-for-sync
upvoted 16 times

Sysadmin007 1 year, 8 months ago

The Register-AzureADConnectHealthSyncAgent cmdlet is used to register the Azure AD Connect Health Sync Agent with Azure AD. This cmdlet should be run from an Azure AD Connect server, which is responsible for synchronizing on-premises Active Directory with Azure AD.

Option A, a member server, is not specific enough as it could refer to any server that is a member of the domain.
Option B, a domain controller, is not the correct answer as it is not directly related to AD FS or Azure AD Connect.
Option D, an AD FS server, is also not the correct answer as this cmdlet is used to register the Azure AD Connect Health Sync Agent, not to configure AD FS user authentication auditing
upvoted 1 times

lamrandom Highly Voted 2 years, 12 months ago

I think AD Connect server is the correct one.
The command is "Register-AzureADConnectHealthSyncAgent" and not "Register-AzureADConnectHealthADDSAgent or Register-AzureADConnectHealthADFSAgent".

Also Register-AzureADConnectHealthSyncAgent is recommended when the registration fails after you install AD Connect (see here https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#manually-register-azure-ad-connect-health-for-sync)

Also, we can see the difference in prerequisites when it's clearly distinguished the agent for Sync, for ADDS and ADFS:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#install-the-agent

I would go for C too.
upvoted 12 times

GetEsn Most Recent 1 year, 3 months ago

Selected Answer: C

Your AD FS server should be separate from your sync server. Don't install the AD FS agent on your sync server.
upvoted 1 times

osxzvkwpfcfxobqjby 1 year, 4 months ago

Selected Answer: D

You must audit ADFS logs, so you install the agent on the ADFS server. AD Connect is not installed at all. So you start the command from the ADFS server.

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

ijarosova 1 year, 9 months ago
Vote C - You will need to install the Azure AD Connect Health Sync Agent on the server that is running the Azure AD Connect tool.
upvoted 2 times

Paolaj1 1 year, 10 months ago
Guess D is the valid option: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#install-the-agent-for-ad-fs Later the article refers to manual registration.
upvoted 1 times

Paolaj1 1 year, 10 months ago
My mistake, should read better other answers.. C should be the valid option (due to command name), sorry for confusion.
upvoted 1 times

DeLoc 1 year, 10 months ago
Selected Answer: C
The Register-AzureADConnectHealthSyncAgent cmdlet is used to register the Azure AD Connect Health Sync Agent with Azure AD. It should be run on the server that is hosting the Azure AD Connect Health Sync Agent. Therefore, the correct answer is C, "an Azure AD Connect server".

A. A member server or domain controller is not the correct server to run the cmdlet on as they are not the servers hosting the Azure AD Connect Health Sync Agent.

B. While it is possible to install the Azure AD Connect Health Sync Agent on a domain controller, it is not recommended for security reasons. Therefore, it is not recommended to run the cmdlet on a domain controller.

D. AD FS is a separate service from Azure AD Connect and is not directly related to the Azure AD Connect Health Sync Agent. Therefore, it is not recommended to run the cmdlet on an AD FS server.
upvoted 3 times

Don123 1 year, 11 months ago
C. An Azure AD Connect server.
D. An AD FS server.

The Register-AzureADConnectHealthSyncAgent cmdlet should be run from an Azure AD Connect server and an AD FS server.
Azure AD Connect is the tool that enables you to synchronize your on-premises Active Directory with Azure AD. To monitor the health of AD FS and Azure AD Connect synchronization, you can use Azure AD Connect Health. By running the Register-AzureADConnectHealthSyncAgent cmdlet on the Azure AD Connect server and AD FS server, you can register these servers with Azure AD Connect Health and enable auditing and monitoring of user authentication.
upvoted 2 times

minasamy 2 years ago
answer is : C.
tested
upvoted 2 times

One111 2 years ago
Selected Answer: C
Cmdlet is only for a AADC.
upvoted 2 times

mllerena 2 years ago
You are preparing to run the Register-AzureADConnectHealthSyncAgent cmdlet.
Register-AzureADConnectHealthADFSAgent -> ADFS
Register-AzureADConnectHealthADDSAgent -> ADDS
Register-AzureADConnectHealthSyncAgent -> Azure Ad Connect

https://learn.microsoft.com/es-es/azure/active-directory/hybrid/how-to-connect-health-agent-install#register-the-agent-by-using-powershell
Answer is correct C
upvoted 4 times

ZeTonio 2 years ago

Selected Answer: D

AD Connect automatically installs health agent, so there's no need to run the register cmdlet like the question states. In the other hand, you can manually install the healthagent in ADFS and thus have the need to run the register cmdlet.

upvoted 1 times

Paolo2022 2 years, 1 month ago

Selected Answer: C

I do find the sources slightly confusing, but I believe that C (Azure AD Connect server) is the correct answer.
The agent is normally configured during the installation of Azure AD Connect - on the server where that installation takes place. In case things don't work properly after installation, it is possible to manually register the health agent afterwards. Any other context apart from the Azure AD Connect server to run this cmd doesn't make sense then, I think.

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

upvoted 1 times

Paolo2022 2 years, 1 month ago

Ok, this turns out to be wrong - D is 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."

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

upvoted 4 times

NrdAlrt 1 year, 5 months ago

The question is a sneaky one if this was captured and shared correctly for this dump. You need to read the cmdlet that is being run carefully in this question. This cmdlet is for AAD Connect, not ADFS, so you'd only run it on an AADC server regardless of what you are intending to do.

You are preparing to run the Register-AzureADConnectHealthSyncAgent cmdlet.
Register-AzureADConnectHealthADFSAgent -> ADFS
Register-AzureADConnectHealthADDSAgent -> ADDS
Register-AzureADConnectHealthSyncAgent -> Azure Ad Connect

upvoted 1 times

Pietras123 2 years, 1 month ago

Selected Answer: C

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#manually-register-azure-ad-connect-health-for-sync

upvoted 1 times

LuisAitor 2 years, 1 month 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.

https://learn.microsoft.com/es-es/azure/active-directory/hybrid/how-to-connect-health-agent-install#install-the-agent-for-ad-fs

upvoted 2 times

Paolo2022 2 years, 1 month ago

Thanks for your comment! The reference doesn't match your quote, but the information given is the key for this answer.

The source is: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#requirements

upvoted 1 times

Harry83 2 years, 2 months ago

Selected Answer: C

According to the documentation, it's possible to deploy the agent to an ADFS Server. But in this scenario, the cmdlet is slightly different: Register-AzureADConnectHealthADFSAgent.

Therefore, the Register-AzureADConnectHealthSyncAgent cmdlet only apply to an Azure AD Connect Server.

Answer is C.

Source: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#install-the-agent-for-ad-fs

upvoted 3 times

cscorrupt 2 years, 2 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install states: "Your AD FS server should be different from your Sync server. Don't install the AD FS agent on your Sync server."

upvoted 2 times

Question #35 *Topic 1*

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

Suggested Answer: *A*

zul_n Highly Voted 3 years, 3 months ago
A is correct
upvoted 5 times

Don123 Most Recent 1 year, 11 months ago
A. No adjustment required

The underlined segment is accurate. To make sure that multi-factor authentication is compulsory only for users in the office houses the R&D department, you can create a conditional access policy using Azure Active Directory. Conditional access policies allow you to set specific conditions for access to cloud-based resources, such as requiring multi-factor authentication for users from a specific location or department. Therefore this is the correct action to take for this scenario.
upvoted 1 times

Wojer 2 years, 11 months ago
security -> conditional access -> create policy
upvoted 1 times

YClaveria 3 years, 2 months 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 3 times

Question #36 *Topic 1*

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

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

Community vote distribution
B (100%)

NrdAlrt 1 year, 5 months ago
B is correct. In reality, I'd tackle this with an smtp transport rule actually. It does not specify the user is external, so the email wouldn't necessarily even pass through spam filtering. I did this before as a O365 arch for a security incident where we had to find any additional compromised accounts attempting to send out emails with certain keywords/subjects etc.
upvoted 1 times

Rednevi 1 year, 7 months ago
Selected Answer: B
The solution of creating a spam filter policy via the Security & Compliance admin center does not meet the goal of keeping a duplicate of all email messages from a specified user that includes a specific word.

B. No.

A spam filter policy is used to manage and filter unwanted or malicious emails, typically based on specific criteria such as sender, subject, or content. It is not designed to keep a duplicate of all email messages or perform content-based filtering for specific words.

To achieve the goal of keeping a duplicate of all email messages from a specified user that includes a specific word, an alternative solution would be required. One possible solution could involve using features such as eDiscovery or journaling in Microsoft Exchange Online to capture and store the desired email messages based on the specified criteria.
upvoted 1 times

Don123 1 year, 11 months ago
B. No

The solution described in the statement does not meet the goal of keeping a duplicate of all email messages from a specified user that includes a specific word.
A spam filter policy is used to identify and block unwanted email messages, it is not the right solution to keep a duplicate of all email messages from a specified user that includes a specific word.
A possible solution to meet the goal would be to create an In-Place eDiscovery & Hold in Exchange Online
upvoted 1 times

BigDazza_111 1 year, 8 months ago
what about creating spam policy that forwards emails as BCC to specific user. Wouldnt this be a duplicate?
upvoted 1 times

Rednevi 1 year, 7 months ago
This is correct but i don't know if counts as a correct answer
upvoted 1 times

DoctorCOmputer 2 years, 1 month ago
It"s A ofcourse we can create policy for specific words.
upvoted 1 times

Mercious 2 years, 3 months ago

The answer is right

upvoted 3 times

Question #37 *Topic 1*

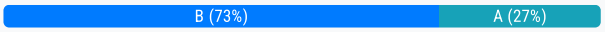
Your company has configured all user email to be stored in Microsoft Exchange Online.
You have been tasked with keeping a duplicate of all the email messages from a specified user that includes a specific word.
Solution: You start by initiating a message trace via the Security & Compliance admin center.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

A. Yes

B. No

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

Community vote distribution



Don123 1 year, 11 months ago

B. No

The solution described in the statement does not meet the goal of keeping a duplicate of all email messages from a specified user that includes a specific word.
A spam filter policy is used to identify and block unwanted email messages, it is not the right solution to keep a duplicate of all email messages from a specified user that includes a specific word.
A possible solution to meet the goal would be to create an In-Place eDiscovery & Hold in Exchange Online

upvoted 1 times

KnightOfH 1 year, 11 months ago

Selected Answer: B

correct

upvoted 1 times

neeewbi 2 years, 3 months ago

Selected Answer: B

correct

upvoted 3 times

ajiejeng 2 years, 4 months ago

Selected Answer: B

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

upvoted 4 times

Wesje 2 years, 10 months ago

Selected Answer: A

duplicate

upvoted 3 times

Question #38 *Topic 1*

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

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

Fcnet Highly Voted 3 years, 5 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 6 times

Downstar 2 years, 1 month ago
Exactly. We use in auto apply policy for an label with sensitive info like I'd card numbers etc.
It sets an retention Policy for 5 years on it automatically.
upvoted 1 times

NrdAlrt Most Recent 1 year, 5 months ago
This answer has me scratching my head. I can't find anywhere where an AIP label retains email in a repository or otherwise. For data retention(not protection/encryption), Exchange Online has multiple options for archival of email messages. I personally would create an ediscovery case and capture those emails where they can be easily accessed. If the issue is more awareness(like monitoring of these emails), you can create a transport rule in EXO that can create copies in whatever manner you prefer to whatever mailbox.
upvoted 2 times

Don123 1 year, 11 months ago
A.YES

A label and label policy are used to classify and protect sensitive information in emails, it is the right solution to keep a duplicate of all email messages from a specified user that includes a specific word.
upvoted 2 times

joergsi 2 years, 11 months 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 select 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 (SSN). 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 3 times

Storm 1 year, 7 months ago
Where is the copy saved ?
upvoted 2 times

Question #39 *Topic 1*

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.

Suggested Answer: *D*
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/supervision-policies

Community vote distribution
D (100%)

ExamTraining24 Highly Voted 2 years, 11 months ago

Selected Answer: D

Outdated question as Supervisor Policies are now deprecated and replaced with the Communication Compliance Policy... But D is the only option here.
upvoted 10 times

Don123 Most Recent 1 year, 11 months ago

C. DLP Policy

A DLP policy should be created in order to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The DLP policy can be configured to scan messages sent from the Support group to external users and identify messages with attachments. Additionally, the DLP policy can be set to only allow the manager access to 10 percent of the messages, meeting the requirement for random review of a limited number of messages.
upvoted 1 times

NrdAlrt 1 year, 5 months ago

I can't find anywhere that a DLP policy, made for classifying and protecting data, can set a threshold of only acting on 10% of messages. This sounds like Purview and Communication Compliance Policy, 100%.
upvoted 1 times

Glorence 2 years, 11 months 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 3 times

Stiobhan 3 years ago

Yeah, it should state a communication-compliance policy - https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide
I guess Supervision Policy would be the closest answer here.
upvoted 3 times

Jcbrow27 3 years, 1 month ago

It is a comunication policy, i think.
upvoted 1 times

Question #40 *Topic 1*

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

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

Community vote distribution
A (100%)

osxzvkwpfcfxobqjby 1 year, 4 months ago

Selected Answer: A
Use the Unsanctioned tag

https://learn.microsoft.com/en-us/defender-cloud-apps/risk-score#overriding-the-risk-score
upvoted 1 times

Don123 1 year, 11 months ago

B. a label
upvoted 2 times

hufflepuff 2 years, 2 months ago

App tags: Tags enable you to customize the Cloud App Catalog. You can select from either Sanctioned, Unsanctioned, or create custom tags for apps. These tags can then be used as filters. Filters are useful for deeper diving into specific types of apps that you want to investigate.

Creating and managing custom app tags
You can create a custom app tag. These tags can then be used as filters for deeper diving into specific types of apps that you want to investigate. For example, custom watch list, assignment to a specific business unit, or custom approvals, such as "approved by legal". App tags can be also used in app discovery policies in filters or by applying tags to apps as part of the policy governance actions.
upvoted 2 times

hopalong 2 years, 3 months 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 3 times

Paolo2022 2 years, 1 month ago

A is definitely correct, see the source that Nastha has provided: https://learn.microsoft.com/en-us/defender-cloud-apps/discovered-app-queries#creating-and-managing-custom-app-tags
upvoted 1 times

NrdAlrt 1 year, 5 months ago

You are awesome for linking. I think you're correct here because you read the details. Yes, you can sanction an app but it won't effect the "risk score" which is what this question is asking us to address specifically. I'd say the broad impact of adjusting how risk is tabulated might be overly broad, but they mention other apps being impact by this so kind of suggests this is something that is unwanted as a risk negative more broadly. Also you can individually override apps to assign whatever score you want, so that would achieve desired goal too with D.

upvoted 1 times

Nastha 3 years ago

I think the correct URL is:-
https://docs.microsoft.com/en-us/defender-cloud-apps/discovered-app-queries

upvoted 2 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

Suggested Answer: *C*
References:
https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365

Community vote distribution
C (100%)

MomoLomo Highly Voted 3 years, 5 months ago
maximum number of 2000
maximum -recommended- number 150
upvoted 19 times

Bobalo Highly Voted 3 years, 5 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 17 times

[Removed] 2 years, 10 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 you just say recommended, that makes it sound like it has to be exactly 150, no more no less, for the recommended number, which would 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 4 times

JCkD4Ni3L Most Recent 1 year, 8 months ago
Selected Answer: C
RECOMMENDED = 150
upvoted 1 times

Don123 1 year, 11 months ago
maximum -recommended- number 150
keyword - recommended
upvoted 1 times

Don123 1 year, 11 months ago
A. 2,000
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 1 times

Genius1289 2 years, 8 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 2 times

kanag1 2 years, 11 months ago

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

upvoted 2 times

mfaisal786 3 years ago

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

upvoted 3 times

sabin001 3 years, 1 month ago

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

So answer will be 2000

upvoted 1 times

Fcnet 3 years, 5 months ago

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

upvoted 2 times

jnashville 3 years, 6 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 3 years, 6 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 3 years, 1 month ago

recommended for 150 though, not maximum

upvoted 3 times

cloudboys 3 years, 6 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 3 years, 6 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 3 times

larnyx 3 years, 6 months ago

The correct answer is A - 2000.

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

upvoted 1 times

vasyab 3 years, 6 months ago

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

upvoted 3 times

subbuhotmail 3 years, 5 months ago

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

upvoted 1 times

Question #42 *Topic 1*

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.

Suggested 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

Community vote distribution
B (100%)

Feyenoord 1 year, 10 months ago

Selected Answer: B

Since I cannot create a .exe file I'm gonna go with XML.
upvoted 3 times

Don123 1 year, 11 months ago

The type of file that you should create is a XML Configuration file.
You can create a network share for Office 365 ProPlus installation and configure it using the XML Configuration file to specify the installation options, including preventing the installation from using the Internet. The XML Configuration file can be used to deploy Office 365 ProPlus to all users in your organization via the network share.
upvoted 1 times

Don123 1 year, 11 months ago

B. An XML download file.
D. An EXE download file.
upvoted 1 times

ARZIMMADAR 1 year, 11 months ago

So is it XML and EXE or just XML? please guys minimize confusion
upvoted 1 times

joergsi 2 years, 11 months 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 should 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 3 times

gxsh 3 years, 2 months ago

Definitively .xml file, so answer is correct.
upvoted 3 times

Rickert 3 years, 4 months ago

Should be XLM & Exe IMHO

upvoted 4 times

emilianogalati 3 years, 4 months ago

You know how to create a .exe file, don't you?

I don't. ;)

Jokes apart, I think the keypoint is "create".

upvoted 8 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

Suggested 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 3 years, 6 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 11 times

zul_n Highly Voted 3 years, 3 months ago
C is correc
• Targeted : SemiAnnualReview / next semi-annually channel release
• broad : semiannual
• Monthly : current / current channel
• Insiders : CurrentPreview channel
upvoted 6 times

Don123 Most Recent 1 year, 11 months ago
The frequency of feature updates for Office 365 ProPlus with the Channel attribute for the OfficeClientEdition attribute set to Broad and the Channel attribute for the Updates element set to Targeted will occur Monthly.

The Channel attribute for the OfficeClientEdition attribute sets the type of Office 365 ProPlus installation, and when set to Broad, it will receive Monthly feature updates. The Channel attribute for the Updates element controls the frequency of updates for Office 365 ProPlus, and when set to Targeted, it will receive updates on a monthly basis.
upvoted 2 times

mfaisal786 3 years ago
Previous attribute value: Broad
New attribute value: SemiAnnual
upvoted 4 times

davem90 3 years, 1 month 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 3 years, 3 months ago
All these answers are so correct MY guy
upvoted 3 times

1ewj7 3 years, 4 months 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

Suggested 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 3 years, 3 months ago
I hate this kind of "memorize" question, we should be tested in Key features of Microsoft 365 and AzureAD and not these stupid questions.
upvoted 30 times

xelirec 3 years ago
wth is the learning goal with this question right? no sense at all.
upvoted 7 times

[Removed] 2 years, 10 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 4 times

NrdAlrt 1 year, 5 months ago
I can't tell you how many times I had to break this down for my desktop management folks and other people across IT that had a vested interest in knowing when these major updates were coming.
upvoted 1 times

stromnessian Highly Voted 3 years, 5 months ago
Messed up question. Security updates are installed on a monthly basis regardless of channel.
upvoted 26 times

stealthster Most Recent 2 years, 3 months ago
can be found here: https://learn.microsoft.com/en-us/training/modules/deploy-microsoft-365-apps-for-enterprise/9-explore-update-channels
upvoted 2 times

MEG 2 years, 11 months 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 3 years ago
All channels getting security updates every month (if needed)
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels

upvoted 2 times

sabin001 3 years, 1 month 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 11 times

YClaveria 3 years, 2 months 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 year, 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-enterprise-channel

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

upvoted 7 times

Turd_Reynolds 3 years, 6 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 3 years, 5 months ago

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

So answer is correct.

upvoted 9 times

vasyab 3 years, 6 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 September
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#preview-upcoming-new-features-of-semi-annual-enterprise-channel

upvoted 2 times

larnyx 3 years, 6 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 3 years, 6 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 3 years, 6 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).

Suggested 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 3 years, 1 month 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 8 times

DArnett Highly Voted 2 years, 3 months ago
Selected Answer: D
Valid; on exam 27 September 2022
upvoted 8 times

st2023 Most Recent 1 year, 10 months ago
Selected Answer: D
You can configure hybrid Azure AD joined devices for various types of Windows device platforms.

-For managed and federated domains, you must configure a service connection point or SCP.
-For federated domains, you must ensure that your federation service is configured to issue the appropriate claims.

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's 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.

https://learn.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-manual#configure-a-service-connection-point
upvoted 1 times

Don123 1 year, 11 months ago
D. A new service connection point (SCP).
upvoted 1 times

Mthaher 2 years, 8 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 2 years, 8 months ago

Still valid, April 2022 - it talked about multiple forests trying to throw you off the scent though.

upvoted 4 times

Question #46 *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 the migration method you should use?

A. Exchange Hybrid

B. IMAP migration

C. Cutover

D. Express migration

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

larnyx Highly Voted 3 years, 6 months ago
Answer is correct, B.
upvoted 5 times

paweu Most Recent 1 year, 7 months ago
You should use Google Endpoint, which for some reason is not the option here.
Pros: Migrate contacts, calendars, tasks etc.
upvoted 1 times

Don123 1 year, 11 months ago
B. IMAP migration
IMAP migration is the migration method you should use to move all email data from corporate Gmail to Microsoft Exchange Online via the Exchange admin center.
upvoted 1 times

mfaisal786 3 years ago
it should be clear that whether it is migration technique or migration strategy...
upvoted 2 times

Davidchercm 3 years, 4 months ago
repeat question
upvoted 1 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.

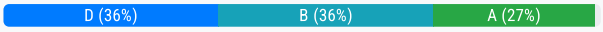
B. Only email data will be migrated.

C. Email and task data will be migrated.

D. Email and contact data will be migrated.

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

Community vote distribution



mfaisal786 Highly Voted 3 years 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 10 times

extrankie 2 years, 12 months ago
Yes, Gsuite will move all
upvoted 3 times

GetEsn Most Recent 1 year, 3 months ago
Selected Answer: A
You can migrate the following functionalities from Google Workspace to Microsoft 365 or Office 365:

Mail & Rules
Calendar
Contacts
upvoted 1 times

osxzvkwpfcfxobqjby 1 year, 4 months ago
Selected Answer: A
https://learn.microsoft.com/en-us/exchange/mailbox-migration/perform-g-suite-migration
upvoted 2 times

hanyeong 1 year, 10 months ago
Selected Answer: D
You can migrate the following functionalities from Google Workspace to Microsoft 365 or Office 365:
Mail & Rules
Calendar
Contacts

https://learn.microsoft.com/en-us/exchange/mailbox-migration/perform-g-suite-migration
upvoted 3 times

Feyenoord 1 year, 10 months ago
Selected Answer: B
They are talking about Exchange native migration and are noty mentioning other tools, so im gonna go with email only. Answer B.
upvoted 1 times

nickstudy 1 year, 10 months ago

Answer is B:

You can only migrate items in a user's inbox or other mail folders. This type of migration doesn't migrate contacts, calendar items, or tasks.

https://learn.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrating-imap-mailboxes
upvoted 1 times

DeLoc 1 year, 10 months ago

Selected Answer: D

When migrating from Gmail to Exchange Online via the Exchange admin center, all email, contacts, and calendar data can be migrated. Therefore, the correct answer is D, "Email and contact data will be migrated."

The Exchange admin center provides an option to migrate email data from Gmail, as well as contacts and calendar data. By selecting the appropriate options during the migration process, all email and contact data can be migrated from Gmail to Exchange Online.

A. While email data will be migrated, other data such as contacts and calendar data can also be migrated.

B. This option is not entirely correct because other data such as contacts and calendar data can also be migrated.

C. This option is not entirely correct because contact data can also be migrated.
upvoted 1 times

Don123 1 year, 11 months ago

B. Only email data will be migrated.
upvoted 1 times

jaysoft 2 years ago

Selected Answer: B

IMAP migration will only migrate emails, not calendar nor contacts .
upvoted 2 times

Mthaher 2 years, 8 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 2 years, 10 months ago

Selected Answer: B

IMAP migration will only migrate emails, not calendar, and contact information.
upvoted 1 times

sabin001 3 years, 1 month ago

with IMAP migration, only emails will get migrated.
upvoted 1 times

extrankie 3 years, 2 months ago

the question is not typically clear, what if one perform Gsuite migration
upvoted 1 times

Joshycannon 3 years ago

It is extremely clear. It says they are using the MS method, so this would obviously lead someone with any reading comprehension to believe they are using the methods they learned about with MS, and that is it. Nowhere does it mention it was using that method, and if they were then the question would be framed around this....
upvoted 3 times

xofowi5140 3 years, 2 months ago

https://docs.microsoft.com/en-us/exchange/mailbox-migration/automated-migration-neweac
upvoted 1 times

YClaveria 3 years, 2 months 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 3 years, 3 months ago

B is correct

for IMAP migration type, only emails will be mirad

upvoted 3 times

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

Suggested 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

Don123 1 year, 11 months ago
B. No

The View service requests option in the Microsoft 365 admin center allows you to view service requests that have been submitted to Microsoft Support and view the status of each request. However, it will not show you a list of features that were recently updated in the tenant.
You can check the Office 365 message center, Office 365 Roadmap, or Release Notes for information on recent feature updates.
upvoted 1 times

simbahmso 2 years, 6 months ago
Selected Answer: B
Makes sense, Message Center is the place to go
upvoted 1 times

Moderator 2 years, 7 months ago
Selected Answer: B
Correct, Message Center is the right place.
upvoted 2 times

Sh1rub10 2 years, 7 months 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

Suggested 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 2 years, 7 months ago

Selected Answer: B

Go to Message Center instead

upvoted 5 times

Rednevi Most Recent 1 year, 7 months ago

Selected Answer: B

B. No

Using the Dashboard in Security & Compliance does not provide a direct way to view a list of recently updated Office 365 features in the tenant. The Dashboard in Security & Compliance primarily provides insights and reports related to security and compliance aspects of the Microsoft 365 environment.

To view a list of recently updated Office 365 features, you would typically refer to the Microsoft 365 Message Center or the Microsoft 365 Admin Center. These platforms provide notifications and announcements regarding updates and changes to the Office 365 services and features in your tenant.

Therefore, the solution of using the Dashboard in Security & Compliance does not meet the goal of viewing a list of recently updated Office 365 features in the tenant.

upvoted 1 times

Don123 1 year, 11 months ago

B. No

The View service requests option in the Microsoft 365 admin center allows you to view service requests that have been submitted to Microsoft Support and view the status of each request. However, it will not show you a list of features that were recently updated in the tenant.
You can check the Office 365 message center, Office 365 Roadmap, or Release Notes for information on recent feature updates.

upvoted 1 times

Question #3 *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 Message center in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Suggested 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 Highly Voted 2 years, 7 months ago
Selected Answer: A
Correct
upvoted 5 times

Moderator 2 years, 7 months ago
Yesh :)
upvoted 2 times

Don123 Most Recent 1 year, 11 months ago
A. Yes
upvoted 1 times

Question #4 *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 review the Security & Compliance report in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Suggested 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 Highly Voted 2 years, 7 months ago
Selected Answer: B
Go to Message Center instead
upvoted 5 times

Don123 Most Recent 1 year, 11 months ago
B. No
Go to Message Center
upvoted 1 times

Question #5 *Topic 2*

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

Suggested 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 3 years, 8 months ago
D - E3 has Conditional Access, PIM is E5
upvoted 17 times

melatocaroca Highly Voted 3 years, 6 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 3 years, 6 months ago

You mean D, right? Your analysis contradicts given answer. Answer D should be correct.
upvoted 4 times

Parzival 2 years, 6 months ago
My thoughts too. Contradiction
upvoted 1 times

Y2 Most Recent 2 years, 3 months 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

Paolo2022 2 years, 1 month ago
E5 includes all E3 features + more. D is correct.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#feature-comparison-based-on-licenses
upvoted 1 times

mikl 2 years, 4 months 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 2 years, 7 months ago
Selected Answer: D
E3 - P1 Conditional access
E5 - PIM

Answer is D.
upvoted 1 times

svenhalen 3 years, 6 months ago
PIM is E5 for sure
upvoted 2 times

RAJULROS 3 years, 7 months ago
This question came last week
upvoted 1 times

kutty09 3 years, 9 months ago
Can i get the document that compares with office Licenses with Azure AD?
upvoted 2 times

kikkens23 3 years, 8 months ago
for sure, you can google it > M365 Licenses
upvoted 5 times

Parzival 2 years, 6 months 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.

Suggested 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

[Removed] Highly Voted 4 years, 5 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 3 years, 6 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-premises organization.
https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship
upvoted 4 times

STFN2019 Highly Voted 4 years, 5 months ago
Here's the valid link: https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/organization-relationships
upvoted 10 times

Don123 Most Recent 1 year, 11 months ago
B. From the Exchange admin center, create a new organization relationship.

To share calendars with a partner organization, you can create a new organization relationship in the Exchange admin center. This will allow the users in your tenant to share their calendars with users in the partner organization's tenant.

To create the organization relationship:

In the Exchange admin center, navigate to organization > sharing.
Select + New to create a new organization relationship.
Enter the email domain of the partner organization (e.g. adatum.com)
Select the Calendar sharing check box.
Click Save to create the relationship
This will allow calendar sharing between the two tenants and the calendar of every user is available to the users in adatum.com immediately.
It's important to note that in order for this to work, the partner organization also needs to create an organization relationship with your tenant.
upvoted 1 times

stoneface 2 years, 12 months ago

Repeated question!

upvoted 2 times

Wojer 3 years ago

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

upvoted 1 times

PDR 3 years ago

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

upvoted 2 times

Mujja 2 years, 6 months 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 domain adatum.com, which can only be done in EAC.

upvoted 1 times

Wojer 3 years ago

I would say C

upvoted 1 times

JakeH 3 years, 1 month ago

In exam today

upvoted 2 times

Panku 3 years, 3 months ago

B is correct answer

upvoted 1 times

Takloy 3 years, 11 months ago

Answer: B

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

upvoted 5 times

mkoprivnj 4 years ago

B for sure!

upvoted 3 times

d6 4 years, 5 months ago

I just had to do this for a client.

upvoted 6 times

Question #7 *Topic 2*

DRAG DROP -

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

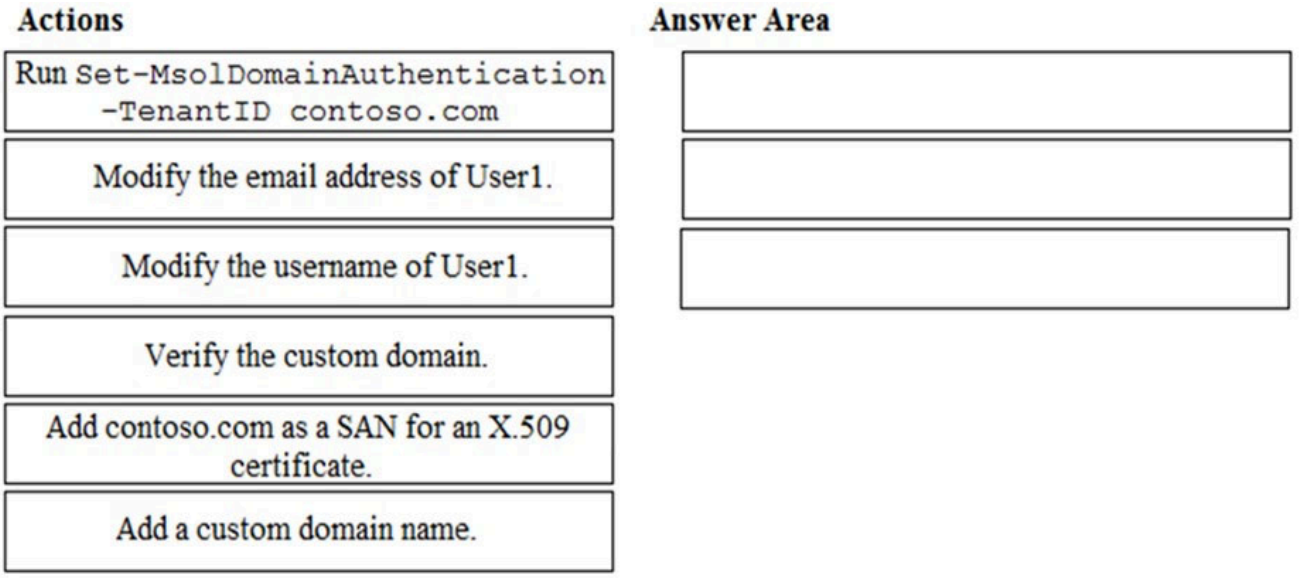
You purchase a domain named contoso.com from a registrar and add all the required DNS records.

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

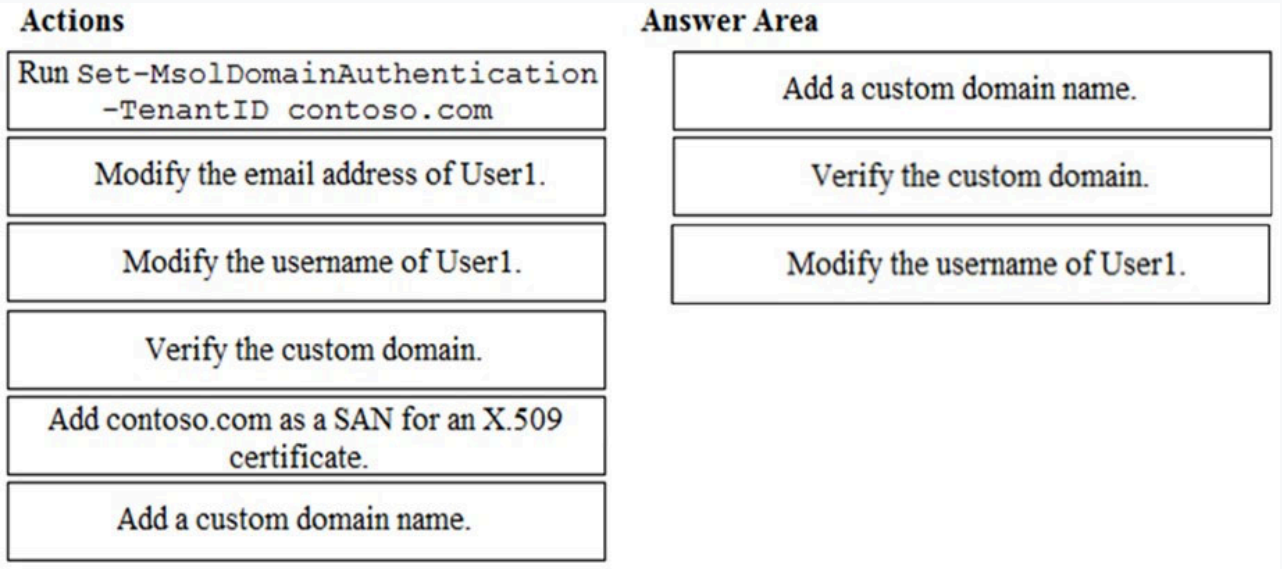
You need to configure User1 to sign in as user1@contoso.com.

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:



Suggested 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 3 years, 5 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 Name) 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 21 times

tf444 3 years ago
UPN is the email address, not the user name.
It should be the email address.
upvoted 1 times

ijarosova 1 year, 9 months ago
user principal name (UPN)
upvoted 1 times

TechMinerUK 2 years, 6 months 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 address we should not mix up the two.

Even on Windows Active Directory the UPN is used as the username alongside the NETBIOS username
upvoted 10 times

sh0wbi Highly Voted 3 years, 7 months ago
correct answer !!
upvoted 15 times

Fcnet 3 years, 5 months ago
not really correct the last should be change email address
upvoted 5 times

Turak64 3 years, 4 months 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 19 times

tf444 3 years ago
wrong, UPN is the email address!
upvoted 2 times

drhousedk 2 years ago
Not correct. When creating the user, the UPN is used to create the primary SMTP proxyaddress. If you want to change the username, you'll have to change the UPN (User Principal Name).
upvoted 1 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

Hanan1234 1 year, 11 months ago
Answer is Correct, you need to select the new domain under "manage username." -- tested in my tenant
upvoted 1 times

Everlastday 1 year, 12 months ago
In Exam 03.01.2023
upvoted 4 times

HaynesO 2 years, 2 months ago
Answer feels correct to me. I feel like you have to recognise that there are three options here that have no relevance to anything. What you're left with is three options that could be. Still, not brilliantly worded.
upvoted 1 times

Kalzonee3611 2 years, 7 months ago
“All dns records in place”

So, they have already added the domain and the TXT record for it???
upvoted 5 times

Rudelke 2 years, 5 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 2 times

Paolo2022 2 years, 1 month ago

That's what I thought, too, at first! But then, as I understand it, you only get the code for the TXT record after you add the custom domain name. So the TXT record cannot be included in "all the required DNS records" mentioned in the question".

upvoted 2 times

slaoui 2 years, 8 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 2 years, 9 months 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 Microsoft 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 2 years, 10 months ago

Correct

upvoted 1 times

tf444 3 years ago

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

upvoted 6 times

JakeH 3 years, 1 month ago

In exam today

upvoted 1 times

sabin001 3 years, 1 month 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 to 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 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 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 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 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 3 years, 2 months 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 3 years, 3 months ago
Yes we need to change username however there is no saprate option for change email address
upvoted 1 times

Panku 3 years, 3 months ago
https://docs.microsoft.com/en-us/microsoft-365/business-video/change-user-name-email?view=o365-worldwide
upvoted 1 times

zacmzee 3 years, 3 months ago
Last one should be change username. Test it yourself, go to O365 admin center -> select user -> Click manage username -> select domain name from drop down list.
upvoted 1 times

spg987 3 years, 4 months ago
It is my exam today- last one- modify the email address
upvoted 2 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.

Suggested 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 4 years, 10 months ago
With the migration endpoint settings you will be able to choose how many simultaneous mailbox will be exported.
upvoted 32 times

[Removed] Highly Voted 4 years, 4 months 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 26 times

extrankie 2 years, 11 months ago
nice explain
upvoted 1 times

Don123 Most Recent 1 year, 11 months ago
You should do C. Modify the migration endpoint settings.

When migrating mailboxes and groups to Exchange Online, it is important to consider the impact on end-user performance. One way to reduce the impact of the migration on end-users is to modify the migration endpoint settings.
upvoted 1 times

waterlego 2 years, 8 months ago
Still valid, April 2022
upvoted 3 times

Wojer 2 years, 11 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 2 times

Paolo2022 2 years, 1 month ago
Well, modifying the migration endpoint settings is the way to implement migration service throttling - and there's no such thing as a throttling policy. See the source that you provided.

So C is definitely correct here.
upvoted 1 times

Jcbrow27 3 years, 1 month 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 and control the performance, for me the answer is C
upvoted 1 times

Panku 3 years, 3 months ago
C is right answer read the office ref document
upvoted 4 times

melatocaroca 3 years, 6 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 phase 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 3 years, 4 months ago
I would prefer D as well. Most of the migration bottleneck is on networking side than the server loading.
upvoted 2 times

lengySK 3 years, 4 months ago
I prefer D as well.
upvoted 2 times

Aysan 3 years, 7 months ago
isn`t this ms-101 question?
upvoted 1 times

zer0en 3 years, 7 months ago
i can confirm that this is in the ms-100 exam per 23.05.21
upvoted 3 times

mkoprivnj 4 years ago
C for sure!
upvoted 3 times

emil568 4 years, 4 months ago
Could be a solution
upvoted 1 times

minajahan 4 years, 10 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 4 years, 9 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 that 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.

Suggested 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 3 years, 6 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 3 years ago
Direct URLs : https://security.microsoft.com/antiphishing; https://security.microsoft.com/threatpolicy and click on Anti-Phishing; Microsoft 365 Defender Portal --> Policies & Rules from left pane --> Threat Policies --> Anti-Phishing under Policies.
upvoted 5 times

nickstudy Most Recent 1 year, 10 months ago
its Exchange online protection anthi phishing policy
https://learn.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 2 times

Don123 1 year, 11 months ago
From the Security & Compliance admin center, create a new threat management policy.
upvoted 1 times

TechMinerUK 2 years, 6 months 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 3 years, 1 month ago
In exam today
upvoted 2 times

sabin001 3 years, 1 month ago

Correct Answer

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-policie

upvoted 2 times

Sr15 3 years, 6 months ago

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

upvoted 2 times

Jcbrow27 3 years, 1 month ago

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

upvoted 3 times

Turak64 3 years, 4 months ago

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

Suggested 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

Razuli Highly Voted 3 years, 8 months ago
C + E as others specified, just tested
upvoted 25 times

PeterC 3 years, 8 months ago
Agree ->
https://docs.microsoft.com/en-us/microsoft-365/admin/email/change-email-address?view=o365-worldwide
upvoted 5 times

YuvaRajaVignesh 2 years, 6 months 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 3 years, 4 months ago
answer C no, because blade SETUP doesn't include domain...its in SETTINGS
upvoted 3 times

Aps123 3 years, 3 months 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 3 years 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 2 times

MartinTexel Highly Voted 3 years, 3 months 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 address templates to use "@contoso.com" as the primary SMTP address and "@contoso.onmicrosoft.com" and "@contoso.microsoftonline.com" as 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 14 times

zacmzee 3 years, 3 months ago
Nice one, tested to confirm!
upvoted 1 times

rfox321 3 years, 3 months ago
It's simply wrong because the answer states: "In Windows" - You don't run these from windows..
upvoted 1 times

Davidchercm 2 years, 11 months ago
what you mean you don't run these from windows ?
upvoted 2 times

XW_64 2 years, 3 months ago
Tested and confirmed! E and D are correct!
upvoted 2 times

bbshk Most Recent 1 year, 7 months ago
Selected Answer: BD
B+D should be.
upvoted 1 times

Rednevi 1 year, 7 months ago
Selected Answer: CE
D is not a correct solution to achieve the goal:

D. Run the Set-EmailAddressPolicy Windows PowerShell command.

The Set-EmailAddressPolicy command is used in on-premises Exchange environments to modify email address policies. However, in a cloud-only Microsoft 365 subscription where all identities are managed in the cloud, this command is not available or applicable.

In the cloud-only environment, the recommended approach is to use the Exchange admin center or the Microsoft 365 admin center to configure email address policies and domain settings.

Therefore, option D is not a possible way to ensure that all new mailboxes use the new domain as their primary email address. The correct options are B, C, and E.

upvoted 2 times

vanr2000 1 year, 9 months ago

Selected Answer: CD

You first add the custom domain and validate it.
The second step you need to assign the new email domain to be use.

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

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 address policy named "Office 365 Groups" and sets the enabled email address templates to use "@contoso.com" as the primary SMTP address and "@contoso.onmicrosoft.com" and "@contoso.microsoftonline.com" as proxy addresses.

upvoted 1 times

Sjoerd123 1 year, 9 months ago

Selected Answer: CE

Set-EmailAddressPolicy in Exchange online are only for Groups. Not Users

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

Use the New-EmailAddressPolicy cmdlet to create email address policies. In Exchange Online, email address policies are only available for Microsoft 365 Groups.

upvoted 1 times

ijarosova 1 year, 9 months ago

Selected Answer: BD

I vote B+D

upvoted 1 times

Meebler 1 year, 9 months ago

C. From the Microsoft 365 admin center, select Setup, and then configure the domains.
E. From the Azure Active Directory admin center, configure the custom domain names.

Option C allows you to add and configure the new domain name in the Microsoft 365 admin center. Once the new domain is added and verified, you can set it as the primary email address for all new mailboxes by updating the default email address policy.

Option E allows you to add the new domain name in the Azure Active Directory admin center. Once the domain is added and verified, you can set it as the primary email address for all new mailboxes by updating the default domain in the Azure Active Directory.

Options A and D are related to updating email address policies in Exchange Server, which is not applicable in this scenario as all identities are managed in the cloud. Option B is also related to Exchange Server, so it is not applicable either.

upvoted 1 times

Don123 1 year, 11 months ago

D. Run the Set-EmailAddressPolicy Windows PowerShell command.
E. From the Azure Active Directory admin center, configure the custom domain names.

upvoted 4 times

Hanan1234 1 year, 11 months ago

Using PowerShell, Answer should be "D".
Using 365 admin center, we can configure domains and make the new domain as default under "Settings" blade not "SETUP" so CAN'T BE "C".
Using Azure AD we can add Custome Domain Name and make is as Primary Domain and it considered as default domain name so any new user will have the new domain and not affecting the existing users. so answer is "E"
Can't be "B" because no option to add a domain under Exchange.
Answer is "DE"

upvoted 1 times

KnightOfH 1 year, 11 months ago

Selected Answer: BD

B+D because it's only about mailboxes, not login UPN.

upvoted 1 times

Startkabels 2 years ago

D+E

Checked in production and confirmed that it's not M365 Admin Center but Azure AD:

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-manage

upvoted 1 times

XW_64 2 years, 3 months ago

Selected Answer: DE

E & D are correct! Admin please check and update

upvoted 1 times

KemalM 2 years, 3 months 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 2 years, 4 months ago

Selected Answer: CE

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

upvoted 2 times

[Removed] 2 years, 6 months ago

Selected Answer: CE

C + E is a correct answer

upvoted 3 times

TechMinerUK 2 years, 6 months 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 domain in AzureAD via the blade. Because it is the default domain any new user accounts will have the domain set as their default username and if they have an Exchange Online license as their default email address domain as well (It won't change existing account usernames or email addresses though)

upvoted 2 times

Question #11 *Topic 2*

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

Suggested 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
C (83%) B (17%)

Carlo5 Highly Voted 3 years, 6 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 without location will inherit the license. You can find it in the AAD license page.
upvoted 19 times

Kotor987 2 years, 5 months ago
Can confirm.
upvoted 1 times

rfox321 3 years, 3 months ago
Big round of applause for actually testing.. instead of impulsively providing an incorrect answer. Thank you!
upvoted 15 times

[Removed] 2 years, 3 months ago
user 2 not 3
upvoted 1 times

[Removed] Highly Voted 3 years, 8 months ago
C for sure
upvoted 14 times

tfoi0001 Most Recent 1 year, 9 months ago
Group-based licensing currently doesn't 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.
upvoted 1 times

st2023 1 year, 10 months ago
Selected Answer: C
C - 3 is correct and the reasoning provided for inheriting the directory's location and nested groups is available in the links provided

upvoted 1 times

Don123 1 year, 11 months ago

Answer: C

User 1,3,4 will be assigned the required license from group 1 but not User 2 has nested groups (group 2) are not supported.

upvoted 1 times

Kotor987 2 years, 5 months ago

Selected Answer: C

Tested. It's C.

upvoted 1 times

ConveneSupport 2 years, 5 months ago

Now Azure supports nested security access

upvoted 1 times

KrisDeb 2 years, 3 months 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 nested group, only the immediate first-level user members of the group have the licenses applied.

upvoted 2 times

Rudelke 2 years, 5 months ago

Had this question 07.2022

upvoted 1 times

TechMinerUK 2 years, 6 months 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 with 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 2 years, 7 months 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 2 years, 7 months ago

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

upvoted 1 times

frankchen0609 2 years, 9 months 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 2 years, 11 months ago

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

upvoted 1 times

IamSherlocked 3 years, 6 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 7 times

Luiza 3 years, 6 months ago

B.2

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

upvoted 12 times

Joshycannon 3 years ago

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

upvoted 4 times

prabhjot 1 year, 8 months ago

agree 100 Percent it should be B

upvoted 1 times

melatocaroca 3 years, 6 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 to a user, you must specify the Usage location property for the user. You can specify the location under the User > Profile > Edit section in the Azure portal.

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

Answer B

upvoted 3 times

melatocaroca 3 years, 6 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 location of the directory.

User 4 Canada and group 1

So 3

upvoted 2 times

Maroslaw 3 years, 7 months ago

The answer is correct, C

upvoted 2 times

jeremyburrows 3 years, 7 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%20group%20licenses%20car under known limitations is says nested groups not supported. So the count should be 2

upvoted 1 times

Question #12 *Topic 2*

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

Suggested 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 3 years, 9 months ago
Tested this. Answer is corrct.
upvoted 9 times

Puneet30 Highly Voted 3 years, 7 months ago
Exam Q on 15May21
upvoted 6 times

charat Most Recent 2 years, 7 months ago
05/22 exam. Great stuff ExamTopics!
upvoted 3 times

Wojer 3 years ago
I think you can do daily reports but the report will have information from a last 7 days
upvoted 2 times

JakeH 3 years, 1 month ago
In exam today
upvoted 3 times

jjong 3 years, 3 months ago
came out today on my exam on 27-sep-21
upvoted 3 times

Ash473 3 years, 4 months ago
In today's exam
upvoted 2 times

RAJULROS 3 years, 7 months ago
This question came on 28May21
upvoted 3 times

PeterC 3 years, 8 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

Suggested 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 4 years, 10 months ago
A is correct, under licenses, go to All Products, you'll see group assignments
upvoted 29 times

WoneSix 4 years, 10 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, but I'll not argue symantics), Licenses, Licensed Groups, then select the individual groups to find a) members, and b) licenses assigned to it. A is correct.
upvoted 7 times

PhantomPhixer 4 years, 7 months ago
slight clarification, Licenses, Licensed Groups, then select the individual licenses to find the info as stated under Licensed users or licensed groups..
upvoted 2 times

[Removed] Highly Voted 4 years, 5 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 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
upvoted 18 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

Cheekypoo 2 years, 5 months ago
Was in my exam today 05/08/22.
upvoted 1 times

TechMinerUK 2 years, 6 months 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 not name the group which they are licensed through

upvoted 1 times

trexar 2 years, 9 months ago

Selected Answer: A

correct

upvoted 1 times

Aze 3 years, 11 months ago

A is correct

upvoted 3 times

mkoprivnj 4 years ago

A for sure!

upvoted 2 times

mkoprivnj 4 years ago

ctfalci great job!

upvoted 1 times

FcoGlezRoy 4 years, 7 months ago

Correct answer is A but will require AD P2 or EMS

upvoted 5 times

JaBe 4 years, 4 months 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. but you can just click 'manage your purchased licenses' and access the Licensed users - groups panes.

upvoted 3 times

DUSHIWORLD 4 years, 10 months ago

Correct Answer is A.

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

upvoted 7 times

WoneSix 4 years, 10 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're saying here?

upvoted 1 times

[Removed] 4 years, 6 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.

Suggested 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

[Removed] Highly Voted 4 years, 5 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 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
upvoted 20 times

rleijten Highly Voted 4 years, 10 months ago
Unless the PST-files were uploaded in februari, and a month later no 30 days had passed :)
upvoted 9 times

Vsurvase Most Recent 2 years, 9 months ago
I got this question on 26 March 2022 exam.
upvoted 2 times

Turak64 3 years, 4 months 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, then B is no longer the correct answer!
upvoted 4 times

Paolo2022 2 years, 1 month ago
At MS they don't know my colleagues - D is definitely the best answer! :-)
upvoted 1 times

Ash473 3 years, 4 months ago
In today exam
upvoted 1 times

melatocaroca 3 years, 6 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 3 years, 7 months ago

Exam Q on 15May21

upvoted 3 times

mkoprivnj 4 years ago

B for sure!

upvoted 3 times

DUSHIWORLD 4 years, 10 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.

Suggested 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 4 years, 11 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 their 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 20 times

test123123 Highly Voted 4 years, 11 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 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 Office 365 endpoints, network traffic destined for Office 365 can connect to Office 365 front end servers as close as possible to the user

Ref:
https://docs.microsoft.com/en-us/office365/enterprise/office-365-network-connectivity-principles#BKMK_P2
upvoted 14 times

Don123 Most Recent 1 year, 11 months ago
D. In the branch offices, configure name resolution so that all queries for external host names are redirected to public DNS servers directly.
upvoted 1 times

Vsurvase 2 years, 9 months ago
I got this question on 26 March 22 exam.
upvoted 4 times

Nastha 3 years ago
Local DNS and Internet egress is of critical importance for reducing connection latency and ensuring that user connections are made to the nearest point of entry to Microsoft 365 services. In a complex network topology, it is important to implement both local DNS and local Internet egress together.

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide
upvoted 3 times

Ash473 3 years, 4 months ago
In today's exam
upvoted 4 times

mkoprivnj 4 years ago
D for sure!
upvoted 6 times

[Removed] 4 years, 5 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 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.
upvoted 9 times

PDR 4 years, 10 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 like because it doesnt specify which public DNS servers - it could be configured for DNS servers that are further /slower than the main office 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.

Suggested 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%)

[Removed] Highly Voted 4 years, 4 months 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 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.
upvoted 36 times

donathon 4 years, 3 months ago
Yes, I can personally verify this because my environment has this issue. Once you change th UPN suffix to the domain that is verified, the issue will go away.
upvoted 7 times

DUSHIWORLD Highly Voted 4 years, 10 months ago
Correct Answer is C.
upvoted 7 times

LamestDuck 4 years, 1 month ago
They literally give it away with D, that's the problem but not the solution haha.
upvoted 2 times

Don123 Most Recent 1 year, 11 months ago
From Active Directory Users and Computers, modify the UPN suffix of the five user accounts.
upvoted 1 times

Startkabels 2 years ago

Selected Answer: C

Can't change the user in the cloud in a hybrid environment.
Needs to be changed in AD to begin with and the reason they have the default MS UPN is because their UPN is set to domain.local.

upvoted 1 times

SkullRage 2 years, 4 months ago

Correct answer is C

upvoted 1 times

Moderator 2 years, 5 months ago

Selected Answer: C

Still a valid question as of July 30th 2022.

upvoted 2 times

gaem 2 years, 7 months ago

Selected Answer: C

C correct answer

upvoted 2 times

jjong 3 years, 3 months ago

in today's exam too. seems like whatever Ash473 encountered, i oso have.

upvoted 2 times

Ash473 3 years, 4 months ago

In today's exam

upvoted 2 times

syswiz85 3 years, 8 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 domain 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 are 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 3 years, 9 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 domain 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 setup). 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 3 years, 10 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.com 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 3 years, 11 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 3 years, 11 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 4 years ago

C for sure!

upvoted 3 times

Noppawat 4 years 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 4 years ago

correct

upvoted 1 times

Question #17 *Topic 2*

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.	○	○

Suggested 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 4 years ago

Y, Y, Y is correct. All users are licensed for SPO!

upvoted 11 times

init2winit Highly Voted 3 years, 8 months ago

Trick question, Y,Y,Y

upvoted 7 times

honeyman123 Most Recent 2 years, 6 months ago

Y, Y, Y is correct.

Just fyi: Nested groups are there as a new feature via dynamic membership rules. :)

upvoted 1 times

Bren 2 years, 7 months 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 group 2 is no longer working?

upvoted 1 times

Rudelke 2 years, 5 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 2 times

Nilz76 2 years, 10 months ago

YYY. All 3 members have explicit membership. 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.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues

upvoted 3 times

[Removed] 2 years, 10 months 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 2 years, 10 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 2 years, 11 months ago

direct question with unnecessary information

upvoted 4 times

bingomutant 3 years, 11 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 makes no difference

upvoted 4 times

[Removed] 4 years, 5 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.

Suggested 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%)

[Removed] Highly Voted 4 years, 5 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 the AD Connect Health Sync Agent. You can do this manually by running theRegister-AzureADConnectHealthSyncAgentcmdlet. Alternatively, you can reinstall the Azure AD Connect Health agent. The Azure AD Connect Health agent is registered as part of the installation.
upvoted 29 times

Jokke71 Highly Voted 4 years, 10 months ago
After deleting a service instance from Azure AD Connect Health service, if you want to start monitoring the same server again, uninstall, 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

Amir1909 Most Recent 11 months ago
A and E is correct
upvoted 1 times

Don123 1 year, 11 months ago
A. From Windows PowerShell, run the Register-AzureADConnectHealthSyncAgent cmdlet.
E. From Server1, reinstall the Azure AD Connect Health agent.
upvoted 1 times

Moderator 2 years, 5 months ago
Selected Answer: AE
Still a valid question (July 30th 2022).
upvoted 4 times

mikl 2 years, 4 months ago

Thank you :)

upvoted 1 times

spg987 3 years, 4 months ago

It is my exam today

upvoted 5 times

mikl 3 years, 10 months ago

A and E seems correct.

upvoted 4 times

mkoprivnj 4 years ago

A & E for sure!

upvoted 6 times

Tarek 4 years, 9 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 4 years, 9 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.

Suggested 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

[Removed] Highly Voted 4 years, 5 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 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
upvoted 24 times

mkoprivnj Highly Voted 4 years ago
A & B for sure!
upvoted 11 times

Matt789 Most Recent 3 years, 7 months ago
Definite exam question
upvoted 5 times

Puneet30 3 years, 7 months ago
Exam Q
upvoted 6 times

lucidgreen 3 years, 9 months ago
The mobile app part gave it away for me. Both those answers pointed to the same place.
upvoted 4 times

mikl 2 years, 4 months ago
Thank you :)
upvoted 1 times

Question #20 *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 Monitoring and reports from the Compliance admin center.
Does this meet the goal?

A. Yes

B. No

Suggested 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 2 years, 7 months ago

Selected Answer: B

Go to Message Center instead
upvoted 3 times

ProfesorF 2 years, 6 months ago

Thankyou
upvoted 1 times

Question #21 *Topic 2*

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.

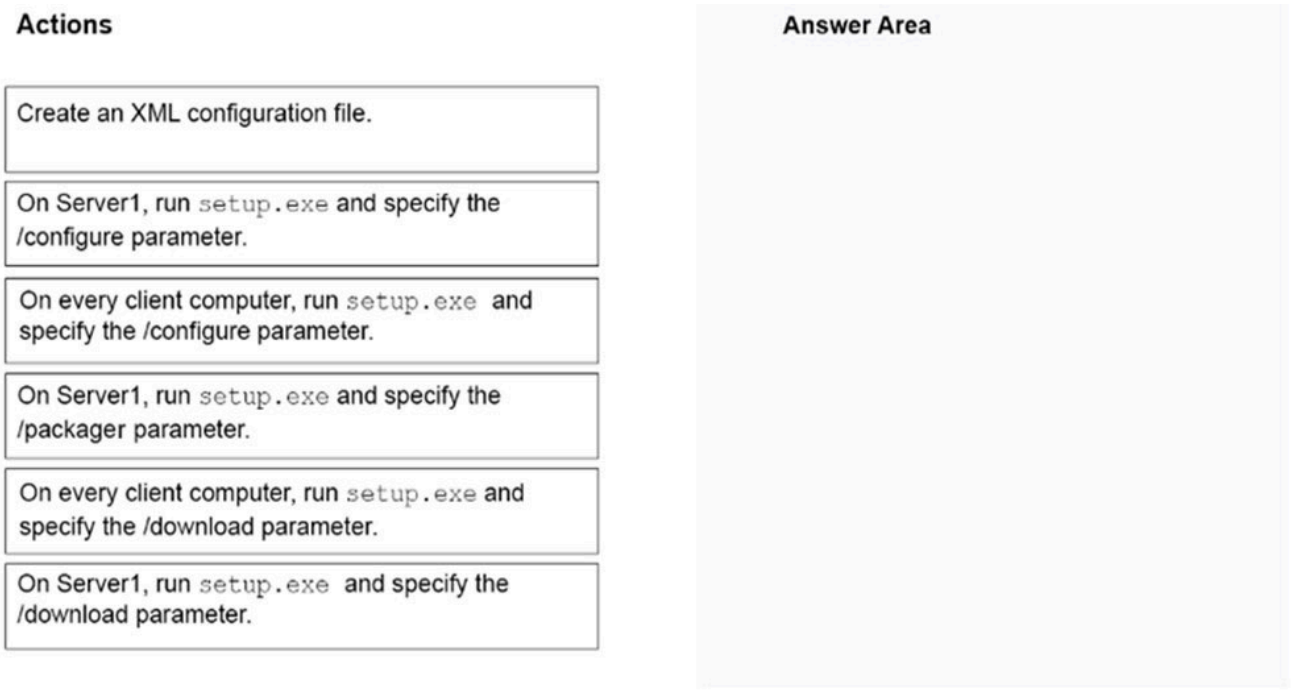
Your company purchases a Microsoft 365 subscription.

On Server1, you create a file share named Share1. You extract the Microsoft Office Deployment Tool (ODT) to Share1.

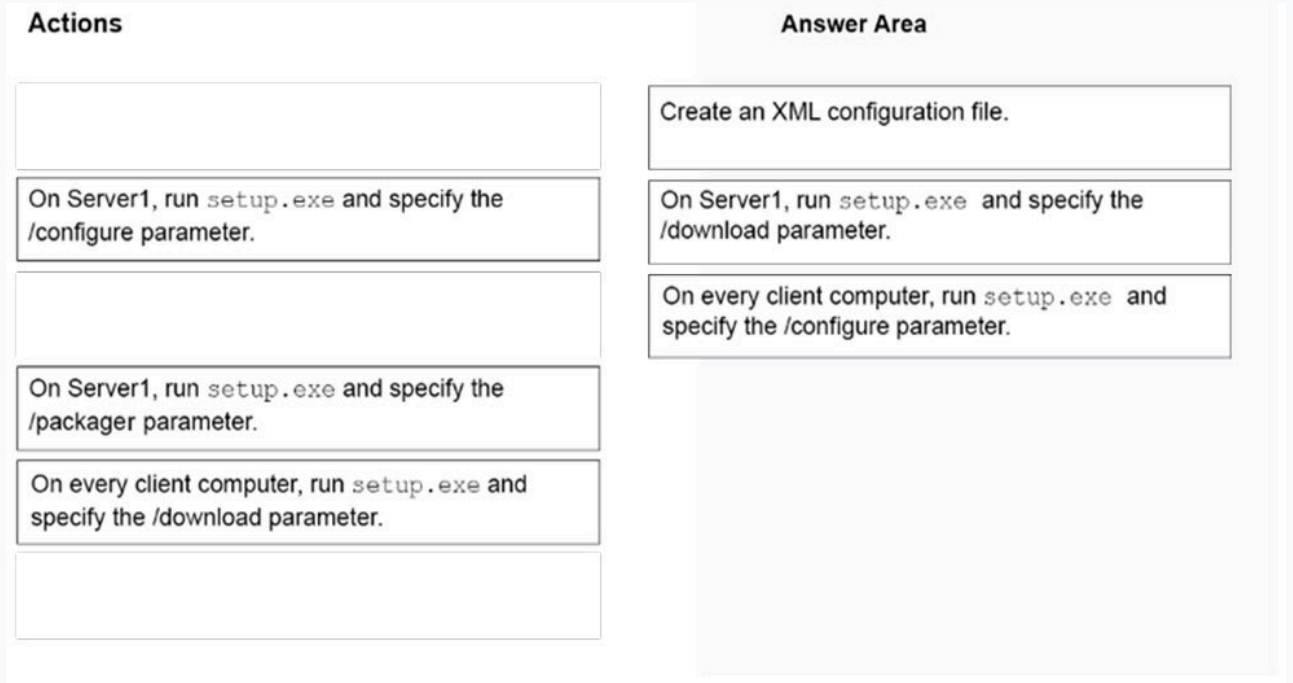
You need to deploy Microsoft 365 Apps for enterprise and the French language pack from Share1 to the Windows 10 computers.

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:



Suggested Answer:



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

[Removed] Highly Voted 3 years, 7 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 65 times

PDR 3 years, 6 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 3 years, 6 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 2 years, 6 months 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 an 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 3 years, 6 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

Everlastday Most Recent 1 year, 12 months ago

On Exam 03.01.2023

upvoted 1 times

donb21 2 years, 4 months ago

answer should be creating a xml file > download > install in target server

upvoted 1 times

Cheekypoo 2 years, 5 months ago

Was in my exam today 05/08/22

upvoted 1 times

Moderator 2 years, 5 months ago

Still a valid question (July 30th 2022).

upvoted 1 times

charat 2 years, 7 months ago

On exam 05/22. Given answer is correct on this one.

upvoted 1 times

Stiobhan 2 years, 7 months 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 exam 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 2 years, 8 months ago

https://docs.microsoft.com/en-us/deployoffice/overview-office-deployment-tool#install-microsoft-365-apps

upvoted 2 times

JakeH 3 years, 1 month ago

In exam today

upvoted 2 times

MartiFC 3 years, 5 months ago

nitvit610 Is correct your answer!

upvoted 2 times

momonoke 3 years, 5 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 3 years, 4 months ago

yeah, dont study the answers.

upvoted 6 times

RAJULROS 3 years, 7 months ago

last week exam question

upvoted 4 times

Khazetul1 3 years, 7 months ago

Agree with nitvit610.

upvoted 6 times

Question #22 *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: You add Device1 to an Active Directory group.
Does this meet the goal?

A. Yes

B. No

Suggested 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 5 years 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

[Removed] Highly Voted 4 years, 5 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 27 times

Don123 Most Recent 1 year, 11 months ago
B. No

Adding the device to an Active Directory group does not directly enable co-management of the device in Configuration Manager and Microsoft Intune. Additional steps are required, such as enrolling the device in Intune and configuring the co-management settings in Configuration Manager.
upvoted 1 times

ServerBrain 2 years, 1 month ago
The answer is NO. Solution is add Device1 to the
Device Collection

upvoted 1 times

Eggsamine 3 years, 2 months ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 5 times

SandyZ 3 years, 9 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 to msendpointmgr, I didn't write anything about adding a device to AD group for co-management. The old post is no longer valid anyway, I have changed the serial post to"how to configure PKI", not Co-management.

upvoted 3 times

Neshiri 3 years, 9 months ago

the answer is no

upvoted 1 times

lucidgreen 3 years, 10 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 3 years, 11 months ago

Dead link: https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/

upvoted 1 times

alecrobertburns 3 years, 11 months ago

To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune

upvoted 2 times

mkoprivnj 4 years ago

B for sure!

upvoted 2 times

MSROCKS 4 years, 2 months ago

NO! most be the correct answer :)

upvoted 2 times

VTHAR 4 years, 2 months ago

The correct answer is NO. It doesn't meet the goal.

upvoted 2 times

FNyirongo 4 years, 2 months ago

The answer there should be no

upvoted 2 times

mkcom 4 years, 5 months ago

https://docs.microsoft.com/en-us/intune/enrollment/windows-enroll#enable-windows-10-automatic-enrollment

upvoted 1 times

Benoit_HAMET 4 years, 6 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 4 years, 6 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) Windows 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 "You 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 of 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

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

Suggested 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 4 years, 11 months ago
The correct solution, so the answer is A
upvoted 42 times

VP11 4 years, 9 months ago
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable
upvoted 2 times

melatocaroca 3 years, 6 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

VTHAR 4 years, 2 months ago
Agreed. The correct answer is A. YES It does meet the goal.
upvoted 4 times

[Removed] 4 years, 5 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 21 times

depmatic Highly Voted 4 years, 11 months ago

Answer is yes, indeed.

upvoted 8 times

Don123 Most Recent 1 year, 11 months ago

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.

upvoted 1 times

Eggsamine 3 years, 2 months ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 2 times

Bitek123 3 years, 9 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 2 times

mkoprivnj 4 years ago

A for sure!

upvoted 3 times

MSROCKS 4 years, 2 months ago

This shoud be YES

upvoted 2 times

FNyirongo 4 years, 2 months ago

I can understand better on this Question than Q22

upvoted 1 times

Lynxy 4 years, 6 months ago

This question has split so many, so far I found both answers to be true?!

upvoted 1 times

STFN2019 4 years, 5 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 4 years, 3 months 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 using a 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 to Intune.
All - Enable automatic enrollment for all Windows 10, version 1709 or later, clients.

upvoted 1 times

Benoit_HAMET 4 years, 6 months ago

This should be yes
piloting co-management is using device collection which can use direct assignmenet

upvoted 1 times

shark1 4 years, 6 months ago

Yes. maybe, anyone? https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/collections/create-collections

upvoted 2 times

Benjam 4 years, 6 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 4 years, 7 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 Active 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 4 years, 7 months ago
The answer is A
upvoted 1 times

Tarek 4 years, 9 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 4 years, 9 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 4 years, 10 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

Question #24 *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: You create a device configuration profile from the Intune admin center.
Does this meet the goal?

A. Yes

B. No

Suggested 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

[Removed] Highly Voted 4 years, 5 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

Don123 Most Recent 1 year, 11 months ago
B. No

Adding the device to an Active Directory group does not directly enable co-management of the device in Configuration Manager and Microsoft Intune. Additional steps are required, such as enrolling the device in Intune and configuring the co-management settings in Configuration Manager.
upvoted 1 times

Eggsamine 3 years, 2 months ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 2 times

junior6995 3 years, 3 months ago
Did someone get this question on MS-100? It feels like this question should be in MS-101 instead
upvoted 2 times

Turak64 3 years, 4 months ago

This feels like it should be a question for MS-101...

upvoted 4 times

adaniel89 3 years, 9 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 4 years ago

B for sure!

upvoted 4 times

gardist 4 years, 3 months ago

add Device1 to an active Directory Groupe will meet the goal.

upvoted 1 times

Takloy 3 years, 11 months ago

add to device collection

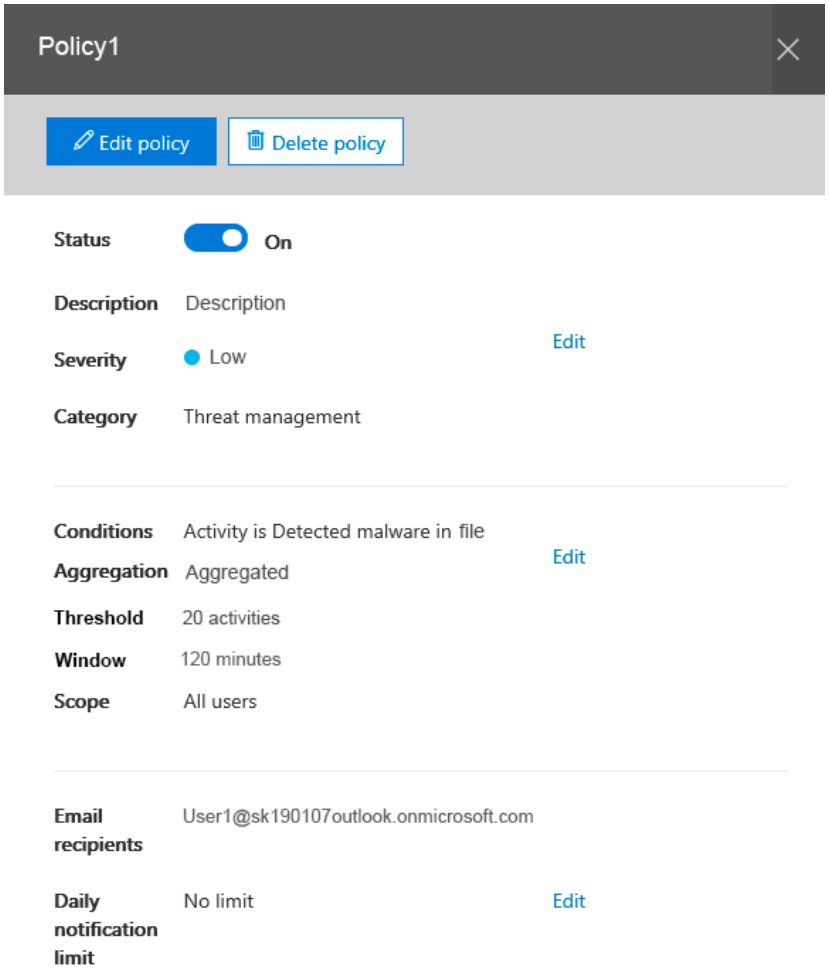
upvoted 7 times

Question #25 *Topic 2*

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

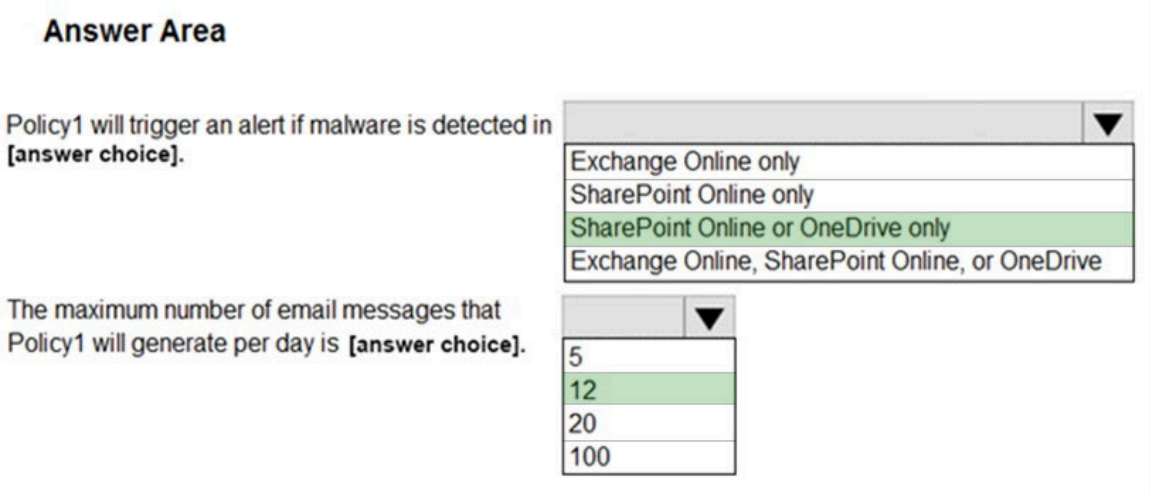
Policy1 will trigger an alert if malware is detected in **[answer choice]**.

- 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

Suggested 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 4 years, 7 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 127 times

Moji1 Highly Voted 5 years 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 "Detect malware in an email message"
upvoted 44 times

zeeess99 4 years, 10 months ago
This explaination is correct
upvoted 2 times

Sachie_Brown 4 years, 8 months ago
I agree with this.
upvoted 2 times

praveen97 4 years, 6 months ago
Agree. "Detect malware in file" alert activity is for SharePoint, OneDrive and MS Teams files only.
upvoted 2 times

AADapson 3 years, 8 months ago
This particular activity only covers for SharePoint and OneDrive. There is another option that covers for Email
upvoted 2 times

melatocaroca 3 years, 6 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 2 years, 6 months ago
This question is still relevant, It was on my MS 101 test in 6/22
upvoted 3 times

trexar 2 years, 9 months ago
Actually they have on Daily Notification Limit:
1,5,10,25,50,100,150,200 or no limit
upvoted 1 times

Jcbrow27 3 years, 1 month ago
i tested and the answer is correct only apply for SharePoint and OneDrive
upvoted 2 times

fofo1960 3 years, 2 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 3 years, 4 months ago
correct
upvoted 1 times

[Removed] 3 years, 6 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 4 years ago
Copied from Sec&Compliance Portal: "Office 365 detected malware in either a SharePoint or OneDrive file" - So SharePoint & OneDrive - 12 MSGS.
upvoted 6 times

lucidgreen 3 years, 9 months ago
If that's the case, SharePoint and OneDrive make sense.
upvoted 1 times

mkoprivnj 4 years ago
4 & 2 for sure!
upvoted 1 times

mkoprivnj 4 years ago
(24*60)/120=12
upvoted 1 times

csribeiro12 4 years, 1 month ago
Resposta correta é SharePoint e OneDrive
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide
upvoted 3 times

scottims 4 years, 2 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 4 years, 1 month 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

[Removed] 4 years, 5 months ago
SharePoint / One Drive only
12
100% Confirmed!
upvoted 14 times

rambo1990 4 years, 5 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 4 years, 2 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 4 years, 6 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 4 years, 8 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 4 years, 8 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 choose 1 5 10 25 50 100 150 200 and unlimited.
upvoted 1 times

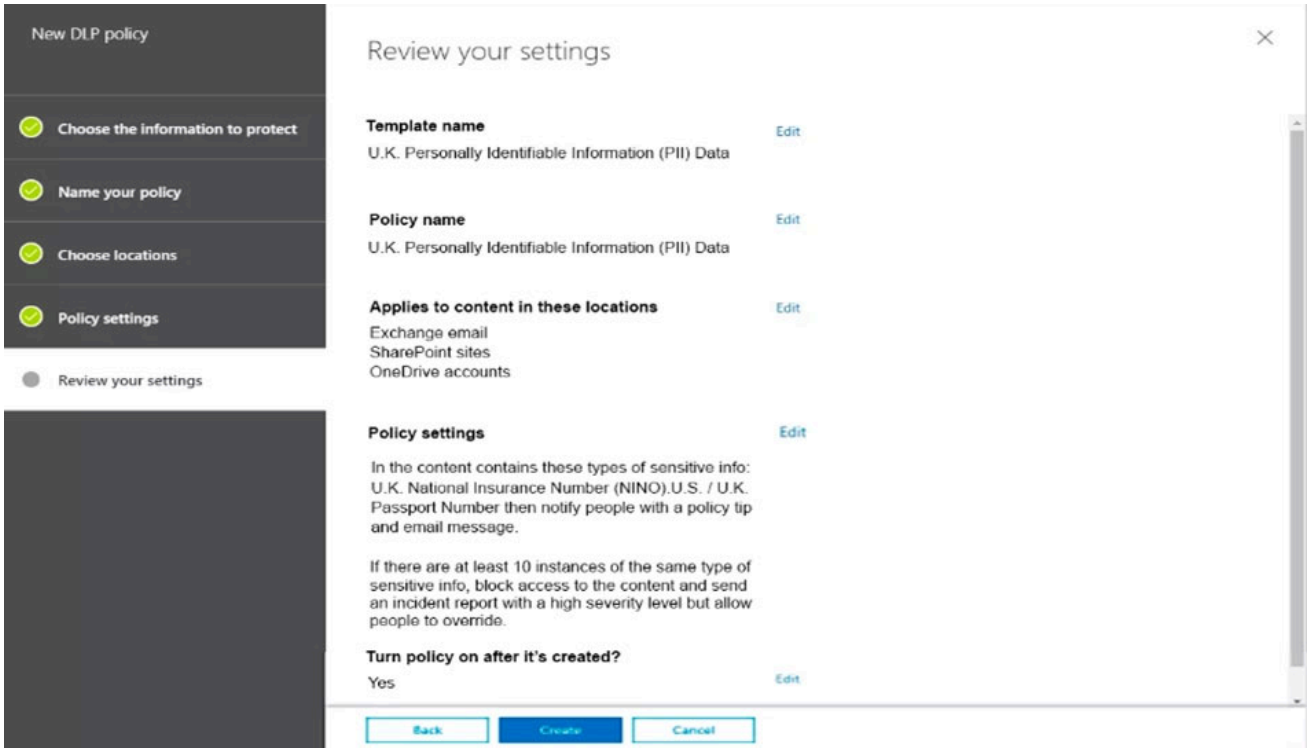
Question #26 *Topic 2*

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

Suggested 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 3 years, 7 months ago
The given answers are correct.
upvoted 18 times

Eggsamine Most Recent 3 years, 2 months ago
Has anyone had this show up in the MS-100 exam as it is an MS-101 question?
upvoted 4 times

sehlohomoletsane 1 year, 9 months ago
Yes i have
upvoted 1 times

InformationOverload 3 years, 4 months 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 business justification
upvoted 1 times

momonoke 3 years, 5 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 2 years, 6 months 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 is 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

Question #27 *Topic 2*

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

Suggested 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 3 years, 8 months ago

I see nothing in the skills measured for this exam about WIP....

upvoted 14 times

Razuli 3 years, 7 months ago

And the training Microsoft provide doesn't include all the stuff covered but I do remember this in the exam

upvoted 7 times

Turak64 3 years, 4 months 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 7 times

fofo1960 3 years, 2 months ago

There are alot of Exchange Online questions also here

upvoted 2 times

PlumpyTumbler Highly Voted 3 years, 7 months ago

MS-101 question.

upvoted 7 times

bernd1976 Most Recent 1 year, 10 months ago

Why is this even in the MS-100 section as this is more of a MD-101 type of question

upvoted 1 times

WickedMJ 2 years, 2 months ago

Correct answers provided.

> To modify which users are affected by WIP, configure: "The MAM user scope"

> To modify which applications are affected by WIP, configure: "App protection policies"

Reference:

https://www.examtopics.com/discussions/microsoft/view/52971-exam-ms-101-topic-3-question-8-discussion/

upvoted 1 times

mikl 2 years, 4 months ago

Beside the fact that this might belong to MS-101, I do believe its correct answers.

upvoted 1 times

Eggsamine 3 years, 2 months 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

Suggested 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%)

[Removed] Highly Voted 4 years, 5 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 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
upvoted 21 times

kevinmwest2112 Highly Voted 4 years, 2 months ago
MS-101 question
upvoted 8 times

VTHAR 4 years, 2 months ago
Yes ... It is.
upvoted 3 times

Startkabels Most Recent 2 years ago
Selected Answer: D
Nobrainer D
upvoted 1 times

mmraouf 2 years, 3 months ago
Starting in July 2022, Microsoft is deprecating Windows Information Protection (WIP). Microsoft will continue to support WIP on supported 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 2 years, 7 months ago

Selected Answer: D

User Override

upvoted 2 times

Eggsamine 3 years, 2 months ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 2 times

B1G_B3N 3 years, 9 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 an override is to ALLOW them to do it not DENY them.

upvoted 2 times

Chipper 3 years, 5 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 but also make is so the user cannot over ride it to send the content.

upvoted 2 times

mkoprivnj 4 years ago

D for sure!

upvoted 4 times

HenriksDisciple 2 years, 9 months ago

are all your 660 comments "___ for sure!"? Your comments don't really add anything except your opinion.

upvoted 3 times

Noppawat 4 years 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 5 times

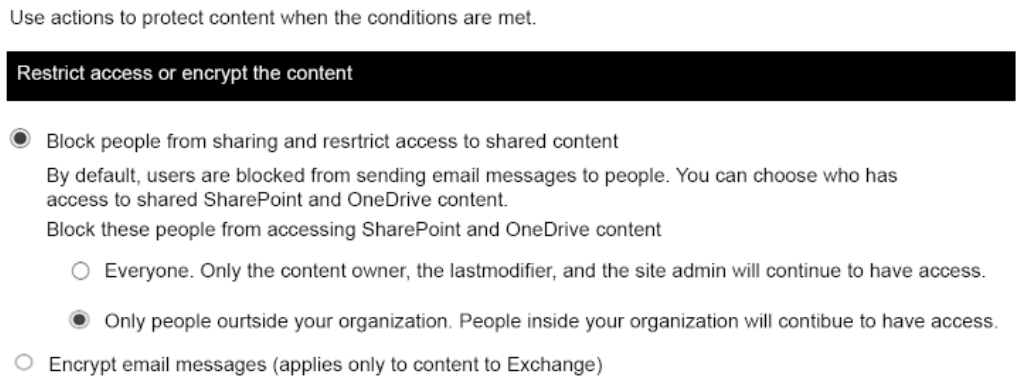
Larency 4 years, 5 months ago

exception

upvoted 2 times

Question #29 *Topic 2*

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

Suggested 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

Community vote distribution
D (100%)

birzorirko Highly Voted 3 years, 7 months ago
D is the way.
upvoted 11 times

zaicnupagadi 2 years, 8 months ago
They want the D
upvoted 8 times

Eggsamine Highly Voted 3 years, 2 months 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 for MS-101 be removed from this dump or are these questions actually coming up on the exam?
upvoted 5 times

TechMinerUK 2 years, 6 months 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 3 times

manwithplan 2 years, 4 months ago
This is correct. When I did the MD100 exam, there were quite a few MD101 questions in the exam.
upvoted 2 times

Startkabels Most Recent 2 years ago

Selected Answer: D

Nobrainer D

upvoted 2 times

Eggsamine 3 years, 2 months ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 1 times

Landy360 3 years, 3 months ago

"Only people ourtside of your organization..."

upvoted 5 times

Question #30 *Topic 2*

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.

Suggested 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

Community vote distribution

SMHH Highly Voted 4 years, 10 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-the-dlp-policy
upvoted 59 times

praveen97 4 years, 6 months ago
Agree with SMHH and the article clearly says that Managed property has to be added to SharePoint Search schema in SP Admin Center.
upvoted 3 times

VTHAR 4 years, 2 months ago
Agreed! Correct answer is A.
upvoted 5 times

WoneSix 4 years, 10 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 create a managed property in the SharePoint admin center."
upvoted 8 times

Ama100 Highly Voted 4 years, 9 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 content 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 are 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-worldwide
upvoted 19 times

[Removed] 4 years, 5 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-or-other-properties

upvoted 8 times

st2023 Most Recent 1 year, 8 months ago

Selected Answer: A

if the question asked for two answers in order would A then C be correct?

upvoted 1 times

srs1020 1 year, 9 months ago

This is an MS-500 question - on exam back in 09/2022

upvoted 1 times

Meebler 1 year, 9 months ago

Answer: A. From the SharePoint admin center, create a managed property.

Explanation: To implement DLP policies for uploaded files based on the Confidential classification, first create a managed property in the SharePoint admin center that maps the on-premises FCI classification to a property in SharePoint Online.

upvoted 1 times

Startkabels 2 years ago

Selected Answer: A

No idea but A it is then!

upvoted 2 times

charat 2 years, 7 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties?view=o365-worldwide

Here's a working link for the MS article

upvoted 1 times

Durden871 2 years, 10 months ago

This cannot possibly be an MS-100 question.

upvoted 1 times

Eggsamine 3 years, 2 months ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 3 times

Eggsamine 3 years, 2 months 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 for MS-101 be removed from this dump or are these questions actually coming up on the exam?

upvoted 1 times

Durden871 2 years, 10 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 pushing 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 3 years, 10 months ago

MS-101 question

upvoted 7 times

mkoprivnj 4 years ago

A for sure!

upvoted 3 times

k2kimmy 4 years, 1 month 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 4 years, 1 month 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 4 years, 2 months ago

to be specific "implement data loss prevention (DLP) policies for the uploaded files based on the classification"

upvoted 1 times

Jayatheerthan 4 years, 2 months ago

It says" uploaded files" . This means they have already have Managed property created and uploaded the content.

upvoted 2 times

[Removed] 4 years, 5 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

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.

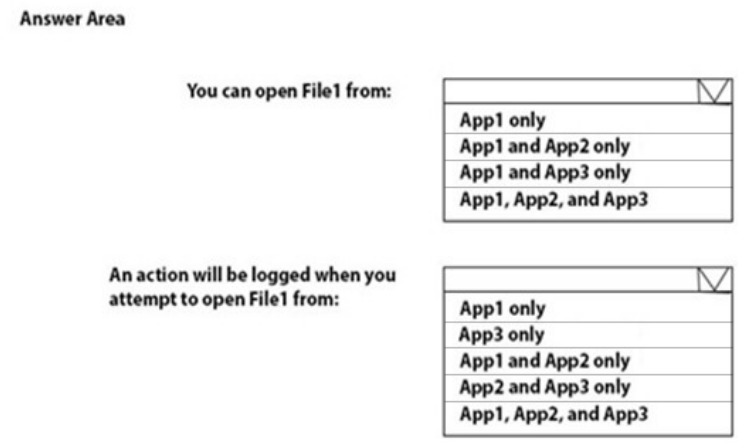
Your company uses Windows Information Protection (WIP). WIP has the following configurations:

- Windows Information Protection mode: Silent
- Protected apps: App1
- Exempt apps: App2

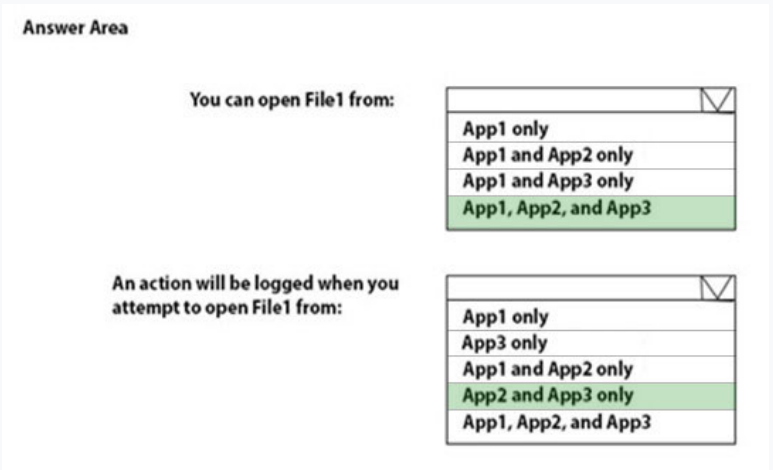
From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

Hot Area:



Suggested 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 4 years, 10 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 70 times

Rosco 4 years, 7 months ago

I think everyone is wrong. I believe inappropriate actions "sharing data" ie. cut and paste are allowed but logged in Silent. Opening in 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-data-using-wip

upvoted 6 times

STFN2019 4 years, 5 months ago

Perfect. Box1: all apps, Box2: App3 only

upvoted 20 times

sailerjerry Highly Voted 4 years, 11 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 30 times

donb21 Most Recent 2 years, 4 months ago

Box 1 should be 1,2,3 and Box2 should be only App3

upvoted 2 times

DenisRossi 2 years, 6 months ago

MS-101 question

upvoted 3 times

Eggsamine 3 years, 2 months ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 3 times

Razuli 1 year, 11 months ago

Yeah I did

upvoted 2 times

MomoLomo 3 years, 4 months 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 verifying 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 enforcement policy, Block.

WIP runs silently, logging inappropriate data sharing, without blocking anything that would have been prompted for employee interaction while in Allow Override mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are 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 3 years, 7 months ago

Ms-101question

upvoted 4 times

Mr01z0 3 years, 7 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 large 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 Overrides 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 does 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 3 years, 8 months ago
is this on the test?
upvoted 1 times

YounesDump 3 years, 9 months ago
i think that skajam66 is right ;
upvoted 1 times

Parvezg 3 years, 10 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, logs will be generated for such type of actions for App1 only because that is the protected app.
upvoted 2 times

Duyons 3 years, 10 months ago
MS-101 question - MS-100 does not cover WIP
upvoted 6 times

Turak64 3 years, 4 months ago
it shoudn't, but this is a MS exam... they tend to pull this sort of thing
upvoted 2 times

Razuli 1 year, 11 months ago
No it doesn't cover this like most of the material in the ms100 but it's definitely in there a I seen it
upvoted 1 times

Takloy 4 years ago
so what's the correct answer?
upvoted 1 times

mkoprivnj 4 years ago
1, 2, 3 & 2, 3.
upvoted 4 times

palani75 4 years, 2 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 enabled apps but also apps you did not add to your WIP policy.
upvoted 10 times

Jayatheerthan 4 years, 2 months ago
Silent mode. The Windows Information Protection-protected work files can be moved or copied to the user's personal local OneDrive sync folder, the files will sync without issue, and an audit log event will be generated.
upvoted 1 times

LucWave 4 years, 3 months ago
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. 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

Question #32 *Topic 2*

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

Suggested 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

Community vote distribution
A (100%)

subbuhotmail Highly Voted 3 years, 5 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 8 times

PDR 3 years, 5 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 AAD 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 6 times

PDR 3 years, 5 months ago
and by not correct in this question, I mean Autopilot is not correct
upvoted 2 times

lengySK Highly Voted 3 years, 4 months ago
It looks like a question from MD100
A: https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages
upvoted 6 times

Exam99111 Most Recent 1 year, 9 months ago
A for provisioning package.
No tenant is no autopilot, inplace upgrade keeps the unwanted apps. Wipe and refresh does not make required changes.

upvoted 1 times

Startkabels 2 years ago

Selected Answer: A

A for provisioning package.
No tenant is no autopilot, inplace upgrade keeps the unwanted apps. Wipe and refresh does not make required changes.

upvoted 1 times

BoxGhost 2 years, 8 months 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 3 times

Eggsamine 3 years, 2 months ago

Has anyone had this show up in the MS-100 exam as it is an MS-101 question?

upvoted 1 times

stoneface 2 years, 12 months ago

You've asking the same question. So, in this case this is completely related to MS-100.

upvoted 2 times

xofowi5140 3 years, 2 months 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

Azuz 3 years, 5 months ago

A
Windows provisioning makes it easy for IT administrators to configure end-user devices without imaging. Using Windows provisioning, an IT administrator can easily specify desired configuration and settings required to enroll the devices into management and then apply that configuration to target devices in a matter of minutes. It is best suited for small- to medium-sized businesses with deployments that range 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 them to configure their device. This can result in a significant reduction in the time required to configure multiple devices in your organization.

upvoted 2 times

goape 3 years, 6 months ago

100% A

upvoted 3 times

JordanJammer 3 years, 6 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 3 years, 6 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 level defined in the package manifest is used to resolve setting conflicts. The pre-defined package owner types are listed below in the order of 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

[Removed] 3 years, 7 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 3 years, 6 months ago

Yes, you can, and you can also provide to your own wim image to your preferred vendor,

upvoted 1 times

tungbache 3 years, 8 months ago

ms - 101 question ?

upvoted 2 times

Bobalo 3 years, 5 months ago

Pretty sure I had this one on my MS-101 exam.

upvoted 1 times

james1 3 years, 10 months ago

Provisioning package for sure - https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages lists all of the requirements

upvoted 4 times

mkoprivnj 4 years ago

A for sure!

upvoted 2 times

Alvaroll 4 years, 3 months ago

1-32 https://www.examtopics.com/exams/microsoft/ms-100/view/7/

upvoted 4 times

Learner3000 4 years, 5 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 3 times

JaBe 4 years, 5 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 software"

https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

upvoted 11 times

Question #33 *Topic 2*

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.

Suggested 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 (57%) B (43%)

Ronald82 Highly Voted 5 years, 3 months 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 ATP will not take care of malicious files within SharePoint Online.
upvoted 44 times

VTHAR 4 years, 2 months ago
Yes, it should be Office 365 ATP.
upvoted 5 times

mikl 2 years, 4 months ago
Which is named : Microsoft Defender for Office 365 now.
upvoted 3 times

Cyclops74 Highly Voted 5 years ago
I agree with both remarks: indeed you can enable malware detection in Cloud App Security, but you need an Office 365 ATP license. Since that is not mentioned, in this case the answer should be A. See: https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy
upvoted 14 times

ijarosova Most Recent 1 year, 9 months ago
Selected Answer: A
I vote A
upvoted 1 times

DeLoc 1 year, 10 months ago
Selected Answer: A
Office 365 Cloud App Security is a comprehensive security management and threat protection service that can be used to detect and respond to potential security threats in Microsoft 365, including SharePoint Online. It allows you to create policies that monitor activity and generate alerts based on specific criteria, such as the detection of malware in SharePoint documents.
upvoted 1 times

Startkabels 2 years ago
Selected Answer: B
It's B.
Nowadays this policy is made in the Purview portal (compliance.microsoft.com), under Alerts > New Alert policy: Activity is: Detected malware in

file (description: Office 365 detected malware in either a SharePoint or OneDrive file).
Learn more link in the top of the Alert Policy page brings you to an article that reads you need Defender for this.

https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies?redirectSourcePath=%252farticle%252f8927b8b9-c5bc-45a8-a9f9-96c732e58264&view=o365-worldwide
upvoted 1 times

vanr2000 1 year, 9 months ago
The problem is, they're talking about Windows ATP, for the client, not SharePoint. That's the tricky part of the answer.
upvoted 1 times

simoen 2 years, 3 months ago
Selected Answer: A
cloud app security
upvoted 1 times

pozzetttt 2 years, 3 months 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 years, 5 months 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 2 years, 4 months ago
I tend to agree.
upvoted 1 times

aaron_roman 2 years, 5 months ago
Selected Answer: A
it should be a
upvoted 1 times

aaron_roman 2 years, 5 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 2 years, 6 months 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 3 times

DenisRossi 2 years, 6 months ago
Selected Answer: B
B is the correct, stop voting A.
upvoted 3 times

mikaiwhodakno 2 years, 6 months ago
Sorry but that is not correct. Look at the wording, Windows Defender ATP protects endpoints and PCs, it does not protect Sharepoint online, therefore the correct answer is A. This is commonly confused with the various products known as Cloud App Security, or Office 365 ATP (now Microsoft Defender for Office 365), which WILL scan and protect Sharepoint.
upvoted 3 times

DenisRossi 2 years, 6 months ago

I see, you are right! I've made a mistake with the names!!!
Thank you!
upvoted 2 times

gaem 2 years, 6 months ago

Selected Answer: B

B is the right answer.
Stop voting A
upvoted 1 times

mikaiwhodakno 2 years, 6 months ago

Sorry but that is not correct. Look at the wording, "Windows Defender ATP" protects endpoints and PCs, it does not protect Sharepoint online, therefore the correct answer is A. This is commonly confused with the various products known as Cloud App Security, or Office 365 ATP (now Microsoft Defender for Office 365), which WILL scan and protect Sharepoint. The "Windows" naming gives it away as the wrong answer.
upvoted 1 times

gaem 2 years, 7 months ago

Selected Answer: B

ATP is the answer
upvoted 1 times

mikaiwhodakno 2 years, 6 months 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 2 years, 7 months 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 for Endpoint. "
Source:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows
upvoted 2 times

joergsi 2 years, 11 months 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 365. 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 3 years, 1 month 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)

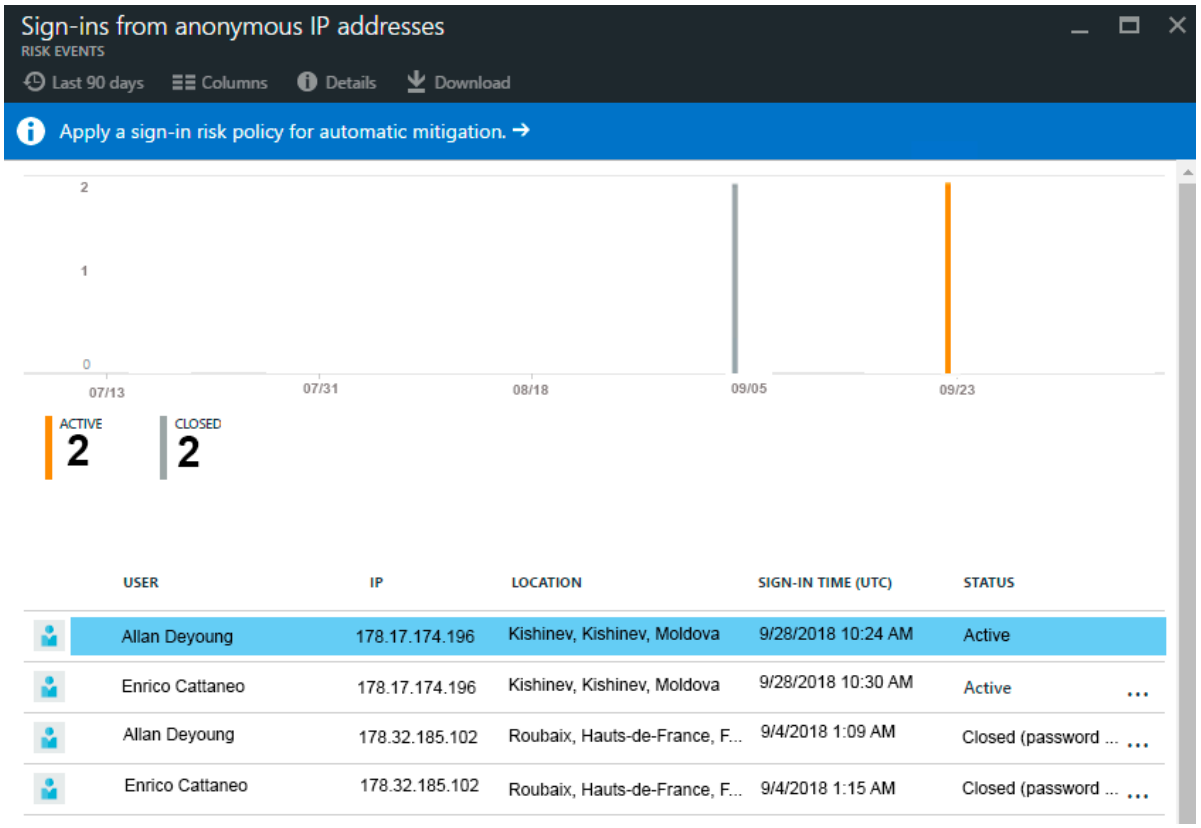
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy
upvoted 3 times

Durden871 2 years, 10 months ago

I doubt recent changes are reflected in the test, but I could be wrong.
upvoted 1 times

Question #34 *Topic 2*

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.

Suggested 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%)

melatocaroca Highly Voted 3 years, 6 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 6 times

Jol 3 years, 6 months ago
Agree!
upvoted 1 times

mikl Most Recent 2 years, 4 months ago
Selected Answer: B
Seems ok.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
upvoted 3 times

gxsh 3 years, 4 months ago
Correct!
upvoted 2 times

Manojch 3 years, 7 months ago
correct
upvoted 3 times

Question #35 *Topic 2*

DRAG DROP -

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

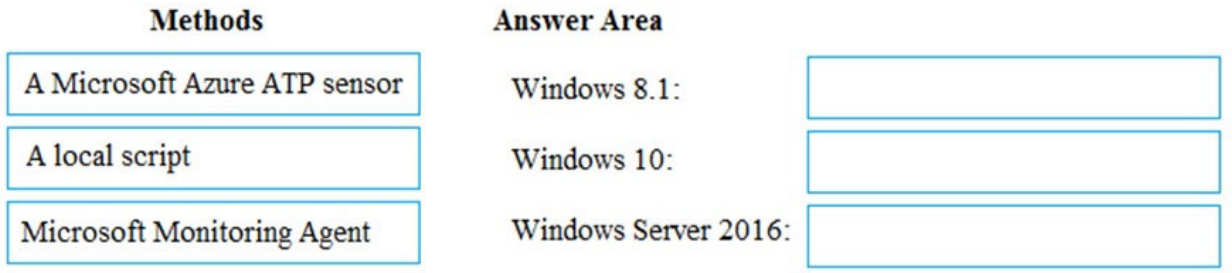
Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Windows Defender Advanced Threat Protection (ATP). The solution must avoid installing software on the devices whenever possible.

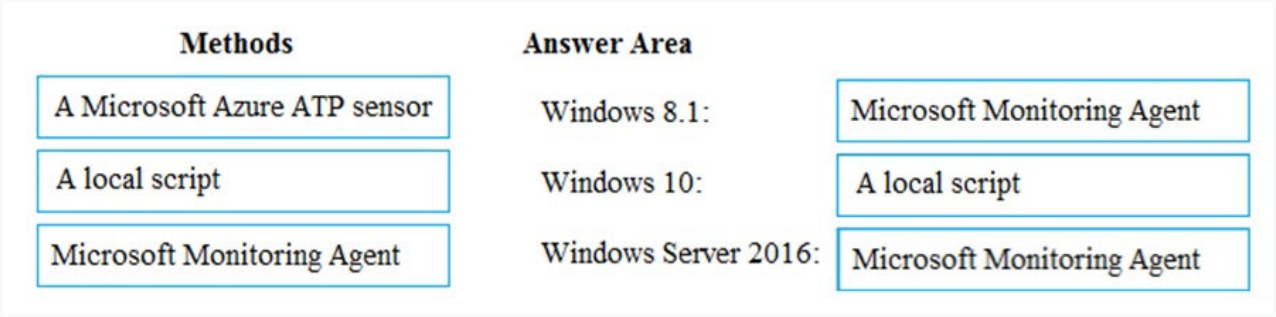
Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested 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

[Removed] Highly Voted 4 years, 5 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 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.
upvoted 17 times

RNG60FR Highly Voted 3 years, 11 months ago

This cannot be an MS-100 exam question.
upvoted 14 times

Turak64 3 years, 4 months 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 adding in questions that are totally out of scope.
upvoted 10 times

suvittech Most Recent 1 year, 11 months ago

1- Microsoft Monitoring Agent
2- Local Script
3- Local Script

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-windows-client?view=o365-worldwide
upvoted 5 times

H_ngM_n 2 years, 3 months ago

i agree
upvoted 1 times

H_ngM_n 2 years, 3 months ago

with windows server 2016 using local script
upvoted 1 times

mmraouf 2 years, 3 months 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 10 times

aaron_roman 2 years, 5 months ago

Box 1 - MMA
Box 2 &3 Local script to comply with the requirement "avoid installing software when possible"
upvoted 2 times

mikaiwhodakno 2 years, 6 months ago

The "avoid installing software when possible", combined with local script available from 2012 R2-newer means local script for Win10 and 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 actually accept as correct?
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide
upvoted 1 times

TechMinerUK 2 years, 6 months 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 GPO 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 Monitoring 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 2 years, 6 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 2 years, 7 months 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 3 years ago
Now its possible to onboard win 2016 and 2012r2 with installation package and after that onboard package
upvoted 1 times

JAPo123 3 years, 4 months ago
in ms-100 exam last friday.
upvoted 7 times

JAPo123 3 years, 4 months ago
In exam last friday.
upvoted 2 times

melatocaroca 3 years, 6 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 agent
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/protecting-windows-server-with-windows-defender-atp/ba-p/267114
upvoted 1 times

jroxas 3 years, 8 months ago

I saw this question on MS-101.

upvoted 5 times

Candice79 3 years, 8 months ago

This seems like a question for the MS 500 not the MS 100.

upvoted 5 times

Rstilekar 3 years, 11 months ago

Seems not a right question and any explainations either. Ques looks outdated

upvoted 2 times

Question #36 *Topic 2*

HOTSPOT -

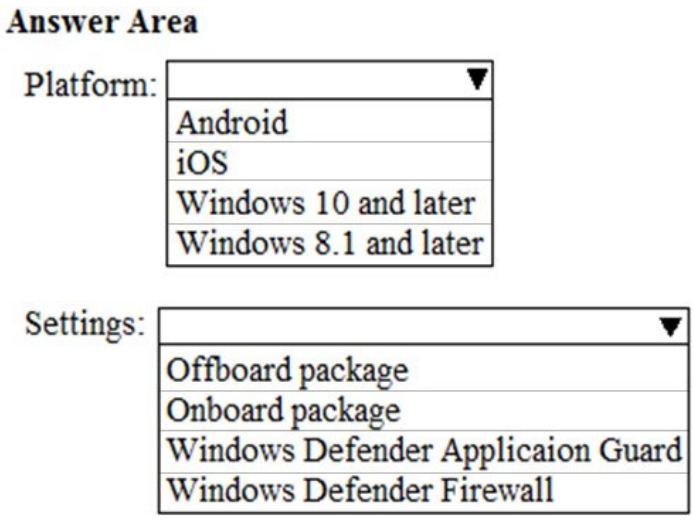
You have a Microsoft 365 subscription.

You need to implement Windows Defender Advanced Threat Protection (ATP) for all the supported devices enrolled devices enrolled on mobile device management (MDM).

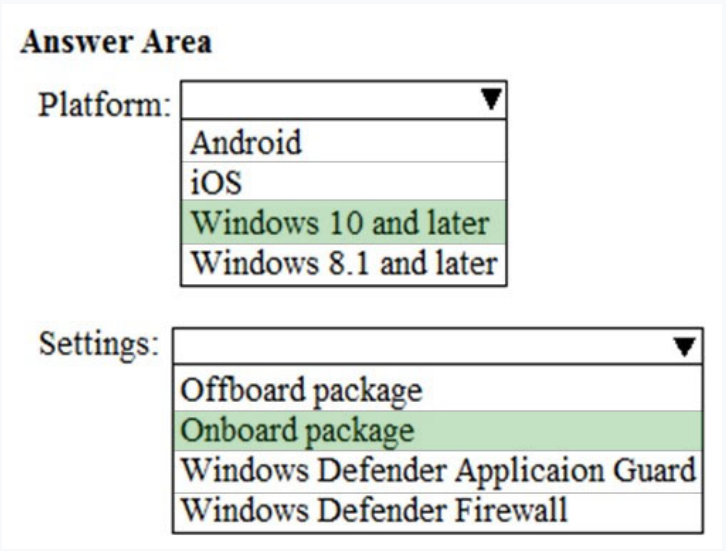
What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested 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

[Removed] Highly Voted 4 years, 4 months 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 2 years, 9 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 4 times

Davidchercm 2 years, 11 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 2 years, 7 months ago
There is no "all" option.
upvoted 1 times

Paolo2022 2 years, 1 month ago
Well, Windows 8.1 won't work. But the other options will. Probably an outdated question.

https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#onboard-devices
upvoted 1 times

melatocaroca 3 years, 6 months ago
They ask to use mobile device management for all the supported devices enrolled devices enrolled on and implement Windows Defender 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 3 years, 7 months ago
is this question still valid with the recent changes in Intune?
upvoted 1 times

RNG60FR 3 years, 11 months ago
This cannot be an MS-10 Exam question.

upvoted 1 times

bog23 3 years, 9 months ago
yes, o365
upvoted 2 times

airairo 3 years, 7 months ago
it is MS 101
upvoted 2 times

mkoprivnj 4 years ago
W10 + onboarding package.
upvoted 3 times

madsa 4 years, 1 month 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 4 years, 3 months 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 4 years, 2 months ago
yes. it was asked in exam.
upvoted 3 times

Kabir93 4 years, 3 months 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 3 years, 4 months ago
Because that's how Microsoft roll...
upvoted 2 times

JohnO1971 4 years, 8 months ago
Microsoft Defender ATP works with devices that run Windows 10 or later, and with Android devices.
upvoted 2 times

JohnO1971 4 years, 8 months ago
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection
upvoted 1 times

PhantomPhixer 4 years, 7 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 to onboard win 10, which is the onboard package referenced in the answer and the link
upvoted 1 times

madmouse256 4 years, 8 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 4 years, 9 months ago
win 8.1 support Defender ATP. why chosen "Windows 10 and later"?
upvoted 3 times

madmouse256 4 years, 8 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.

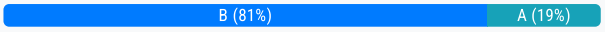
B. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.

C. From the Azure Active Directory admin center, modify the conditional access policy.

D. From Microsoft Cloud App Security, create an app discovery policy.

Suggested 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



joelfrancisco Highly Voted 5 years, 2 months ago
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Impossible travel is on anomaly detection policy see link
upvoted 29 times

WoneSix 4 years, 10 months ago
Thanks, joel - that's the link that should ahve been referenced in the answer. :-(
upvoted 1 times

asdkjhbfc Highly Voted 4 years, 7 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 alert 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 (you 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 3 years, 12 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 3 years, 7 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 over a dozen answers in one exam that differe from
both here & Udemy
upvoted 3 times

lucidgreen 3 years, 9 months ago
asdkjhbfc said that you cannot link an app in anomaly policy but you can in impossible travel policy.

upvoted 2 times

NrdAlrt Most Recent 1 year, 5 months ago

I think it's A. Seems like a classic MS cert question where two answers are potentially right, but one is more right due precedence in what needs to be done first and foremost in order to accomplish the goal. I hate that THIS is how they challenge your knowledge of the subject matter. Making a test confusing and misleading doesn't mean the results indicate who is a better SME.

upvoted 1 times

ijarosova 1 year, 9 months ago

Selected Answer: A

I vote A.

upvoted 1 times

Meebler 1 year, 10 months ago

B,

Option A (creating a Cloud Discovery anomaly detection policy) is incorrect because it is used to detect anomalous behaviors across all apps and cannot be configured to generate alerts for a specific app like App1.

Option C (creating an app discovery policy) is incorrect because it is used to discover and assess apps used by employees in an organization, but not to generate alerts for impossible travel.

Option D (modifying the conditional access policy from the Azure Active Directory admin center) is incorrect because conditional access policies are used to control access to apps based on certain conditions, but they cannot be configured to generate alerts for impossible travel events.

upvoted 1 times

Meebler 1 year, 10 months ago

To be alerted by email if impossible travel is detected for a user of App1 while ensuring that alerts are generated for App1 only, you should modify the impossible travel alert policy in Microsoft Cloud App Security.

Therefore, the correct answer is B. From Microsoft Cloud App Security, modify the impossible travel alert policy.

By modifying the impossible travel alert policy in Microsoft Cloud App Security, you can configure email alerts for impossible travel events that are specific to App1. Conditional Access App Control can be configured as part of the policy to enforce restrictions on App1's access if the user's travel is flagged as impossible.

upvoted 1 times

T10T 2 years, 4 months 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 and then create a filter for "App1".

upvoted 8 times

Storm 2 years, 6 months 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 5 times

Chris1972 2 years, 6 months ago

all of the above

upvoted 1 times

DenisRossi 2 years, 6 months 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 2 years, 6 months ago

Ans: B, refer to https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy#impossible-travel

upvoted 2 times

TechMinerUK 2 years, 6 months 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 on the new configuration.

Any specific granular policies should be created additionally to the default policy to add more protection rather than removing it from 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 apps

upvoted 2 times

salla 2 years, 9 months ago

Selected Answer: A

tested

upvoted 1 times

rockey90 2 years, 10 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

mikaiwhodakno 2 years, 6 months ago

But there is no option there as stated in the question to only protect App1, therefore B is the answer.

upvoted 2 times

T10T 2 years, 4 months 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 Anomaly detection policy. You will need to create a new policy and filter for App1.

upvoted 1 times

AlexLiourtas 2 years, 11 months ago

Selected Answer: B

tested, ans B

upvoted 1 times

kanag1 2 years, 11 months 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 link 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 2 years, 6 months 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 3 years, 5 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 3 years, 6 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 policy you also choose what kind, one does not cover all.

upvoted 3 times

BGM_YKA 3 years, 7 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 for 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 3 years, 9 months ago

Always create a custom policy. Never modify default policies.

upvoted 3 times

lucidgreen 3 years, 9 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

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.

Suggested 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 5 years, 2 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 49 times

Alvaroll 4 years, 3 months 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 Standalone Sensor on a separate server. The standalone sensor monitors traffic that you direct to it by using port mirroring on your network switches."
upvoted 6 times

VTHAR 4 years, 2 months ago
Yes. Correct answer is A. Same question in MS-101.
upvoted 8 times

[Removed] 3 years, 11 months ago
Agreed
upvoted 1 times

mshorty Highly Voted 4 years, 11 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-threat-protection/atp-capacity-planning#choosing-the-right-sensor-type-for-your-deployment
upvoted 9 times

BigDazza_111 Most Recent 1 year, 8 months ago
I hope the exam questions are clearer that this. The way i read it is, the company has a secuirty policy (writen) not configured, to not install any app on DC. And we need to use aATP sensor to monitor and report on this...the scenario does not specify that that it need to be monitored from the DC, but answer is indicated this was in the mind of the question creator.
upvoted 1 times

ijarosova 1 year, 9 months ago
Selected Answer: A
I vote A.
upvoted 1 times

jaysoft 2 years ago

Selected Answer: A

If you don't want to deploy the Azure ATP Sensor directly on your domain controllers, you can instead deploy the Azure ATP Standalone Sensor on a separate server. The standalone sensor monitors traffic that you direct to it by using port mirroring on your network switches.

https://practical365.com/azure-atp-intro/

upvoted 2 times

Arlecchino 2 years, 3 months ago

Selected Answer: A

A is the way imo

upvoted 1 times

aaron_roman 2 years, 5 months ago

Selected Answer: A

no doubt A

upvoted 1 times

sliix 2 years, 10 months ago

Selected Answer: A

This is the answer. Trust me bro :)

upvoted 2 times

AlexLiourtas 2 years, 10 months ago

source: "dude trust me"

upvoted 20 times

tf444 3 years 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 2 years, 6 months 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 3 times

08twitch 3 years ago

Selected Answer: A

Update answer to A

upvoted 3 times

AlexLiourtas 3 years, 1 month ago

Selected Answer: A

A, you cannot install on active directory due to policy

upvoted 1 times

zacmzee 3 years, 3 months 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 on domain controllers." That being said you can install Azure ATP standalone sensor on domain controller.

upvoted 1 times

Panku 3 years, 3 months 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 directly on a domain controller.

upvoted 2 times

jeffyeh 3 years, 4 months 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 2 years, 6 months 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 3 years, 4 months ago

I think correct is A

upvoted 1 times

Azreal_75 3 years, 5 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

Paolo2022 2 years ago

I found this (current) reference in MS Learn: https://learn.microsoft.com/en-us/defender-for-identity/configure-port-mirroring

Also, I do think that A is the correct answer.

upvoted 1 times

mkuczynski 3 years, 6 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

Question #39 *Topic 2*

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

Suggested 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%)

[Removed] Highly Voted 4 years, 5 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 20 times

Duyons Highly Voted 3 years, 10 months ago
Not an MS-100 question but MS-101.
upvoted 10 times

Moderator Most Recent 2 years, 4 months ago
Selected Answer: B
Valid question (30th july 2022)
upvoted 3 times

mkoprivnj 4 years ago
B for sure!
upvoted 4 times

donathon 4 years, 2 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 4 years, 7 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 4 years, 6 months ago

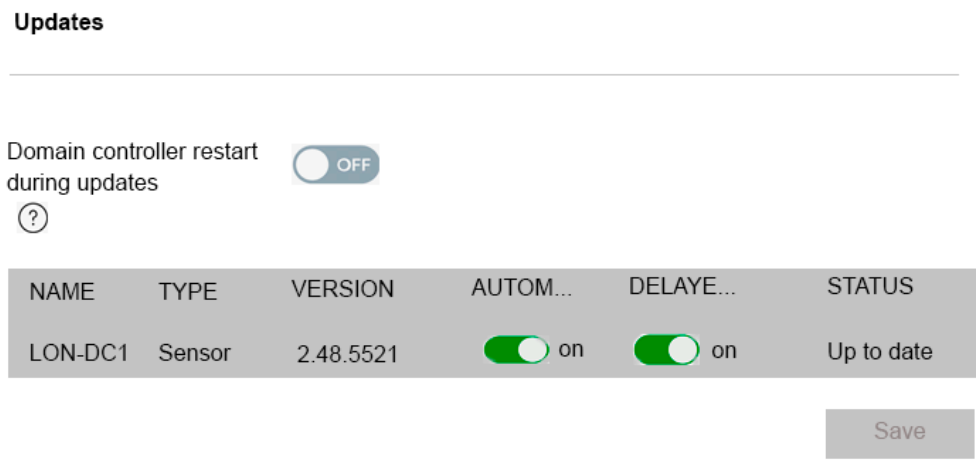
It states "You plan to onboard all devices data to Europe". So you need to remove the devices from the USA servers first

upvoted 6 times

Question #40 *Topic 2*

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

Suggested 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

Community vote distribution
E (100%)

HobGoblinTank Highly Voted 5 years, 2 months ago
I believe this is now 72 hours - https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update
upvoted 28 times

dailyup 3 years, 8 months ago
This question has shown in MS-100 and E is 24 hours. The correct answer is 72 hours.
upvoted 1 times

VTHAR 4 years, 2 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 4 times

Goofer Highly Voted 4 years, 10 months ago
Answer E is changed in the exam to 72 hours
upvoted 10 times

agnesmandriva Most Recent 1 year, 10 months ago

Selected Answer: E

Sensors selected for Delayed update start their update process 72 hours after the Defender for Identity cloud service is updated
https://learn.microsoft.com/en-us/defender-for-identity/sensor-settings
Correct
upvoted 2 times

Rlcky 3 years, 3 months 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 3 years, 6 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 3 years, 9 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 4 times

mikl 3 years, 9 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 update of Azure ATP. See Azure ATP sensor update for configuration instructions."
upvoted 2 times

rRefJr 3 years, 9 months ago

"Sensors not selected for delayed update are updated automatically, each time the Defender for Identity service is updated. Sensors set to 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 3 years, 11 months ago

delayed update is 72 hours
upvoted 1 times

mkoprivnj 4 years 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 4 years, 3 months ago

Meant to add the link
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new
upvoted 1 times

scottims 4 years, 3 months 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 update of Azure ATP. See Azure ATP sensor update for configuration instructions.
upvoted 1 times

Ben22 4 years, 4 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

[Removed] 4 years, 5 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 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
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new
upvoted 5 times

zordss 4 years, 8 months ago
guys, look at the vers. in the screenshot. 25 is correct for v2.48.
upvoted 2 times

TonySuccess 4 years, 6 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. So 72.
upvoted 1 times

itmp 4 years, 8 months ago
version is 2.48 so it is 24hours - no one talks about new versions ..
upvoted 6 times

Jhill777 4 years, 7 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 4 years, 6 months ago
72 hours delay is correct
upvoted 1 times

KingJulian 4 years, 10 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 update of Azure ATP.
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new#azure-atp-release-262
upvoted 2 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

Suggested 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 5 years, 2 months ago
A should be the correct one?
upvoted 56 times

PeterC 3 years, 7 months ago
Off course A - Subscription Activation
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 13 times

[Removed] 4 years, 5 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 3 years, 7 months ago
Correct answer is A
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 5 times

VTHAR 4 years, 2 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 to switch from Win10 Pro to Ent by just assigning license, log off and log on. https://youtu.be/bk9wWc7x_m4
upvoted 29 times

Jayatheerthan 4 years, 2 months ago

Yes, this is there in MS-101 and the answer is A: Windows Autopilot
upvoted 2 times

Jayatheerthan 4 years, 2 months ago
In MS-101 the answer is A:Windows Autopilot. Here the answer is C.
upvoted 1 times

VTHAR 4 years, 2 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 5 times

Takloy 3 years, 11 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 downtime for the users, if you do autopilot, there will definitely be more down time due to the nature of autopilot.
upvoted 5 times

Cyclops74 Highly Voted 5 years, 1 month ago
Indeed, answer is A:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 32 times

BigDazza_111 Most Recent 1 year, 8 months ago
A- as stated here under Dynamic https://learn.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
upvoted 1 times

jwfm 1 year, 11 months ago
I got the paid version and still see the WRONG answer. Correct answer is A.
AutoPilot only get device enrolled into Intune and Intune can do Edition upgrade, but question did not said Intune.
upvoted 1 times

EliasMartinelli 2 years, 2 months ago
Selected Answer: A
In paid versions it`s answer A
upvoted 3 times

Rudelke 2 years, 5 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 2 years, 6 months ago
Selected Answer: A
Go for A: https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 2 times

Gokhan83 2 years, 6 months ago
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#how-it-works
upvoted 1 times

TechMinerUK 2 years, 6 months 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 (In-place upgrade/AutoPilot)
upvoted 1 times

Conkerzin 2 years, 7 months ago

A is Correct

upvoted 2 times

Ibraheem 2 years, 8 months ago

A ---correct answer

upvoted 1 times

Pr9 2 years, 10 months ago

Selected Answer: A

A. Subscription Activation

upvoted 2 times

Mea988 2 years, 10 months 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 2 years, 11 months ago

Selected Answer: A

100% A

upvoted 1 times

AlexLiourtas 2 years, 11 months ago

Selected Answer: A

tested, ans A

upvoted 1 times

Pantoniou 3 years ago

Selected Answer: A

Answer: A

upvoted 1 times

lengySK 3 years, 4 months ago

correct A - subscription activation

https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

upvoted 1 times

Comp_technician 3 years, 7 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

Question #42 *Topic 2*

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.	○	○

Suggested 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 4 years, 10 months ago

Answer is

Device 1 > No

Device 2 > No

Device 3 > Yes

upvoted 85 times

balouchi1964 Highly Voted 4 years, 7 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 18 times

donb21 Most Recent 2 years, 4 months ago
Should be NNY right,
upvoted 1 times

Rudelke 2 years, 5 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 5 times

lengySK 3 years, 4 months ago
correct
upvoted 2 times

Ana22 3 years, 6 months ago
Had this in my MS-101 exam. Given answer is correct.
upvoted 3 times

mikl 3 years, 9 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 3 years, 10 months ago
No, No, Yes for me.
upvoted 2 times

mkoprivnj 4 years ago
No, No, Yes.
upvoted 4 times

[Removed] 4 years, 5 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 4 years, 1 month 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 4 years, 1 month ago

Sorry meant to say: Therefore, Policy 1 would apply to Device 2 and require Bitlocker.

upvoted 1 times

TonySuccess 4 years, 6 months ago

Agree with Shark, No, No, Yes.

upvoted 3 times

shark1 4 years, 6 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 most 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 4 years, 2 months ago

Agreed. Answer is NO NO YES.

upvoted 2 times

rso 4 years, 7 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 4 years, 10 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 4 years, 7 months ago

Device 2 is also part of Group 3 that requires bitlocker. Not compliant.

upvoted 2 times

Durden871 2 years, 10 months 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 the 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

Question #43 *Topic 2*

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

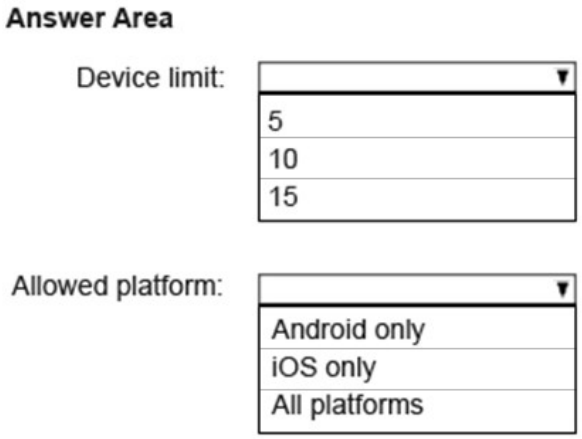
The device limit restrictions are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

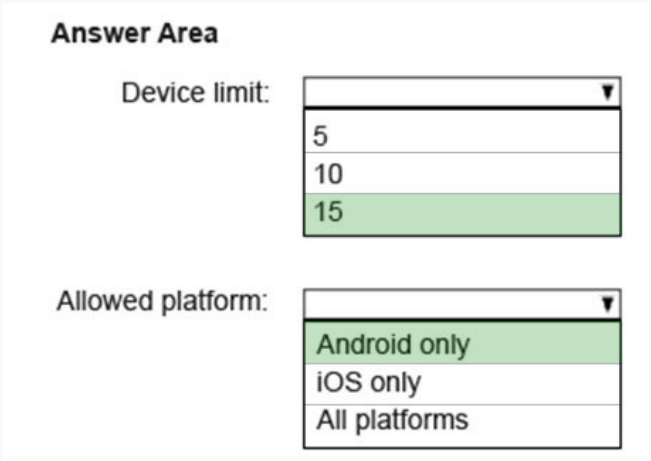
What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested 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

[Removed] Highly Voted 4 years, 5 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 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
upvoted 22 times

VP11 Highly Voted 4 years, 10 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 14 times

DoctorCOmputer Most Recent 2 years, 1 month ago
Guys it s 15 + Android and ios it s supported/.. do your research please omg!
upvoted 2 times

kravielex 2 years, 6 months ago
Correct
upvoted 1 times

Parvezg 3 years, 10 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 just above the default.

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority
upvoted 5 times

mkoprivnj 4 years ago
Android only + 15.
upvoted 4 times

Prianishnikov 4 years, 1 month ago
What is the correct answer?
upvoted 3 times

VTHAR 4 years, 2 months ago
Why is this question here since this related to EMS? It was in my MS-101 exam.
upvoted 7 times

minajahan 4 years, 10 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

Suggested 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 5 years, 1 month ago
I think the ans is A - Wipe and Load Refresh.
upvoted 45 times

[Removed] 4 years, 5 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 11 times

melatocaroca 3 years, 6 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-manager

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

Paolo2022 2 years, 1 month ago
Are you reading the links that you post?
On Autopilot: "[Y]ou don't need to prepare custom images for your devices. Instead, you can use the Windows Autopilot tools to automate Windows 10 deployment remotely."
This clearly states that you can use Autopilot instead of custom images...
upvoted 2 times

Razuli 1 year, 11 months ago

I tried to deploy custom image to systems via autopilot but found we had to deploy the blank image then push software to it so in place upgrade it is
upvoted 1 times

VTHAR 4 years, 2 months ago
Yes, answer is A. Wipe and Load refresh
upvoted 3 times

melatocaroca 3 years, 6 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 of the deployment process. The target can be the same as for the new computer scenario.
upvoted 2 times

PlasticMind 5 years ago
since this question specifically states that a custom image of windows needs to be deployed, wipe-and-load refresh i.e. the traditional 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 14 times

itmp Highly Voted 4 years, 8 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 14 times

itmp 4 years, 7 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-deployment-toolkit
upvoted 4 times

EliasMartinelli Most Recent 2 years, 2 months ago
Selected Answer: A
Answer A is right
upvoted 1 times

miry117 2 years, 5 months ago
Selected Answer: A
Wipe and Load is the best option.
upvoted 1 times

Davood 3 years, 9 months ago
Correct answer is A.
upvoted 1 times

lucidgreen 3 years, 9 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 given a choice -- next to provisioning with a wipe and refresh. Clean out all the gremlins!
upvoted 2 times

mkoprivnj 4 years ago
A for sure!
upvoted 3 times

choy1977 4 years, 1 month 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 3 years, 8 months ago
well, at the time of me reading this, yes
upvoted 1 times

k2kimmy 4 years, 1 month ago
Ans is A https://www.interfacett.com/videos/windows-10-deployment-wipe-and-load-in-place-and-provisioning/
upvoted 1 times

Martyvdb 4 years, 1 month 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 3 years, 9 months ago
Totally agree.
upvoted 1 times

csribeiro12 4 years, 1 month 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 4 years, 2 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

[Removed] 4 years, 5 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 4 years, 6 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 4 years, 3 months ago
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#dynamic-provisioning
upvoted 1 times

DJHASH786 4 years, 7 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 4 years, 6 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 the old and new operating system"
upvoted 3 times

MichealAlex5 4 years, 7 months ago

Te answer is wipe and load fresh.

upvoted 1 times

Hakimi 4 years, 8 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 by using an in-place upgrade, Windows Autopilot

upvoted 2 times

Question #45 *Topic 2*

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

Suggested 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 4 years, 12 months ago
Only Windows 10 is supported: https://docs.microsoft.com/en-us/configmgr/comanage/overview
upvoted 50 times

djlink 4 years, 4 months 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

[Removed] Highly Voted 4 years, 5 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 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
upvoted 13 times

Cafarelli Most Recent 3 years, 2 months 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 3 years, 9 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 3 years, 9 months ago
Answer is C - Windows 10 only.

https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#prerequisites
upvoted 2 times

Parvezg 3 years, 10 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 hybrid 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 2 times

estarisbourne 3 years, 11 months ago
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
upvoted 1 times

estarisbourne 3 years, 11 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 3 years, 11 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%20configuration%20is%20called management.
upvoted 1 times

paddyh 4 years ago
Windows 10 only , as for the given answer should this be co-existence
upvoted 1 times

mkoprivnj 4 years ago
Windows 10 only, so I would say C.
upvoted 1 times

mkoprivnj 4 years ago
Only Windows 10.
upvoted 1 times

Prianishnikov 4 years ago

Only Win 10 devices

upvoted 1 times

madsa 4 years, 1 month ago

Fcnet is 100% correct, co-management means managing devices with Endpoint and SCCM, meaning all platforms, this is another MS-101 exam question and the answer is on the MS-101 exam reference book. Correct answer D

upvoted 1 times

hchafloque 4 years, 3 months 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 4 years, 6 months ago

Microsoft Answer is - C. Windows 10 only

upvoted 5 times

TonySuccess 4 years, 6 months ago

Also went for C, and looking at the comments and references am confident.

upvoted 2 times

scottims 4 years, 3 months 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 4 years, 7 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 this case that means you have both solutions. What that means : you can manage Win10, Android and IOs from Intune, And Win81 and Win10 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 4 years, 7 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 4 years, 7 months ago

"Co-management requires Windows 10 version 1709 or later. Once you update Windows and configure auto-enrollment, your clients are automatically enrolled to co-management."

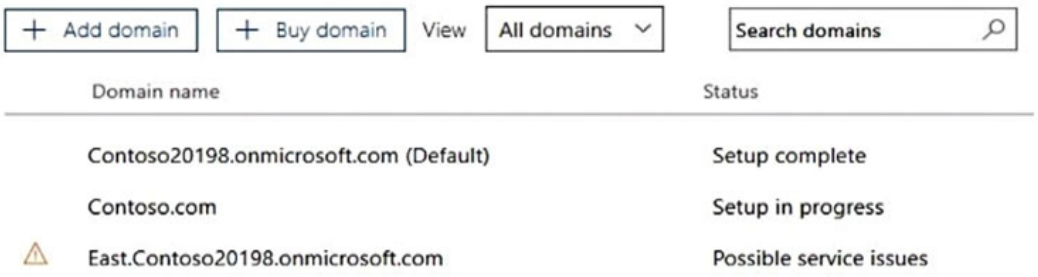
https://docs.microsoft.com/en-gb/mem/configmgr/comanage/quickstart-upgrade-win10

upvoted 1 times

Question #46 *Topic 2*

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

Suggested 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 3 years, 8 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 used with 3rd party spam filters.

upvoted 39 times

Arargnum 3 years, 8 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 the message of possible issues however because MX records are setup correctly email works fine. correct answer in this case should be C and C
upvoted 9 times

One111 2 years ago
You can't manage records for onmicrosoft.com subdomains. You can 't configure emails without having mx record, etc.
upvoted 2 times

Justin1 Highly Voted 3 years, 6 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 19 times

devilcried Most Recent 1 year, 9 months ago
Tested C&A
upvoted 1 times

renrenren 2 years, 2 months ago
1st C
2nd C - I have an example in the real world. MX records direct to a third-party antispam vendor. Users still using this domain to send and receive mail
upvoted 3 times

paweu 1 year, 7 months ago
While i agree this is a real world answer, this exam does not check for real world answers.
upvoted 1 times

Moderator 2 years, 4 months ago
Valid Question (30th july 2022)
upvoted 4 times

donb21 2 years, 4 months ago
answer I agree is C and A
upvoted 1 times

TechMinerUK 2 years, 6 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 2 years, 7 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

[Removed] 2 years, 8 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 3 times

[Removed] 2 years, 8 months ago

Prefix (not sufix)
upvoted 1 times

One111 2 years ago
Subdomain, not prefix or sufix.
upvoted 1 times

waterlego 2 years, 8 months ago
Still valid, April 2022 - variation on it though.
upvoted 2 times

Lukeford89 2 years, 8 months ago
Can anyone confirm 100 % in the exam that the answer given would be correct> what is Microsofts view?
upvoted 1 times

mfaisal786 2 years, 11 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 3 years, 1 month ago
In exam today
upvoted 2 times

xofowi5140 3 years, 2 months 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 3 years, 2 months ago
I love reading these comment, but hate it when it seems like a fight with no clue about the correct answer :(
upvoted 9 times

rfox321 3 years, 3 months 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 3 years, 3 months 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 3 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

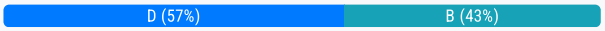
B. cutover migration

C. minimal hybrid migration

D. IMAP migration

Suggested 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

Community vote distribution



MichaelJS Highly Voted 4 years 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 Office 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 15 times

rfox321 3 years, 2 months ago
Correct - https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration
upvoted 2 times

proxyma93 Most Recent 1 year, 7 months ago
Selected Answer: D
IMAP it is. Because outlook.com is not an on prem Exchange server from which to start any sort of migration; therefore you can only do an IMAP one
upvoted 1 times

BigDazza_111 1 year, 8 months ago
Selected Answer: D
I think not B, because cutover migration is for on premise exchange servers, not mail servers hosted by third parties like outlook.com, during the cutover migration set up you need to be able to verify your domain...
upvoted 2 times

BobDobolina 1 year, 9 months ago
chatGPT
Based on the scenario you described, where the company has 20 employees and each employee has a mailbox hosted in Outlook.com, the recommended migration method would be the cutover migration to Microsoft 365.

A cutover migration is a type of migration where all mailboxes are migrated at once to Microsoft 365. This method is suitable for smaller

organizations like yours, with fewer than 2,000 mailboxes to migrate. With a cutover migration, all mailboxes, email, contacts, and calendar items are moved from Outlook.com to Microsoft 365 in a single step.

To perform a cutover migration, you need to have administrative access to the Outlook.com account and the Microsoft 365 account. You'll need to create user accounts in Microsoft 365, assign licenses, and set up email forwarding to ensure no emails are lost during the migration process.

Overall, a cutover migration is a quick and simple way to migrate mailboxes to Microsoft 365 for small businesses. However, it may not be suitable for larger organizations with more complex email systems or those that require a longer transition period.

upvoted 1 times

Rydaz 1 year, 9 months ago

its B 100%, because why IMAP? your mailbox his hosted in outlook, if you use IMAP your contacts wont be migrated, but if you use cutover your contacts will migrate to ms 365

upvoted 1 times

ijarosova 1 year, 9 months ago

Selected Answer: B

A cutover migration allows for all mailboxes to be migrated at once, which minimizes disruption to the business and reduces migration complexity

upvoted 3 times

proxyma93 1 year, 7 months ago

But the question is about private mailboxes, so there are not On Prem Exchange server to operate from to run a cutover migration. Therefore, the only possible option is IMAP

upvoted 1 times

devilcried 1 year, 9 months ago

Selected Answer: D

Definitely D

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 Office 365 for business account.

https://learn.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrating-your-outlook-com-account

upvoted 1 times

Meebler 1 year, 9 months ago

Answer: D (IMAP migration)

Explanation: In this scenario, the mailboxes are hosted on Outlook.com, which is not an on-premises Exchange server. Therefore, the other migration types (staged, cutover, and minimal hybrid) are not applicable. IMAP migration is suitable for migrating mailboxes from a non-Exchange email system like Outlook.com to Microsoft 365.

upvoted 1 times

Blagojche 1 year, 9 months ago

B. cutover migration

Explanation:

Since all the mailboxes are hosted in Outlook.com, a cutover migration would be the best migration method to use for this scenario. A cutover migration allows you to migrate all mailboxes at once and it's the simplest and most efficient migration method for small organizations with fewer than 2000 mailboxes.

An IMAP migration is used to migrate email from email systems that support the IMAP protocol, such as Gmail or Yahoo. Since the mailboxes in this scenario are hosted in Outlook.com, IMAP migration is not the best migration method to use.

upvoted 1 times

SkullRage 2 years, 4 months 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 or 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 2 years, 8 months ago

Still valid, April 2022 - Larger number (above 150) was used though so different answer.

upvoted 3 times

Ibraheem 2 years, 8 months 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 3 times

trexar 2 years, 10 months 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 3 times

Jcbrow27 3 years, 1 month 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 3 years, 4 months ago

It is on today's exam

upvoted 2 times

lengySK 3 years, 4 months 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 3 years, 5 months ago

I would also say cutover.
Any other opinion + Explanation?

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

Suggested 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 4 years ago
B for sure. MS SPO migration tool!
upvoted 6 times

diego17 Most Recent 1 year, 7 months ago
A Ferramenta de Migração do Microsoft SharePoint é usada para migrar conteúdo do SharePoint Server local para o SharePoint Online ou OneDrive no Microsoft 365. No entanto, ela não pode ser usada para identificar quais arquivos no Share1 foram modificados ou criados durante os últimos 90 dias. Portanto, a resposta correta é a opção A
upvoted 1 times

charat 2 years, 7 months ago
Selected Answer: B
05/22 Exam. B is correct
upvoted 4 times

charat 2 years, 7 months ago
Migration manager if the service mentioned is OneDrive
upvoted 1 times

TechMinerUK 2 years, 6 months 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 After.

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 3 years ago
regarding my previous answer its Migration Manager
upvoted 1 times

Wojer 3 years 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 3 years, 4 months ago
It is my today's exam
upvoted 3 times

PeterC 3 years, 7 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 2 years, 7 months ago
So even if the question were to rephrase with OneDrive, it should be SPMT. Thanks!
upvoted 1 times

Question #49 *Topic 2*

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.

Suggested 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 3 years, 7 months ago
The answer provided is correct
upvoted 11 times

spg987 Highly Voted 3 years, 4 months ago
It was my today's exam
upvoted 5 times

st2023 Most Recent 1 year, 8 months ago
Internal relay (also known as non-authoritative): Recipients for this domain can be in Microsoft 365 or Office 365 or your own email servers. Email is delivered to known recipients in Office 365 or is relayed to your own email server if the recipients aren't known to Microsoft 365 or Office 365.
upvoted 1 times

donb21 2 years, 4 months ago
The answer B is correct
upvoted 1 times

Wesje 2 years, 10 months ago

Selected Answer: B

B seems to be good.

upvoted 2 times

JakeH 3 years, 1 month ago

In exam today

upvoted 3 times

MartiFC 3 years, 5 months ago

Internal Relay is correct

upvoted 2 times

mackypatio 3 years, 7 months ago

answer is internal relay for adatum. done the same few months ago.

upvoted 4 times

dmillion 3 years, 8 months ago

no comment means B is the answer

upvoted 2 times

Question #50 *Topic 2*

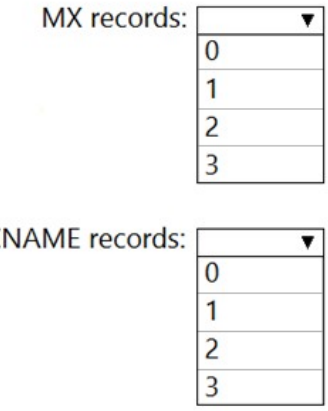
HOTSPOT -
Your company has a Microsoft 365 subscription that contains the following domains:

Contoso.onmicrosoft.com -

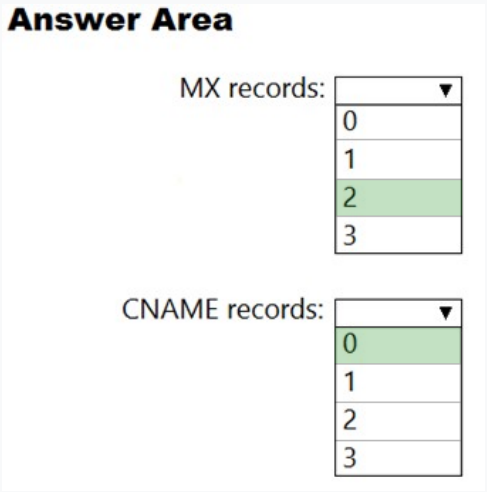
Contoso.com -
You plan to add the following domains to Microsoft 365 and to use them with Exchange Online:
- Sub1.contoso.onmicrosoft.com
- Sub2.contoso.com
- Fabrikam.com

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



Suggested Answer:



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 3 years, 9 months ago

what lmao, I get the technicality but what lmao
upvoted 22 times

proxyma93 1 year, 7 months ago
This is why I'm practising exam questions...
upvoted 1 times

monsterjuice Highly Voted 3 years, 6 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 6 times

venwaik 3 years, 5 months ago
"You plan to add the following domains" which says that contoso.com and fabrikam are not added beforehand. therefore we need to 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 MX records
upvoted 2 times

Wearsy Most Recent 3 years, 7 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 3 years, 7 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 3 years, 8 months ago
which one?
upvoted 1 times

prepre 3 years, 8 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 9 times

melatocaroca 3 years, 6 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

Question #51 *Topic 2*

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.

Suggested 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

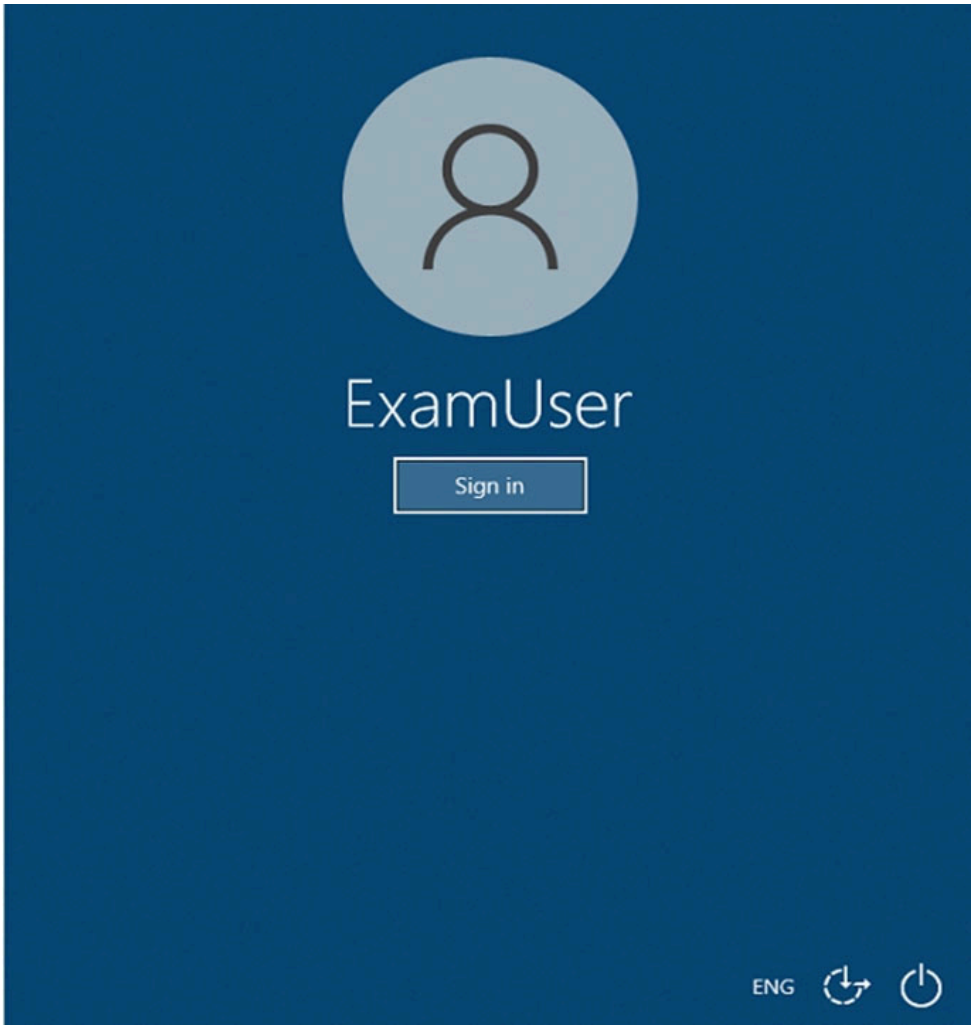
Paolo2022 2 years, 1 month ago
The question doesn't require to set up a new default domain. So that step in the answer provided would be unnecessary.
upvoted 2 times

Oval61251 2 years, 1 month ago
Admin Center----Settings------Domains----Add Domains
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 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.

Suggested 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 ג€Use Notifications to inform usersג.¦€ג€ to Off.
8. Click Save to save the changes to the policy rule.
9. Click Save to save the changes to the policy.

Paolo2022 Highly Voted 2 years ago
I doubt the question will be asked in this form.

But here is where the setting can be found by now:
Microsoft Purview compliance portal (https://compliance.microsoft.com/) > Data Loss Prevention > Policy > Default Policy (now called "Default Policy for Teams") > Edit > Name your policy: Next > Choose locations to apply the policy: toggle off Exchange > Follow the rest of the wizard and save the changes at the end.

Currently, Exchange is switched off in the default policy, so, again, I don't think this question will be asked in this form.
upvoted 5 times

Hanan1234 Most Recent 1 year, 11 months ago
it's now under https://compliance.microsoft.com/
upvoted 1 times

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

Suggested 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 4 years ago
A for sure!
upvoted 7 times

ALPHA_DELTA 3 years, 10 months ago
For sure!
upvoted 4 times

PattiD Highly Voted 4 years ago
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
upvoted 6 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

WizerEyez 1 year, 2 months ago
You can do it from "domain registrar". Means that it is from DNS provider that we subscribe like Cloudflare.
upvoted 1 times

Moderator 2 years, 4 months ago
Selected Answer: A
Valid question (30th July 2022)
upvoted 3 times

JakeH 3 years, 1 month ago
In exam today
upvoted 3 times

VictorSaiz 3 years, 2 months ago
Regarding the provided link, there is no mention to the provided answer, is there any other link which explains the correct answer? Thanks & regards
upvoted 2 times

Question #54 *Topic 2*

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

Suggested 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

Community vote distribution
B (100%)

mkoprivnj Highly Voted 4 years ago
Email only is correct answer!
upvoted 12 times

Storm 2 years, 9 months ago
Thank you so much
upvoted 1 times

vanr2000 Most Recent 1 year, 8 months ago
Selected Answer: B
You can only migrate emails. Outlook.com is an IMAP platform.

https://learn.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrating-your-outlook-com-account
upvoted 1 times

Don123 1 year, 11 months ago
B. email
C. calendar
D. contacts
upvoted 1 times

qjgwcnseeewpnarovn 2 years, 2 months ago
Selected Answer: B
Correct
upvoted 1 times

PattiD 4 years 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.

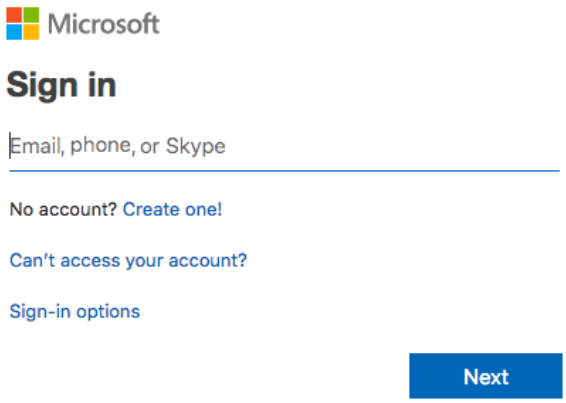
IMAP migration also doesn't create mailboxes in Microsoft 365 or Office 365. You'll have to create a mailbox for each user before you migrate their email.
upvoted 3 times

Question #55 *Topic 2*

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.

Suggested 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 Highly Voted 2 years, 3 months 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 8 times

MostWare_certificering 2 years, 1 month ago

Correct, this should be the right answer.

upvoted 1 times

PeterAth Most Recent 2 years, 1 month ago

I'm wondering if they still have these simulations in exams. I've written 3 exams and not encountered one simulation.

upvoted 3 times

rajeshrengasamy 2 years, 3 months ago

https://www.howto-outlook.com/howto/automaticreply.htm

upvoted 1 times

Question #56 *Topic 2*

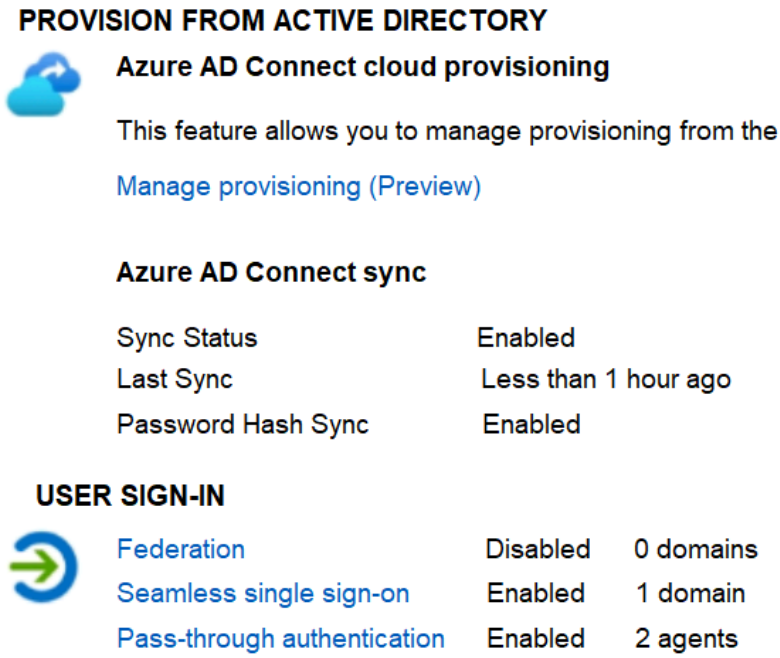
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 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

Suggested 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 (58%) B (42%)

Andy_S Highly Voted 3 years, 8 months ago

I think answer B. Adding adatum.com to custom domain does not configure ADConnect.

upvoted 16 times

tf444 3 years ago

ADATUM?

upvoted 1 times

[Removed] 3 years, 8 months ago

All users are in the contoso domain. Also the fabrikam users. No need to set up additonal ADConnect.

upvoted 6 times

Hanan1234 1 year, 11 months ago

Where did you see Adatum ??

upvoted 1 times

dngd Highly Voted 3 years, 8 months ago

I go for B. It's not mentioned that the domain is verified.

upvoted 13 times

NrdAlrt Most Recent 1 year, 5 months ago

This environment has pass through enabled on one domain which is presumably working for contoso.com. Simply adding the domain wouldn't make this work. So yeah B

upvoted 1 times

Blagojche 1 year, 9 months ago

B. No

Adding a custom domain to Azure AD and instructing User2 to sign in with that domain does not meet the goal of allowing User2 to access the resources in Azure AD.

The issue is that User2 is not able to authenticate with Azure AD using their user principal name (UPN) of user2@fabrikam.com. This is because the on-premises Active Directory user object for User2 does not have a matching user principal name in Azure AD.

To allow User2 to access the resources in Azure AD, you need to ensure that the on-premises Active Directory user object for User2 is synchronized to Azure AD and that the user object has a matching user principal name in Azure AD. You can do this by configuring Azure AD Connect to synchronize the user principal name attribute from Active Directory to Azure AD.

Therefore, the correct solution is to synchronize the on-premises Active Directory user object for User2 to Azure AD and ensure that the user object has a matching user principal name in Azure AD. Adding a custom domain to Azure AD and instructing User2 to sign in with that domain does not address the root cause of the issue.

upvoted 5 times

One111 1 year, 3 months ago

You may be right,but the reasoning given is not correct. Both domains can be configured in 1 AD forest as user suffixes. Fabrikam can be an alternative suffix in the contoso.com forest,it is nothing unusual.

upvoted 1 times

Harry83 2 years, 2 months ago

Selected Answer: B

It's not a complete answer. You need to run Az AD Connect & select the domain.

upvoted 3 times

ckanoz 2 years, 3 months 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 AD) with the @fabrikam.

upvoted 3 times

RenegadeOrange 2 years, 5 months 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 Connect is configured with Pass-through so another option is local AD is down and no-one can sign into M365. Then you would change AD Connect to use Password Hash instead.

upvoted 1 times

One111 2 years ago

And what would it give you when domain is offline and you can't sync passwords as well.

upvoted 1 times

aaron_roman 2 years, 5 months ago

Selected Answer: B

the answer is - you need to change the upn to contoso.com
upvoted 3 times

TechMinerUK 2 years, 6 months 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 a delta sync has completed they should receive fabrikam.com as a UPN suffix in AzureAD allowing them to login.
upvoted 11 times

charat 2 years, 7 months ago

Selected Answer: B

Answer is B. Domain was added according to the question, but it wasn't verified.
upvoted 4 times

jjong 3 years, 3 months ago

this qns came out in exam today
upvoted 3 times

TimurKazan 3 years, 3 months ago

Besides that, domain is not verified
upvoted 1 times

Ash473 3 years, 4 months ago

In today's exam
upvoted 3 times

venwaik 3 years, 6 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 not 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 or wait for an automatic sync cycle.

Therefore, i think, the answer should be B; "no"
upvoted 9 times

melatocaroca 3 years, 6 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 and configure the rest of required steps answer is Yes
upvoted 3 times

melatocaroca 3 years, 6 months ago

Two agents means two domains are connected, so may be YES
upvoted 3 times

venwaik 3 years, 5 months ago

Two agents means two servers with Azure AD Passtrhough authentication module installed for high availability. "Domains" showing how much domains are in sync.
upvoted 3 times

adaniel89 3 years, 6 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 sync 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 3 years, 7 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 3 years, 7 months ago

Sorry. I revew my comment and it is wrong. No need remove and resync user2. So the answer A.

upvoted 3 times

Question #57 *Topic 2*

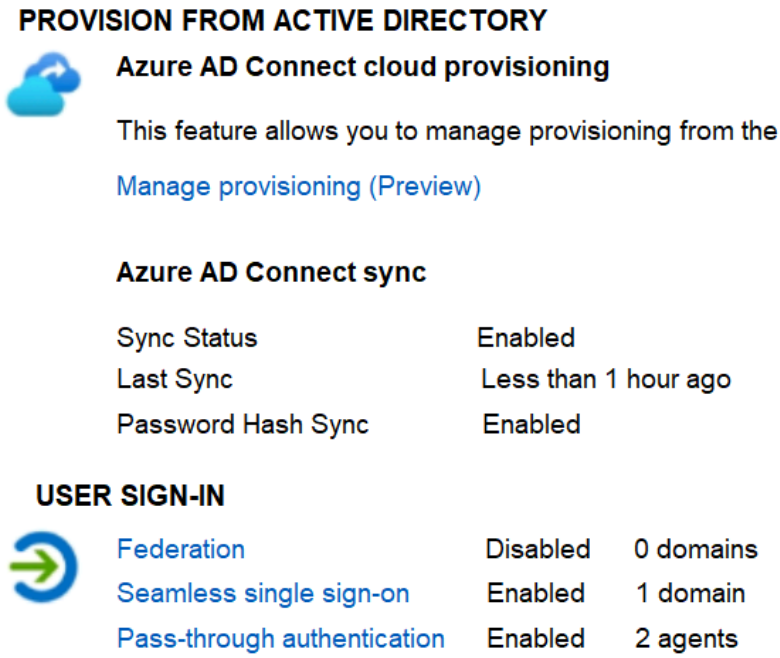
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 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

Suggested 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 3 years, 4 months ago

Correct answer

upvoted 3 times

Storm 1 year, 7 months ago

Super - Thank you

upvoted 1 times

Question #58 *Topic 2*

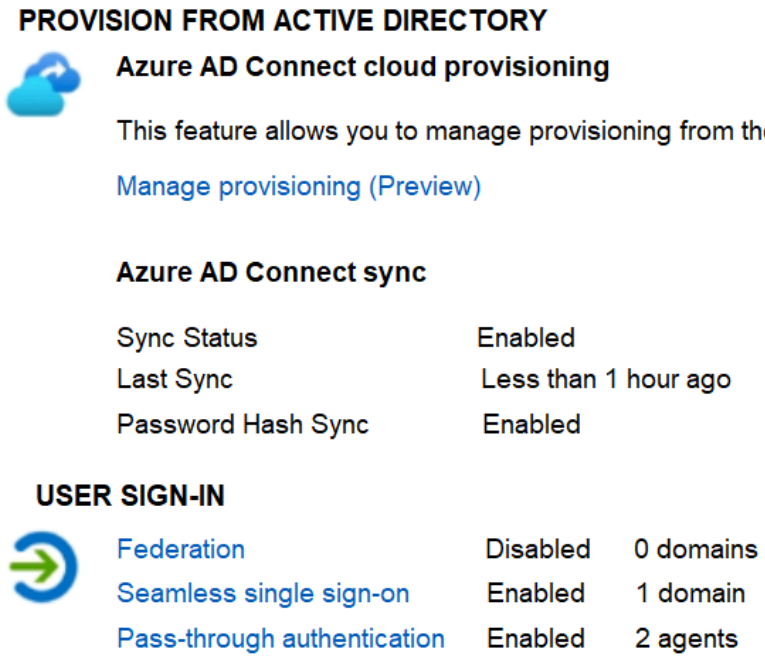
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 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

Suggested 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 (86%) 14%

MartiFC Highly Voted 3 years, 5 months ago

Yes is correct. change UPN

upvoted 7 times

gkp_br Highly Voted 3 years, 7 months ago

Yes for me. User already sync, probably with @contoso.com UPN. So, user can sign in with user2@contoso.com.
upvoted 6 times

TechMinerUK Most Recent 2 years, 6 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 3 times

charat 2 years, 7 months 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 different UPN suffix. Therefore, A is correct.
upvoted 3 times

gaem 2 years, 7 months ago

Selected Answer: B

Correct answer
upvoted 1 times

jjong 3 years, 3 months ago

this qns came out in exam today
upvoted 4 times

jc1993 3 years, 8 months ago

This is correct. Granted you wait for the next AD sync.
upvoted 2 times

forummj 2 years, 7 months ago

You could just push it through with Start-ADSyncSyncCycle -PolicyType Delta Powershell and you don't have to wait.
upvoted 1 times

Josephsmith 3 years, 8 months ago

Not sure this is right. The answer is No
upvoted 3 times

chaoscreater 3 years, 6 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

Nico95 3 years, 4 months ago

Maybe answer C "not sure" is hidden
upvoted 3 times

TimurKazan 3 years, 4 months ago

Agree. He aint want no smoke
upvoted 1 times

venwaik 3 years, 5 months ago

You two should swap names :)
upvoted 4 times

BoxGhost 2 years, 8 months ago

The question hints that contoso.com is already verified since it's been configured as part of AD connect. Therefore changing the UPN to contoso.com will allow the user to sign in and solves the issue.
upvoted 1 times

Question #59 *Topic 2*

HOTSPOT -

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

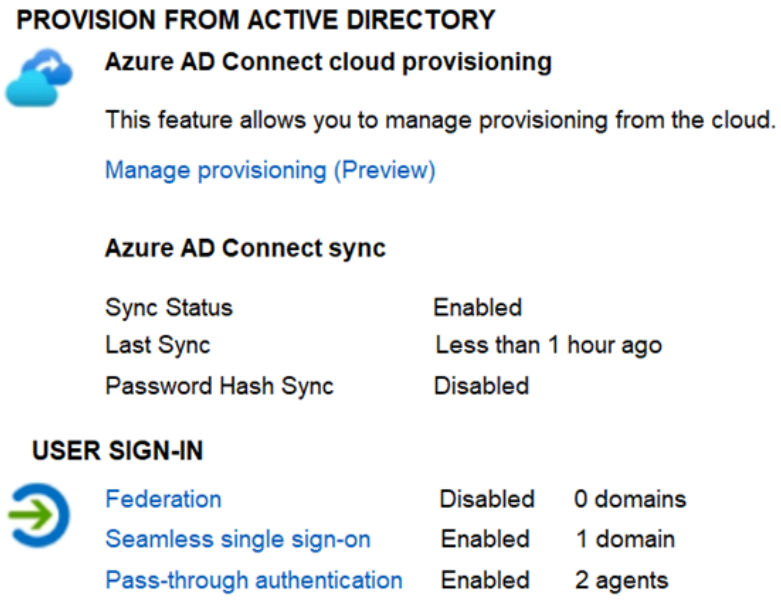
➪ Contoso.com

➪ 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	○	○

Suggested Answer:

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	○	○

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 3 years, 8 months ago
User1 can authenticate by on-prem AD. YNN
upvoted 10 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

One111 1 year, 3 months ago
In Active Directory, each user has two UPN's:

Explicit UPN (eUPN): This is the value of the user object's userPrincipalName attribute. This can be changed to any value, regardless of any alternate UPN suffixes you have configured in the forest.

Implicit UPN (iUPN): This is constructed by concatenating the value of the user object's samAccountName attribute with the value of the domain's FQDN. The FQDN is stored as the value of the dnsRoot attribute of the domain's crossRef object stored at LDAP://CN=DOMAIN_NETBIOS_NAME,CN=Partitions,CN=Configuration,DC=DOMAIN)

If PtA uses AD to find user it will work for 'root domain' and 'any subdomain' within forest added as alternative suffix domain.
upvoted 1 times

mllerena 1 year, 12 months ago
usuario1@contoso.com (Autentícate) -> UPN contoso.com -> SI
usuario2@contoso.com (Autentícate) -> UPN East.contoso.com -> NO
usuario32@contoso.com (Autentícate) -> UPN Fabrikam.com -> NO
upvoted 1 times

Cheekypoo 2 years, 5 months ago
Was in my exam today 05/08/22.
upvoted 1 times

TechMinerUK 2 years, 6 months ago
I believe the answer provided is correct as from the question it appears that contoso.com is setup in AzureAD and Microsoft 365 however 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 suffix 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 3 years, 3 months 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

One111 1 year, 3 months ago
Suffix is used on Azure to recognize domain and determine authentication mode, which is PtA. Lokal domain lookup for user with whatever.contoso.com\user in contoso.com forest willa be successfully completed. Questions is how PtA looks for user ,is IT by upn or samAccountName mapped (alternative suffix configuration have to applied before).

upvoted 1 times

melatocaroca 3 years, 6 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 is for password hash sync, pass-through authentication and federation. UserPrincipalName and sourceAnchor/immutableID come from this 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 3 years, 6 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 to sign-in that way

upvoted 2 times

Gus01 3 years, 8 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 3 years, 7 months ago

It doesn't specify that he must use the same on-prem password.

upvoted 1 times

Jaxon_84 3 years, 7 months ago

Passthrough authentication is on however, so, that allows for authentication.

upvoted 6 times

J0J0 3 years, 6 months ago

but not on Azure AD. Authentication happens in on-premise.

upvoted 1 times

venwaik 3 years, 5 months ago

if pass-through is on, that means that the on-prem pass-through module is installed and is communicating with Azure. Therefore, User1 can succesfully sign in with the on-prem password.
Authentication for User 1 = Yes

upvoted 5 times

Rudelke 2 years, 5 months 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 2 times

Question #60 *Topic 2*

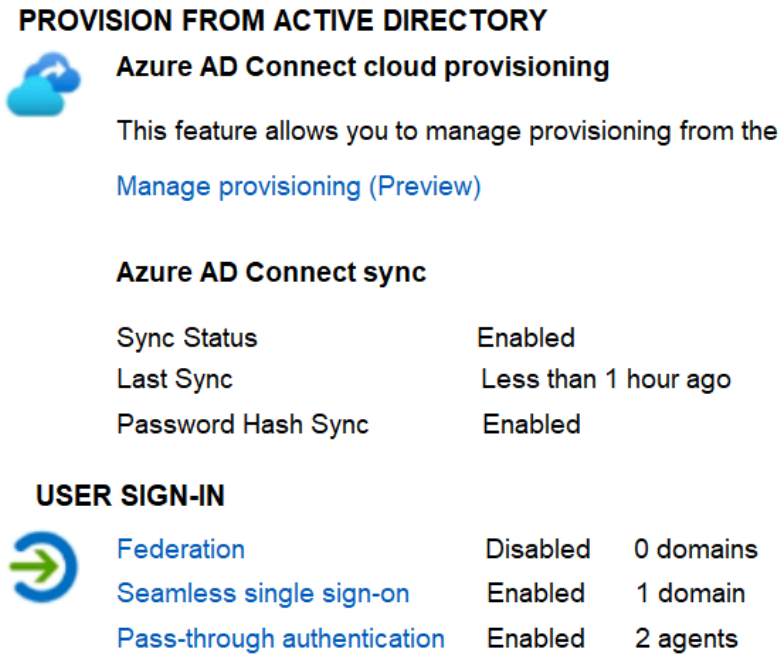
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 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

Suggested 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 3 years, 4 months ago

In today's exqm

upvoted 8 times

TimurKazan 3 years, 4 months ago

we are glad for you

upvoted 10 times

One111 Most Recent 1 year, 3 months ago

Selected Answer: B

Role has nothing to do with suffix recognition.

upvoted 1 times

Moderator 2 years, 6 months ago

Selected Answer: B

Correct answer given.

upvoted 3 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

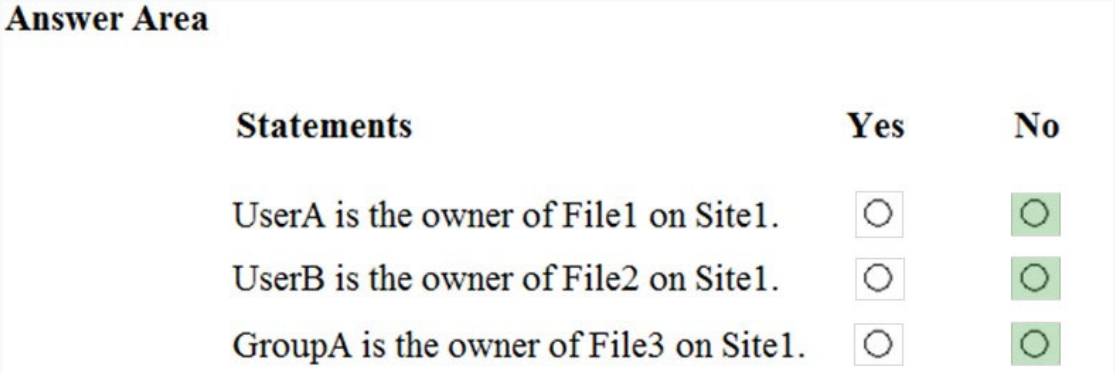
Hot Area:

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.	○	○

Suggested Answer:

Answer Area



dngd Highly Voted 3 years, 8 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 21 times

NHaikes 2 years, 5 months 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 4 times

cscorrupt 2 years, 2 months ago

Correct. It says "For Full control permission, the file will be migrated as Full control in SPO". So noone is owner of anything, thus NNN.
upvoted 3 times

Storm 1 year, 7 months ago

Super - Good to know
upvoted 1 times

lucidgreen 3 years, 8 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 20 times

tf444 3 years ago

Agreed %100.
upvoted 5 times

bLINDmONKEY Highly Voted 3 years, 3 months 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 16 times

Durden871 2 years, 9 months ago

What if there are more than one member with Full Control?

upvoted 2 times

Archie_Bunker 3 years, 2 months 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 3 years, 1 month 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 2 years, 9 months ago

Why not test before answering?

Full Control translates to owner in sharepoint

upvoted 3 times

Paolo2022 2 years, 1 month ago

I don't find any evidence for what you write.

https://learn.microsoft.com/en-us/sharepointmigration/understanding-permissions-when-migrating#what-happens-to-the-permissions-on-a-file-when-it-is-migrated

This source says: "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."

Ownership - and especially the "translation" of Full Control to ownership - that you talk about - isn't mentioned. I don't have a way to test this - as everyone else commenting here. But my approach to the answers provided is that you need good reason to go against them. I don't see that in this case.

upvoted 1 times

ijarosova Most Recent 1 year, 9 months ago

I vote Y|N|N

upvoted 1 times

Monk16 2 years, 2 months ago

Answer YNY

--You have the Full Control permission level --
If you can change the content and the settings on the site you belong to the Owners group which has the Full Control permission level.

https://support.microsoft.com/en-gb/office/understand-groups-and-permissions-on-a-sharepoint-site-258e5f33-1b5a-4766-a503-d86655cf950d

upvoted 1 times

forummj 2 years, 7 months 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 because 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 will still have the same effective permissions.

Hell, I'm probably wrong, but the logic appears sound to me.

upvoted 1 times

joergsi 2 years, 11 months 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 2 years, 11 months 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 2 years, 11 months 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 this question, I setup my tenant to match the conditions of this question to get the actual answer. I also matched my on-prem user accounts and the files to migrate. Same user permissions on the files, same permission preservation on the files in SPMT, and same User Mapping 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. So I am confident with my results.
upvoted 9 times

kanag1 2 years, 11 months 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, 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.
##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 3 years 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 settings in 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 3 years 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 dont actually have permission to access the document library and would have to access using a direct link.

upvoted 1 times

TimurKazan 3 years, 2 months ago

YNY just read the links and articles if you are not familiar with SPMT

upvoted 3 times

melatocaroca 3 years, 6 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 7 times

melatocaroca 3 years, 6 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 3 years, 1 month 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 on 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, enter FALSE. Required.

Close and save as a comma-delimited (*.csv) file.

upvoted 3 times

Question #62 *Topic 2*

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.

Suggested 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 3 years, 7 months ago

Definitely B - Modify TXT Record

upvoted 8 times

spg987 Highly Voted 3 years, 4 months ago

It was in my exam

upvoted 7 times

BigDazza_111 Most Recent 1 year, 7 months ago

Selected Answer: B

True dat

upvoted 1 times

agnesmandriva 1 year, 10 months ago

Selected Answer: B

correct

upvoted 1 times

Cheekypoo 2 years, 5 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Moderator 2 years, 5 months ago

Selected Answer: B

Still a valid question (July 30th 2022).

upvoted 1 times

charat 2 years, 7 months ago

Selected Answer: B

On the MS-100 05/22. Answer is B

upvoted 2 times

dumpmaster 2 years, 11 months ago

Selected Answer: B

Right.

upvoted 2 times

mackypatio 3 years, 7 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 5 times

jc1993 3 years, 8 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

Question #63 *Topic 2*

DRAG DROP -

You have a Microsoft 365 subscription and a DNS domain. The domain is hosted by a third-party DNS service.

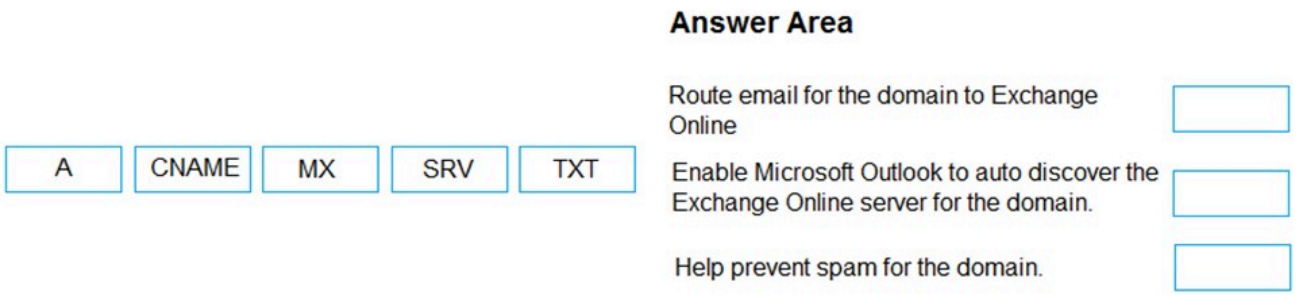
You plan to add the domain to the subscription.

You need to use Microsoft Exchange Online to send and receive emails for the domain.

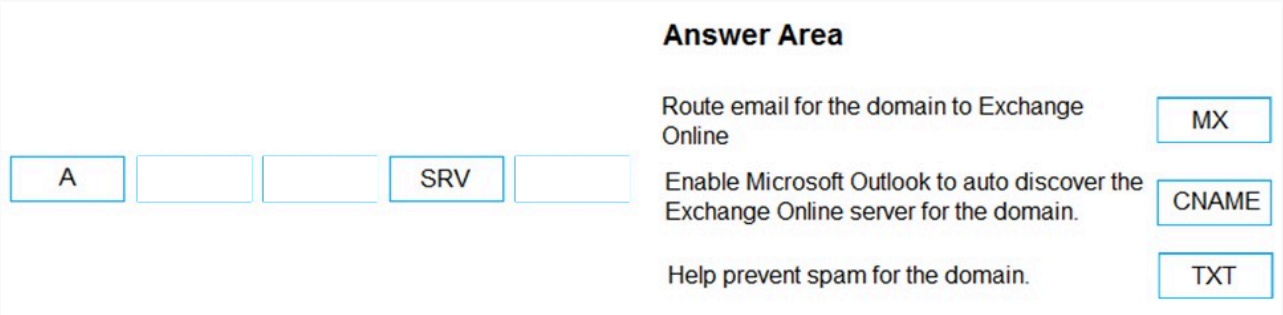
Which type of DNS record should you add to the DNS zone of the domain for each task? To answer, drag the appropriate records to the correct tasks. Each record may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested 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

JCkD4Ni3L 1 year, 8 months ago

Correct !

upvoted 1 times

agnesmandriva 1 year, 10 months ago

correct

upvoted 1 times

Cheekypoo 2 years, 5 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Moderator 2 years, 6 months ago

Correct answers given.

upvoted 3 times

dumpmaster 2 years, 11 months ago

Correct.

upvoted 1 times

spg987 3 years, 4 months 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 3 years, 5 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

Suggested 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 3 years, 9 months ago

Think answer should be:
Sub1: User1 and Group1 Only
Sub2: Contact2 and Group2 Only
?
upvoted 101 times

extrankie 2 years, 11 months ago

i think same
upvoted 1 times

Bobalo 3 years, 5 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 2 years, 11 months 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 8 times

lucidgreen Highly Voted 3 years, 8 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 50 times

vanr2000 Most Recent 1 year, 8 months ago

For Sub1, you need to delete User1 & Group1
For Sub2, you need to delete only Group2, you don't need to delete the contact, this is not a resource in the tenant, is a contact as its name says, so all users within the tenant can see the organization contacts

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-manage#delete-a-custom-domain-name
upvoted 3 times

Meebler 1 year, 9 months ago

Before you can delete the custom domains sub1.contoso.onmicrosoft.com and sub2.contoso.onmicrosoft.com, you must delete or modify the following objects:

For sub1.contoso.onmicrosoft.com:
Group1: Delete the distribution group or change its email address.
user1: Modify the user's username to use a different domain.
For sub2.contoso.onmicrosoft.com:
Group2: Delete the mail-enabled security group or change its email address.
contact2: Delete the contact or change its email address.
upvoted 1 times

JEricThomas610 2 years, 4 months 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 6 times

Rudelke 2 years, 5 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" to confirmation dialog).

Assuming M$ want's you to find what will be afected the answeer provided seems correct.
upvoted 1 times

chriscert 2 years, 6 months 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 2 years, 6 months ago
I Just deleted one and it worked :)
upvoted 2 times

chriscert 2 years, 6 months 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

One111 1 year, 3 months ago
Not all o onmicrosoft.com are its subdomains. You cannadd new root onmicrosoft.com domain which can't be deleted without suport ticket and subdomain which can be deleted if three are no identity using it in their names or UPNs.
upvoted 1 times

Durden871 2 years, 10 months 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 2 years, 10 months 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/modified then mail sent to contact2 will result in delivery failure
upvoted 3 times

Durden871 2 years, 9 months 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 2 years, 9 months ago
Meant to say we don't NEED to delete or modify the contact.
upvoted 1 times

PDR 3 years 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 8 times

davem90 3 years, 1 month 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 22 times

FumerLaMoquette 3 years, 1 month ago
Contacts do not need to be deleted as their external to your tenant. I agree with davem90
upvoted 5 times

TechMinerUK 2 years, 6 months 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 3 years, 2 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 9 times

nicolasganzaroli 3 years, 3 months 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 16 times

Kas1990 2 years, 8 months ago
Correct - you don't need a verified domain to add exchange contacts (as they'll mostly be external domains)
upvoted 1 times

TimurKazan 3 years, 3 months ago
I think nothing is neccesarry to be deleted before deleting domain. Also, I think that would be too easy question - you can actually check 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 3 years, 1 month ago
it says "delete or modify"
upvoted 1 times

lengySK 3 years, 4 months ago
I think the answers are:
Sub1: Group1 only
Sub2: Contact2 and Group2 only
upvoted 1 times

saikelu 3 years, 6 months ago

I believe contact is independent on domain.

upvoted 5 times

birzorirko 3 years, 6 months ago

Group3 is an error.

upvoted 7 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.

Suggested 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
D (100%)

PeterC Highly Voted 3 years, 7 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-where-some-mailboxes-are-in-microsoft-365-or-office-365-and-some-mailboxes-are-on-your-organizations-email-servers
upvoted 8 times

st2023 1 year, 10 months ago
I Agree, pointing mx record to Exchange Online is the way. Here is how Exchange Online Protection (EOP) works
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/eop-about?view=o365-worldwide
upvoted 1 times

Cheekypoo Most Recent 2 years, 5 months ago
Was in my exam today 05/08/22.
upvoted 2 times

TechMinerUK 2 years, 6 months 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 2 years, 11 months ago
Selected Answer: D
Answer is D
upvoted 1 times

blackbic 3 years, 3 months 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 to send the mail to onsite exchange. That's why D was chosen for the answer.
upvoted 3 times

zacmzee 3 years, 3 months 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 3 years, 5 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 recommended 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 through 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 3 years, 7 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 asks 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 3 years, 7 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 4 times

J0J0 3 years, 6 months ago

Agreed. No correct answer here.

upvoted 1 times

saikelu 3 years, 6 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 it is correct.

upvoted 2 times

jc1993 3 years, 8 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

Suggested 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 3 years, 6 months ago
"Consider creating a new role group in Exchange Online that's specifically intended for importing PST files to Office 365. For the minimum level of privileges required to import PST files, assign the Mailbox Import Export and Mail Recipients roles to the new role group, and then add members."
upvoted 11 times

melatocaroca 3 years, 6 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 3 times

sohopros Most Recent 2 years, 2 months ago
The question is still relevant. It was in the exam on 10/21/22
upvoted 3 times

charat 2 years, 7 months ago
Selected Answer: AD
This question was in exam on 05/22/22
upvoted 4 times

JakeH 3 years, 1 month ago
In exam today

upvoted 2 times

Ash473 3 years, 4 months ago

In labs today

upvoted 3 times

Question #67 *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 review the Windows release health in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Suggested 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 3 years, 4 months ago
We have seen this question many times. The answer is B: No. We can see the updates in the Message Center.
upvoted 24 times

LouahZA Highly Voted 3 years, 4 months ago
B, should be Message Center
upvoted 14 times

BigStan82 Most Recent 1 year, 9 months ago
Selected Answer: B
Message Center
upvoted 1 times

TheRem 1 year, 9 months ago
The verb used in the question is "review" not "use" lol
upvoted 1 times

mancio 2 years ago
Selected Answer: B
B, should be Message Center
upvoted 2 times

top587 2 years, 2 months ago
Selected Answer: B
B. Message Center.
upvoted 1 times

EliasMartinelli 2 years, 2 months ago
Selected Answer: B
B. Message Center.
upvoted 1 times

samstorm10 2 years, 2 months ago
Selected Answer: B
B. Message Center.
upvoted 1 times

boxerwalrus 2 years, 2 months ago

Selected Answer: B

Message Center

upvoted 1 times

sliix 2 years, 10 months ago

Selected Answer: B

Pretty direct answer actually.

upvoted 1 times

VictorPCS 2 years, 11 months ago

Selected Answer: B

Should be called Message Center

upvoted 1 times

Blankenp 2 years, 11 months ago

Selected Answer: B

Windows Release Health shows known issues for supported versions, not update features.

upvoted 3 times

LillyLiver 2 years, 11 months ago

Selected Answer: B

Yeah, the Message Center is where you'll see this info. B for sure.

upvoted 1 times

davem90 3 years ago

Selected Answer: B

B, Message Center

upvoted 1 times

PDR 3 years ago

Selected Answer: B

definitely B

upvoted 1 times

opek 3 years ago

Selected Answer: B

Message Center

upvoted 1 times

AlexLiourtas 3 years, 1 month ago

Selected Answer: B

b for obviously reasons

upvoted 3 times

Question #68 *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 Service health option in the Microsoft 365 admin center.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide

Community vote distribution
B (100%)

Davidchercm 2 years, 11 months ago

Selected Answer: B

message centre
upvoted 1 times

xofowi5140 3 years, 2 months ago

Service health
View the health status of all services that are available with your current subscriptions.
upvoted 1 times

Rlcky 3 years, 3 months ago

Correct its B, Message Center
upvoted 3 times

Question #69 *Topic 2*

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

Suggested 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

thehighlandcow 1 year, 9 months ago

Just tested now, please test this yourself and you will see.

Can only apply rule to a user mailbox

Can add recipients to Distribution group, mail enabled security and 365 group

upvoted 1 times

devilcried 1 year, 9 months ago

Just Tested in my Lab
In both cases I can select user1 and group3
upvoted 2 times

Startkabels 2 years, 1 month ago
Tested in production:
M365/distribution/mail-enabled groups cannot be added to the To-field.
As for the first box, the answer is a bit unclear cause it is unspecific.
Apply this rule if: The Recipient > Is this person
or The Recipient > Is a member of this group
or The Message > To box contains this person
or The Message > To box contains a member of this group
etc.
Anyway all the options (indirectly) specify a user.
So indeed both boxes should be User1
upvoted 3 times

theaaronmello 2 years, 1 month ago
It doesn't make for both to be user1. If mail is sent to user1, add user1 as a recipient?
upvoted 1 times

pozzetttt 2 years, 3 months 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 the following "Add these recipients to the To box"
Only user 1 can be added.
upvoted 4 times

[Removed] 2 years, 8 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

[Removed] 2 years, 8 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 2 years, 8 months 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 if…The recipient is”, and, regarding the second question, the same happens, you can add all the resources except the Microsoft 365 Group to “Do the following…Redirect the message to”. So the answer is C&C.
upvoted 2 times

sandi412 2 years, 8 months ago
I tested and in both casses only user mailbox could be used.
upvoted 2 times

briandavisrtr 2 years, 8 months 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 creating 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 2 years, 4 months 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 years, 3 months ago

Tested. Only user mailbox could be used in both.

upvoted 2 times

DRAG DROP -

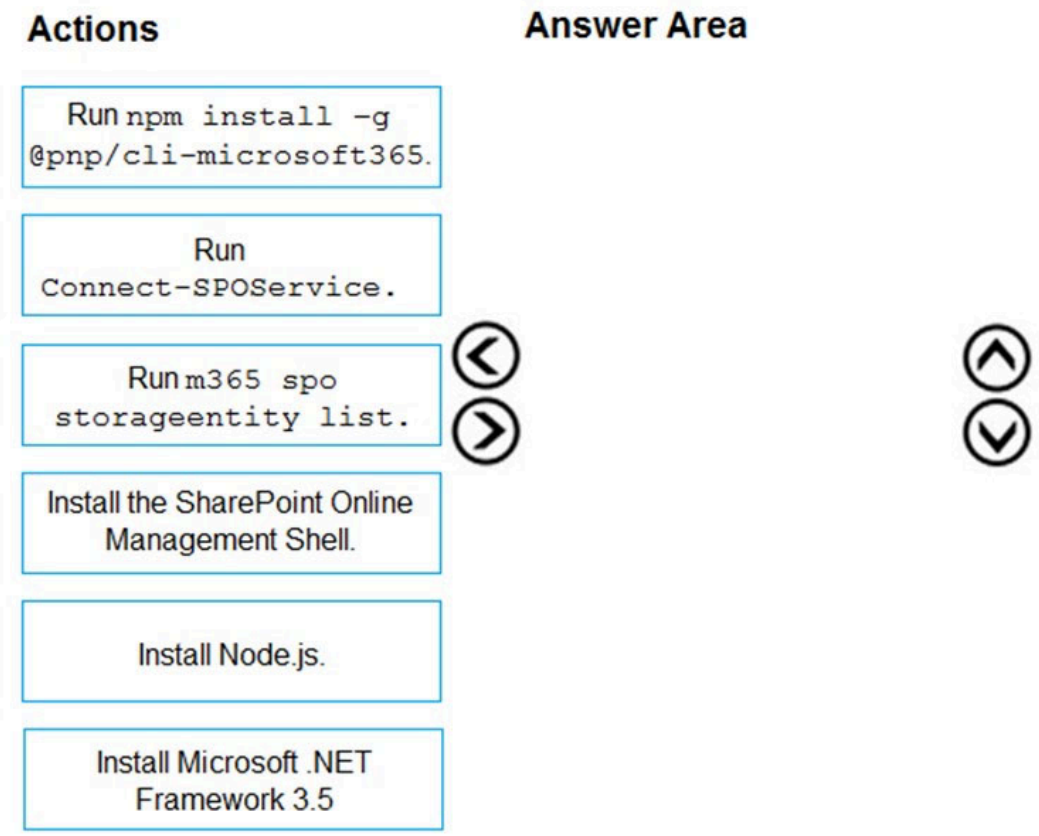
You have a Microsoft 365 E5 tenant.

You have a computer named Computer1 that runs Windows 10.

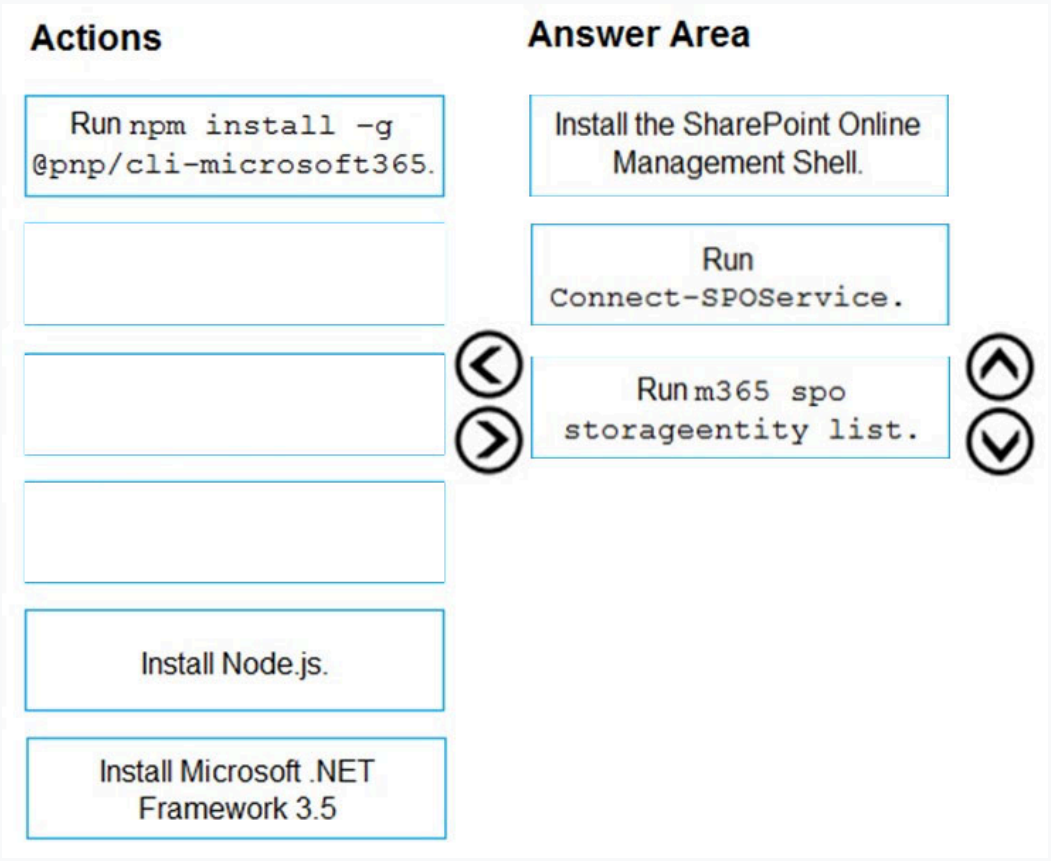
You need to list the properties of a Microsoft SharePoint Online tenant by using the CLI for Microsoft 365 on Computer1.

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:



Suggested 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

MEG Highly Voted 2 years, 8 months 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 9 times

devilcried Most Recent 1 year, 9 months ago

1. Install Node.js
2. Run npm install -q @pnp/cli-microsoft365
3. Run m365 spo storageentity list

connect-sposervice is for Sharepoint- Powershell not CLI

upvoted 2 times

Meebler 1 year, 9 months ago

@MEG is right.. tested it :)

Install Node.js: The CLI for Microsoft 365 is built on Node.js, so you need to install the latest LTS version of Node.js on Computer1. Download it from the official website (https://nodejs.org/) and follow the installation instructions. Node.js is required as a prerequisite for the CLI for Microsoft 365.

Run npm install -g @pnp/cli-microsoft365: After installing Node.js, this command installs the CLI for Microsoft 365, which is a cross-platform command-line interface that allows you to manage settings and perform administrative tasks within your Microsoft 365 tenant.

Run m365 spo storageentity list: After the installation is complete, you can connect to your Microsoft 365 tenant and list the SharePoint Online tenant properties. First, connect to your Microsoft 365 tenant using the m365 login command. Once authenticated, this command will display the properties of the SharePoint Online tenant in your Microsoft 365 tenant.

upvoted 2 times

sufisuffix 1 year, 11 months ago

In exam on 4th Feb 2023.

upvoted 2 times

Miqqo 2 years, 8 months 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 you 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

Balvosko 2 years, 8 months 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 you to use the Node.js"
-> then install CLI itself
-> run the command m365 spo storageentity list

https://pnp.github.io/cli-microsoft365/user-guide/installing-cli/
https://pnp.github.io/cli-microsoft365/cmd/spo/storageentity/storageentity-list/

upvoted 4 times

rrivenn 2 years, 8 months ago

- Install NET Framework
- Install the Powershell Module
- Connect to Sharepoint Online

upvoted 1 times

ARYMBS 2 years, 8 months ago

But to my knowledge W10 comes with .NET 4.X pre-installed?

upvoted 1 times

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.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/sharepoint/hybrid/plan-hybrid-federated-search

Ste_83529 1 year, 2 months ago
Is it me, or should the first thing needed not be to Run the SharePoint Hybrid Configuration Wizard?
https://learn.microsoft.com/en-us/sharepoint/hybrid/configure-cloud-hybrid-searchroadmap
upvoted 1 times

Meebler 1 year, 9 months ago
C. Create a site collection that uses the Enterprise Search Center template.

To include content from the on-premises SharePoint Server environment in Microsoft 365 search results, you need to set up a hybrid federated search. The provided article explains that there are two ways to achieve this: inbound hybrid search and outbound hybrid search.

In your scenario, you want the users to search for content from Microsoft 365 and include content from the on-premises SharePoint Server environment in the search results. This is referred to as inbound hybrid search.

To set up inbound hybrid search, you need to create an Enterprise Search Center in the on-premises SharePoint Server environment using the Enterprise Search Center template. Once this is done, you can configure the inbound hybrid search, which will allow the SharePoint Online search to include the on-premises content in the search results.
upvoted 2 times

diego17 1 year, 7 months ago
Mas ele pergunta o que se deve fazer PRIMEIRO, sendo assim não seria a opção D?
upvoted 1 times

Mercious 2 years, 3 months ago
A has nothing to do with content search on SharePoint
upvoted 1 times

[Removed] 2 years, 8 months 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 Configure hybrid federated search from SharePoint Server to SharePoint in Microsoft 365 - roadmap. You must also do the following:

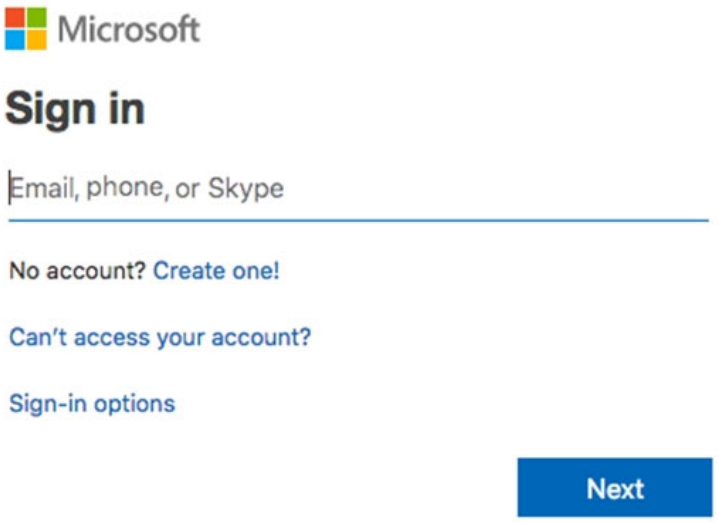
Perform at least one crawl in the SharePoint Server deployment, so that there is content in the SharePoint Server search index. (The SharePoint in Microsoft 365 content must also be crawled, but you don't have to attend to that because SharePoint in Microsoft 365 crawls its content automatically.) For 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 new site collection. For more info, see Create a Search Center site in SharePoint Server.
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@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.

Suggested 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

GotDamnImIn Highly Voted 2 years, 2 months ago

My approach was different.

1. Go to 365 Admin portal
2. Click on the Users blade, search for the user
3. Click on the user, under Roles, click on Manage roles
4. Click on "Show all by category", under "Other" select "Service Support Administrator"

upvoted 6 times

BigDazza_111 Most Recent 1 year, 7 months ago

correct --> azure AD--> roles and admins--> service support admin ...'Users with this role can open support requests with Microsoft for Azure and Office 365 services, and view the service dashboard and message center in the Azure portal and Office 365 admin portal.'

upvoted 1 times

One111 2 years ago

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#service-support-administrator

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#message-center-reader

upvoted 1 times

Balvosko 2 years, 8 months 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

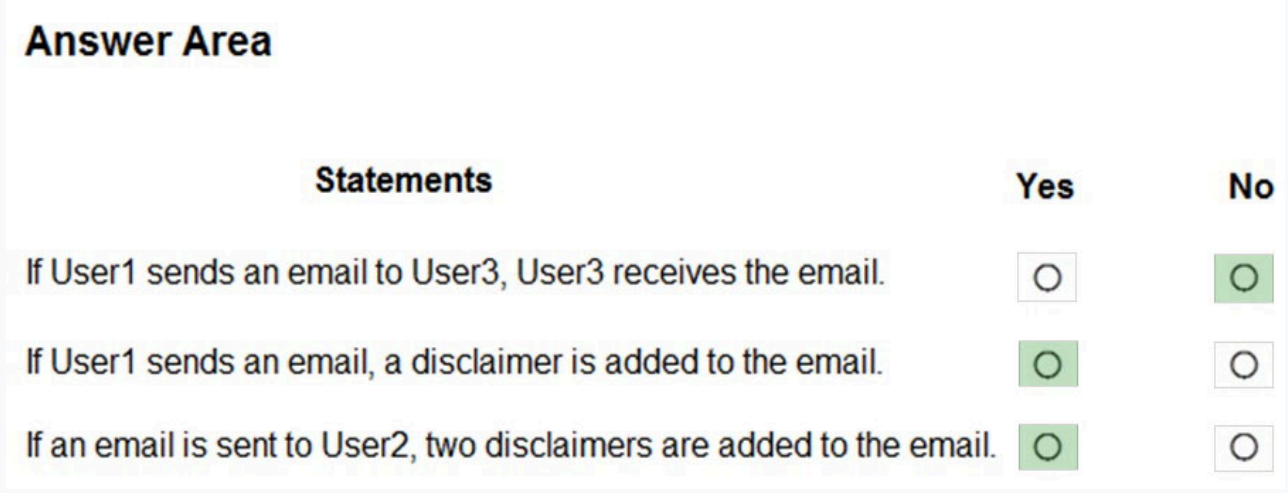
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

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.	○	○

Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

xyz213 Highly Voted 2 years, 3 months 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 26 times

miszczswiata Highly Voted 2 years, 4 months 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 16 times

Sysadmin007 1 year, 9 months ago

Rule 1 redirects the email to user2. This activates rule 2 and now since the recipient is user2, the disclaimer is added. I tested it and got the disclaimer.

upvoted 1 times

HenryVo 2 years, 3 months ago

Confirm. I tested.

upvoted 1 times

proxyma93 Most Recent 1 year, 7 months ago

N Y N

Only one disclaimer because rule 2 has "stop processing more rules", therefore the rule 3 cannot be enforced to add another disclaimer

upvoted 1 times

Everlastday 1 year, 12 months ago

Was on Exam 03.01.2023

Question #74 *Topic 2*

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:

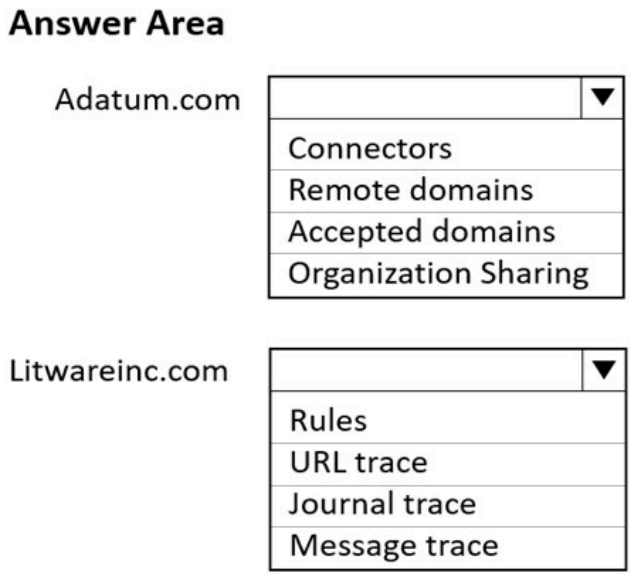
✑ Connections to the email server of adatum.com must use TLS and require that the remote server has a digital certificate.

✑ Email messages sent to litwareinc.com that contain the word `confidential` must be encrypted.

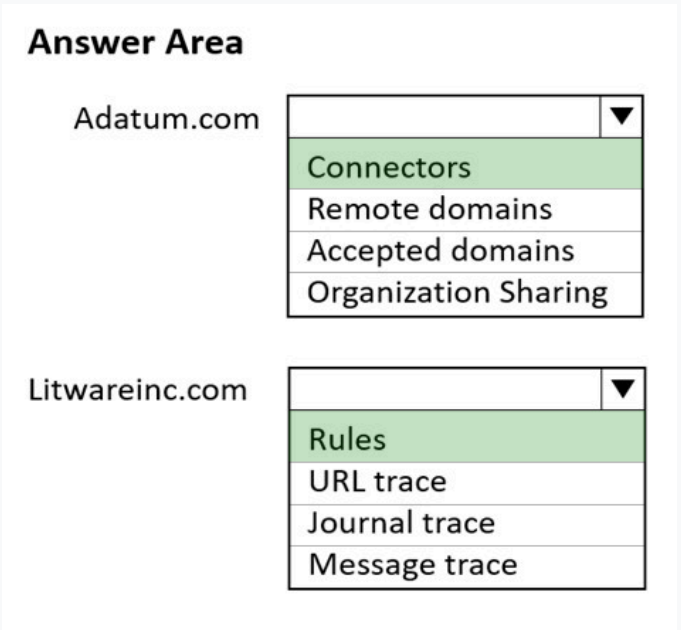
What should you use for each domain? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested 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/

JCkD4Ni3L 1 year, 8 months ago

Meebler is correct !

upvoted 1 times

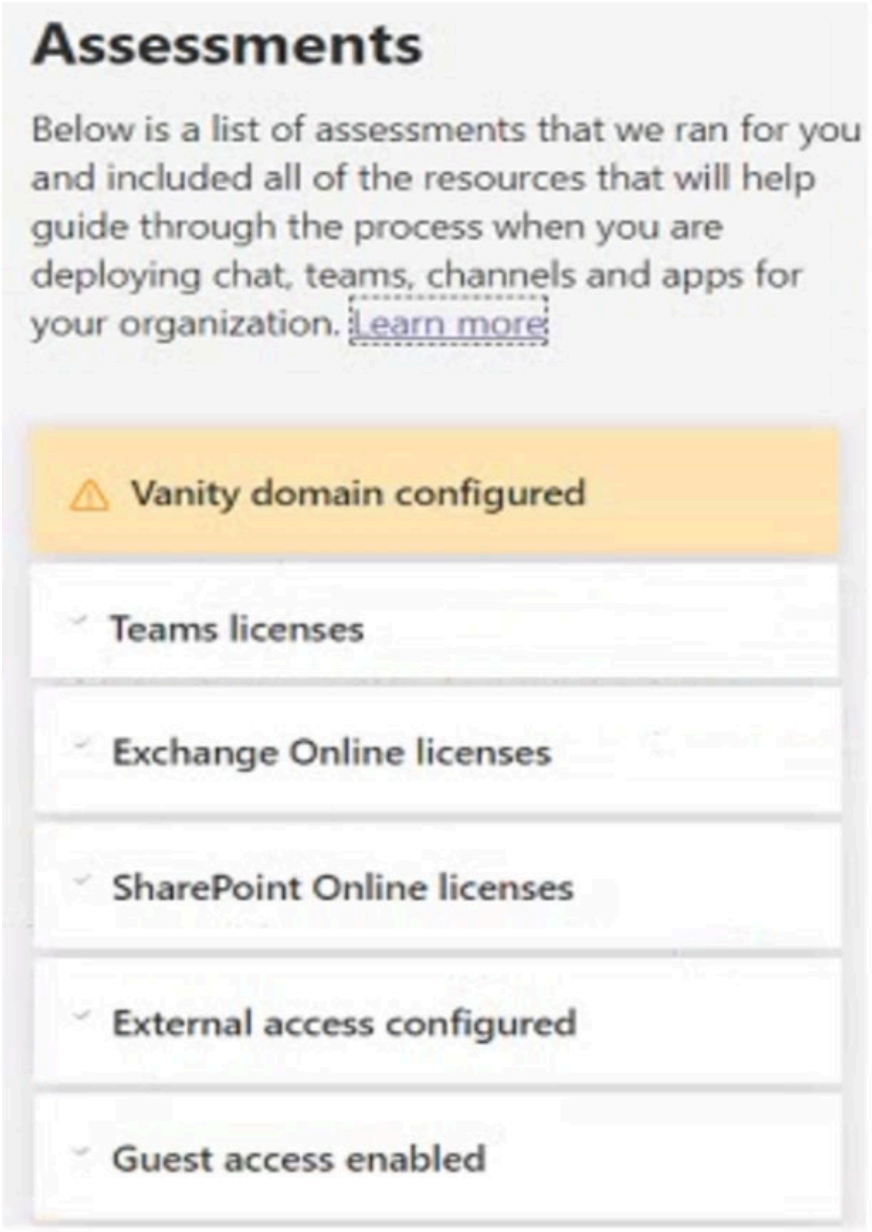
Meebler 1 year, 9 months ago

Adatum.com: Connectors
You need to create a mail flow connector in Exchange Online that enforces TLS and requires a valid digital certificate from the remote server at adatum.com. Connectors help to ensure secure mail flow between partner organizations.

Litwareinc.com: Rules
You need to create a transport rule in Exchange Online that encrypts email messages sent to litwareinc.com if the message contains the word "confidential." Rules can be used to apply specific conditions and actions to email messages, such as encryption in this case.
upvoted 4 times

Question #75 *Topic 2*

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.

Suggested 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

don_bendino 1 year, 12 months ago

Correct answer is A.
"This error is usually caused when an Azure subscription is moved to a new Azure AD directory and the old Azure AD directory that's associated with Azure AD DS is deleted.

This error is unrecoverable. To resolve the alert, delete your existing managed domain and recreate it in your new directory. If you have trouble deleting the managed domain, open an Azure support request for additional troubleshooting assistance."

https://learn.microsoft.com/en-us/azure/active-directory-domain-services/troubleshoot-alerts
upvoted 3 times

Question #76 *Topic 2*

You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You need to deploy the Microsoft Power Platform Center of Excellence (CoE) solution to a Microsoft Dataverse for Teams environment.

What should you do first?

A. From the Teams client add PowerApps.

B. From the Teams client import the CoE solution.

C. Create a new team.

D. Create a canvas app.

Suggested Answer: *D*

Community vote distribution

A (100%)

glitchlessxddd Highly Voted 1 year, 12 months ago

WTF is canvas app

upvoted 14 times

ZauberSRS Highly Voted 1 year, 12 months ago

Guess this question is End-of-Life?

Effective October 2022, we will stop investing in the CoE Starter Kit version for Dataverse for Teams....We recommend that customers transition to installing the CoE starter Kit in a Production environment and setting up pay-as-you-go plans for the usage of apps within the CoE Starter Kit.

https://learn.microsoft.com/en-us/power-platform/guidance/coe/setup

upvoted 5 times

JCkD4Ni3L Most Recent 1 year, 8 months ago

Selected Answer: A

A. From the Teams client add PowerApps.

upvoted 1 times

Meebler 1 year, 9 months ago

A. From the Teams client add PowerApps.

Before you can deploy the Microsoft Power Platform Center of Excellence (CoE) solution to a Microsoft Dataverse for Teams environment, you need to first add Power Apps to your Teams client. This will enable you to access the Power Apps features and import the CoE solution into the Dataverse for Teams environment.

upvoted 3 times

Blagojche 1 year, 9 months ago

B. From the Teams client import the CoE solution.

To deploy the Microsoft Power Platform Center of Excellence (CoE) solution to a Microsoft Dataverse for Teams environment, you should first import the CoE solution into your environment. The CoE solution is a set of pre-built Power Platform components, including Power Apps, Power Automate flows, and Power BI reports, that help organizations govern, manage, and drive adoption of the Power Platform.

upvoted 1 times

DeLoc 1 year, 10 months ago

Probably out of date, as suggested. However, the correct first step would either be create team or import the CoE solution from the team's client to an existing team.

@glitchlessxddd. A canvas app is just a PowerApp that you fully manage, like a blank canvas, unlike model driven apps which are based on your dataverse entities.

upvoted 1 times

Question #77 *Topic 2*

HOTSPOT

-

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

Install [▼]
- The Azure Active Directory (Azure AD) Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server [▼]
- Server1 or Server3 only
- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Suggested Answer:

Install [▼]
- The Azure Active Directory (Azure AD) Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server [▼]
- Server1 or Server3 only
- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

ZauberSRS Highly Voted 1 year, 12 months ago

Right answer should be Server2 only:

Azure AD Connect must be installed on a domain-joined Windows Server 2016 or later - note that Windows Server 2022 is not yet supported. (entry is from 6 January 2023)

The Azure AD Connect server must have a full GUI installed. Installing Azure AD Connect on Windows Server Core isn't supported.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites
upvoted 7 times

ZauberSRS 1 year, 11 months ago
Wish we could edit, the quest was about Azure AD Connect cloud sync not Azure AD Connect
Supplied answer is correct:
An on-premises server for the provisioning agent with Windows 2016 or later... Installing the agent on a domain controller is supported.
https://learn.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites?tabs=public-cloud

Can I install the cloud provisioning agent on Windows Server Core?
No, installing the agent on server core is not supported.
https://learn.microsoft.com/en-us/azure/active-directory/cloud-sync/reference-cloud-sync-faq
upvoted 10 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

NitishKarmakar 1 year, 7 months ago
Windows Server 2022 is now supported as of 5/4/23.
"We recommend the usage of domain joined Windows Server 2022."
so servers 1 and 2 are indeed supported.
upvoted 3 times

Rydaz 1 year, 9 months ago
so write answer is provision agent, you dont need AAD connect, and provision agent can be installed on DC and server 2022, AAD connect can not be installed on server 2022
upvoted 2 times

BigDazza_111 1 year, 7 months ago
Yes it can. We have it installed on Server 2022 on our DC production environ.
upvoted 1 times

Rydaz 1 year, 9 months ago
answer is AD Connect, and install it on either server 1 or 3
upvoted 1 times

devilcried 1 year, 9 months ago
Provided answer is right
An on-premises server for the provisioning agent with Windows 2016 or later. This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.
https://learn.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites?tabs=public-cloud
upvoted 2 times

Meebler 1 year, 9 months ago
You can install the Azure AD Connect provisioning agent on Server2 only

The Azure AD Connect provisioning agent should be installed on a member server, not on a domain controller. In this case, Server2, a Windows Server 2016 member server, is the appropriate choice.
upvoted 1 times

Question #78 *Topic 2*

You have a Microsoft 365 subscription.

You need to be notified to your personal email address when a Microsoft Exchange Online service issue occurs.

What should you do?

A. From the Microsoft 365 admin center, update the technical contact details.

B. From the Microsoft 365 admin center, customize the Service health settings.

C. From the Microsoft Outlook client configure an Inbox rule.

D. From the Exchange admin center, create a contact.

Suggested Answer: *B*

Community vote distribution

B (100%)

Amir1909 11 months ago

B is correct

upvoted 1 times

fessebook 1 year, 8 months ago

Selected Answer: B

B is correct.

Options has slightly changed.
From Microsoft 365 Admin Center go to :
Health / Service Health. Click on Customize and select the Email tab.
Tick "Send me service heath notifications in email", specify email address the tick the issue types and services to include.

upvoted 1 times

Meebler 1 year, 9 months ago

B. From the Microsoft 365 admin center, customize the Service health settings.

By customizing the Service health settings, you can add your personal email address to receive notifications about service issues related to Exchange Online or any other Microsoft 365 services.

upvoted 1 times

matthijsb18 1 year, 11 months ago

Selected Answer: B

To sign up for email notifications of new incidents that affect your tenant and status changes for an active incident, select Preferences > Email, click Send me service heath notifications in email, and then specify:
Up to two email addresses.
Whether you want notifications for incidents or advisories
The services for which you want notification

https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide#how-to-check-service-health

upvoted 2 times

Question #79 *Topic 2*

Your company has a main office and three new branch offices.

The company has a Microsoft 365 subscription.

From the Microsoft 365 admin center, you open Microsoft 365 network connectivity.

You need to configure the prerequisites for enabling Microsoft 365 network connectivity.

What should you do first?

A. Select a SD-WAN solution and the data location.

B. Enable Productivity Score.

C. Update the organization information.

D. Add location data to Microsoft 365.

Suggested Answer: *D*

Community vote distribution

D (100%)

yawb 1 year, 11 months ago

Selected Answer: D

Adding Location data is correct:

https://learn.microsoft.com/en-US/microsoft-365/enterprise/office-365-network-mac-perf-overview?WT.mc_id=365AdminCSH_inproduct&view=o365-worldwide#pre-requisites-for-network-connectivity-assessments-to-appear

upvoted 4 times

Question #80 *Topic 2*

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to access service health alerts from a mobile phone.

What should you use?

A. the Intune app

B. the Microsoft 365 Admin mobile app

C. Intune Company Portal

D. the Microsoft Authenticator app

Suggested Answer: *B*

Amir1909 11 months ago

B is correct

upvoted 1 times

Meebler 1 year, 9 months ago

B. the Microsoft 365 Admin mobile app

The Microsoft 365 Admin mobile app allows you to monitor the service health of your Microsoft 365 environment, including receiving alerts and viewing the status of individual services, directly from your mobile device.

upvoted 1 times

minasamy 1 year, 12 months ago

answer is correct

upvoted 1 times

Question #81 *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 review the Product Feedback in the Microsoft 365 admin center.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Meebler 1 year, 9 months ago

To view a list of recently updated features in your Office 365 tenant, you should check the Message Center.

upvoted 1 times

Question #82 *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 Reports from the Microsoft 365 compliance center.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Meebler 1 year, 9 months ago

To view a list of recently updated features in your Office 365 tenant, you should check the Message Center.

upvoted 1 times

Question #83 *Topic 2*

You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You need to provide Teams administrators with early access to Teams preview features.

What should you configure?

A. Release preferences in the Microsoft 365 admin center

B. Teams upgrade settings in the Microsoft Teams admin center

C. Office installation options in the Microsoft 365 admin center

D. Teams update policies in the Microsoft Teams admin center

Suggested Answer: *B*

Community vote distribution

D (100%)

soosha Highly Voted 1 year, 12 months ago

Selected Answer: D

D

https://learn.microsoft.com/en-us/microsoftteams/public-preview-doc-updates

upvoted 12 times

ago_inline Highly Voted 1 year, 12 months ago

D: Teams Admin Center>Teams>Teams Update Policies: "Update policies are used to manage Teams and Office preview users that will see pre-release or preview features in the Teams app. You can use the Global (Org-wide default) policy and customize it, or create one or more custom policies for your users."

upvoted 10 times

proxyma93 Most Recent 1 year, 7 months ago

Selected Answer: D

It's D, B is for going from Skype to Teams

upvoted 1 times

BigDazza_111 1 year, 8 months ago

Selected Answer: D

Definately

upvoted 2 times

BigStan82 1 year, 9 months ago

Selected Answer: D

Teams Update policies in the Microsoft Teams admin center.

upvoted 1 times

Meebler 1 year, 9 months ago

D,Teams Update policies in the Microsoft Teams admin center.

Here's how to configure the update policy:

1) Sign in to the Microsoft Teams admin center (https://admin.teams.microsoft.com/).
2) In the left navigation pane, click on "Teams" and then click on "Teams Update policies."
3) You can either select "Add" to create a new policy or select an existing policy to open the "Update policy" settings.
4) Name the update policy, add a description, and select the setting for "Show preview features" (e.g., "Enabled" or "Follow Office Preview (default)").
5) Assign the policy to the specific Teams administrators who should have access to the public preview features.

With this configuration, you can enable public preview features for specific users in your organization, allowing them to explore and test upcoming features in Microsoft Teams

upvoted 3 times

minasamy 1 year, 12 months ago

Selected Answer: D

answer should be D

upvoted 7 times

Question #84 *Topic 2*

You have a Microsoft 365 subscription.

You plan to implement a hybrid configuration that has the following requirements:

• Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
• Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned changes implementation.

Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Pass-through authentication

B. Password writeback

C. Enable single sign-on

D. Password Hash Synchronization

E. Directory extension attribute sync

Suggested Answer: *AB*

Community vote distribution

Beanpole Highly Voted 1 year, 11 months ago

C and D

We need to support the use of Azure AD Identity Protection.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#cloud-authentication

upvoted 9 times

glitchlessxddd Highly Voted 1 year, 12 months ago

Why in earth password writeback, I'll go A and C

upvoted 8 times

Amir1909 Most Recent 11 months ago

C and D is correct

upvoted 1 times

Infraestrutura 1 year, 4 months ago

C e D - O Azure AD Identity Protection requer Sincronização de Hash de Senha, independentemente de qual método de entrada escolhido, para fornecer o relatório Usuários com credenciais vazadas. As organizações podem fazer failover para sincronização de Hash de senha se o método de entrada principal falha, e ele foi configurado antes do evento de falha.

upvoted 1 times

obheech 1 year, 5 months ago

C and D

upvoted 1 times

BigDazza_111 1 year, 8 months ago

Selected Answer: CD

So many answers are wrong on this dump, Exam topics is substandard and misleading students.

upvoted 4 times

Rydaz 1 year, 9 months ago

c and d

upvoted 3 times

Meebler 1 year, 9 months ago

A & C (Pass-through authentication and Enable single sign-on):
-Authentication happens in the cloud after a secure password verification exchange with the on-premises authentication agent.
-Requires at least one server for each additional authentication agent.
-Offers single sign-on for domain-joined devices within the company network.
-Supports Azure AD Identity Protection.

D & C (Password Hash Synchronization and Enable single sign-on):
-Authentication happens in the cloud.
-No additional on-premises server requirements beyond Azure AD Connect.
-Offers single sign-on for domain-joined devices within the company network.
-Supports Azure AD Identity Protection.
-Simpler implementation and reduced on-premises infrastructure.

Based on the requirements mentioned in your question, the combination of D & C (Password Hash Synchronization and Enable single sign-on) might be a better choice as it provides a simpler implementation with fewer on-premises infrastructure requirements while still meeting the needs for single sign-on and Azure AD Identity Protection support.
upvoted 3 times

Blagojche 1 year, 9 months ago
To implement a hybrid configuration that meets the specified requirements, you should select the following options in Azure AD Connect:

A. Pass-through authentication: This authentication method enables users to sign in to Microsoft 365 resources using their on-premises passwords, minimizing the number of times they are prompted for credentials.

C. Enable single sign-on: This option ensures that users can access Microsoft 365 resources without having to re-enter their credentials, as long as they are logged in to their on-premises Active Directory domain.

Therefore, options A and C are correc
upvoted 2 times

st2023 1 year, 10 months ago
Selected Answer: CD
C.
D.Azure AD Identity Protection requires Password Hash Sync regardless of which sign-in method you choose, to provide the Users with leaked credentials report. Organizations can fail over to Password Hash Sync if their primary sign-in method fails and it was configured before the failure event.
sauce: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 1 times

KalSiva 1 year, 11 months ago
Selected Answer: CD
C: SSO - Avoids typing Username and Password to every time we access resource
D: Hash - Pre-requisite to use Azure Identity Protection
upvoted 1 times

mrwhite 1 year, 11 months ago
Selected Answer: CD
You need Azure AD password hash synchronization in order for Identity Protection to work. So C and D.
upvoted 3 times

theaaronmello 1 year, 11 months ago
Selected Answer: CD
Need password hash sync for cloud auth
upvoted 2 times

Kees1990 1 year, 11 months ago
C and D
Azude AD IP requires password hash.
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 6 times

soosha 1 year, 12 months ago

Selected Answer: AC

A and C

We need SSO

upvoted 2 times

torestaelens 1 year, 12 months ago

Selected Answer: AC

I'd also go for AC. Password writeback doesn't have anything to do with the authentication itself

upvoted 2 times

Question #85 *Topic 2*

You have a Microsoft 365 subscription.

You plan to use Productivity Score and need to ensure that it can obtain device and software metrics.

What should you do?

A. Enable privileged access.

B. Configure Support integration:

C. Enable Endpoint analytics.

D. Run the Microsoft 365 network connectivity test on each device.

Suggested Answer: *C*

Amir1909 11 months ago

Correct

upvoted 1 times

steveofrobust 1 year, 10 months ago

C is correct answer.

In order to use Microsoft 365 Productivity Score, you need to enable Endpoint analytics. This will allow Microsoft 365 to obtain device and software metrics, which are required for the Productivity Score. Endpoint analytics enables the collection of information about the devices and applications used by users in your organization. This information is used to provide insights into the productivity and effectiveness of your organization, and can help you identify areas for improvement.

upvoted 4 times

Question #86 *Topic 2*

You have a Microsoft 365 subscription.

You create a new Conditional Access policy named CAPolicy1.

You need to be able to review how CAPolicy1 has affected users after 90 days.

What should you do?

A. From the Microsoft 365 admin center, view the Email activity report.

B. Run the Get-AzureADAuditSignInLogs cmdlet.

C. From the Azure Active Directory admin center, review the sign-in logs for each user.

D. Deploy the Conditional Access insights and reporting workbook.

Suggested Answer: *D*

Community vote distribution

D (100%)

ZauberSRS Highly Voted 1 year, 11 months ago

Selected Answer: D

The magic phrase here is 90 days. Sign-In logs are only stored for 30 days so B & C are out.

The Conditional Access insights and reporting workbook enables you to understand the impact of Conditional Access policies in your organization over time...Time range: Select a time range from 4 hours to as far back as 90 days
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

upvoted 6 times

JCkD4Ni3L Most Recent 1 year, 8 months ago

Selected Answer: D

Correct, answer is D.

upvoted 1 times

Question #87 *Topic 2*

DRAG DROP
-

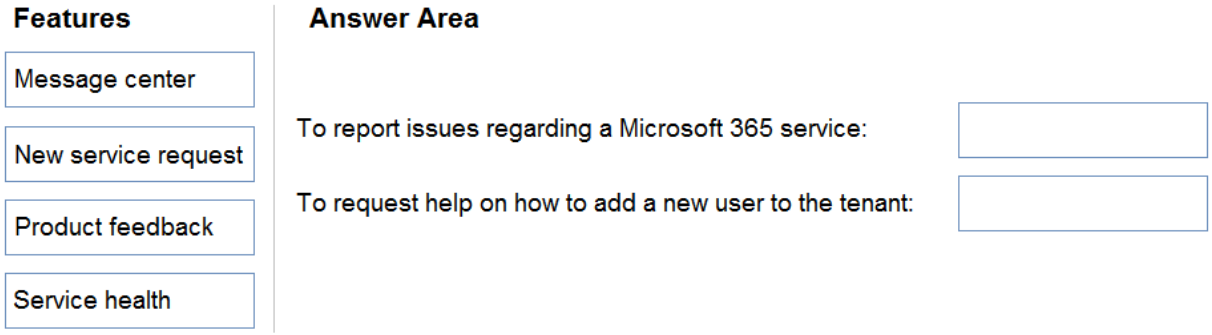
You have a Microsoft 365 subscription.

You need to meet the following requirements:

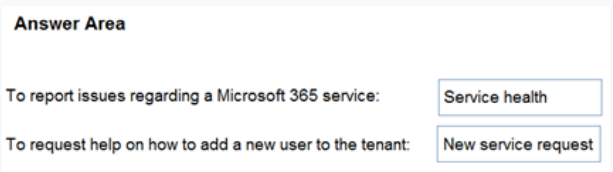
• Report a Microsoft 365 service issue.
• Request help on how to add a new user to an Azure AD tenant.

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature 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.



Suggested Answer:



Amir1909 11 months ago
Correct
- Service Health
- Help & Support
upvoted 1 times

MarkusSan 1 year, 2 months ago
correct answers
upvoted 1 times

bsaksham 1 year, 10 months ago
Its Service Health Guys, product feedback isnt the available option.
upvoted 2 times

KalSiva 1 year, 11 months ago
I think the first box should be - "Product Feedback" but definitely not "Service Health"
upvoted 1 times

nyashac 1 year, 11 months ago
https://support.microsoft.com/en-us/office/how-do-i-give-feedback-on-microsoft-365-2b102d44-b43f-4dd2-9ff4-23cf144cfb11#:~:text=From%20your%20app%2C%20go%20to%20Help%20%3E%20Feedback.&text=From%20your%20app%2C%20go%20to%20File%20%
upvoted 1 times

kerberos99 1 year, 11 months ago

It is Service Health\Report na issue -> check again :)

upvoted 3 times

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.

Suggested 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

Community vote distribution
D (100%)

[Removed] Highly Voted 4 years, 5 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 configure user onboarding controls by using the Set-
AadrmOnboardingControlPolicy
References:
https://docs.microsoft.com/en-us/azure/information-protection/activate-service
upvoted 17 times

AlexanderSaad Highly Voted 4 years, 9 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 9 times

vanr2000 Most Recent 1 year, 8 months ago
Selected Answer: D
The command was deprecated, now you use Set-AipServiceOnboardingControlPolicy.

If you don't want all users to be able to protect documents and emails immediately by using Azure Information Protection, you can configure user onboarding controls by using the Set-AipServiceOnboardingControlPolicy PowerShell command. You can run this command before or after you activate the Azure Rights Management service.

Reference link
https://learn.microsoft.com/en-us/azure/information-protection/activate-service
upvoted 2 times

charat 2 years, 7 months ago
Updated module is Set-AipServiceOnboardingControlPolicy
:https://docs.microsoft.com/en-us/powershell/module/aipservice/set-aipserviceonboardingcontrolpolicy?view=azureipps

upvoted 3 times

emilianogalati 3 years, 3 months 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 3 years, 3 months 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 3 years, 5 months ago

New answer would be: Set-AipServiceOnboardingControlPolicy as the AADRM module is deprecated. Answer is correct in though.

upvoted 8 times

airairo 3 years, 7 months ago

This is in ms 101

upvoted 5 times

bog23 3 years, 9 months ago

D. should be Set-AipServiceOnboardingControlPolicy.
The AADRM cmd is deprecated from July 2020

upvoted 4 times

Bempa 3 years, 11 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 4 years ago

D for sure!

upvoted 3 times

sam76 4 years, 6 months ago

I guess the answer should be B. Sice the Question relates to Azure Information Protection.

upvoted 2 times

kmjunk 4 years, 6 months ago

I thought that as well.

upvoted 1 times

DiscGolfer 4 years, 5 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 4 years, 10 months ago

I agree WoneAix

upvoted 1 times

WoneSix 4 years, 10 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 4 years, 11 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 4 years, 11 months ago
Set-AipServiceOnboardingControlPolicy is replacing Set-AadrmOnboardingControlPolicy . The latter will now be just an alias and still work but new exams may have the new one as the answer.
upvoted 11 times

SMHH 4 years, 10 months ago
Yup
https://docs.microsoft.com/en-us/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps#description
upvoted 1 times

h3nk13 4 years, 4 months ago
This cmdlet from the AADRM module is now deprecated.
upvoted 3 times

Question #2 *Topic 3*

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

Suggested 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

Community vote distribution
D (100%)

Tryggr Highly Voted 3 years, 6 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 21 times

Agbantu Highly Voted 3 years, 6 months ago
Definitely D, Audit log search from the SCC (now compliance.microsoft.com)
upvoted 11 times

BigDazza_111 Most Recent 1 year, 7 months ago
Selected Answer: D
D 4 sure. Azure AD audit logs do not let you search SP online activities
upvoted 1 times

BigDazza_111 1 year, 8 months ago
Selected Answer: D
Audit logs in Azure display device and user athentication data. Not Activity logs.
upvoted 1 times

JCkD4Ni3L 1 year, 8 months ago
Selected Answer: D
Answer is D.
upvoted 1 times

bsaksham 1 year, 11 months ago
Selected Answer: D
No brainer
upvoted 1 times

ARZIMMADAR 1 year, 11 months ago

Absolute Joke. D is the correct answer

upvoted 1 times

Contactfornitish 2 years, 5 months ago

Selected Answer: D

A, are you joking? Deletion of files isn't privileged that way

upvoted 2 times

Contactfornitish 2 years, 5 months ago

Selected Answer: D

Been doing since a while

upvoted 3 times

Stiobhan 2 years, 7 months ago

1000% answer is D. Just ran exact audit on my tenant and all choices are there ☺

upvoted 3 times

jru24 2 years, 8 months ago

yes, I tested it. D is correct

upvoted 1 times

Wojer 3 years ago

just test it and its D

upvoted 2 times

PDR 3 years ago

also D

upvoted 1 times

tcmaggio 3 years ago

Selected Answer: D

D for me.

upvoted 3 times

kaveri123 3 years 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 5 times

tcmaggio 3 years, 1 month ago

Selected Answer: D

I also vote D.

upvoted 5 times

Mavula 3 years, 1 month ago

So why don't they update this answer to be D?

upvoted 2 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

Suggested 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

Community vote distribution
B (100%)

[Removed] Highly Voted 4 years, 5 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 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-andcompliance-permissions
upvoted 16 times

Jokke71 Highly Voted 4 years, 10 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

Startkabels Most Recent 2 years ago
Selected Answer: B
eDiscovery Management it is
upvoted 2 times

gxsh 3 years, 3 months ago
Correct!
upvoted 2 times

Ash473 3 years, 4 months ago
In today's exam
upvoted 3 times

Jake1 4 years, 1 month ago
Answer is correct. eDiscovery Manager & Administrator, as well as Compliance Administrator and Organization Management role allows you to create query-based holds.https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide#rbac-roles-related-to-ediscovery
upvoted 4 times

Question #4 *Topic 3*

HOTSPOT -

You have a new Microsoft 365 subscription.

A user named User1 has a mailbox in Microsoft Exchange Online.

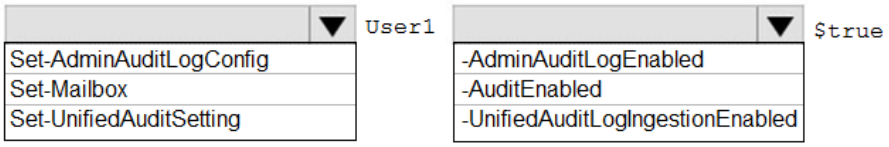
You need to log any changes to the mailbox folder permissions of User1.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

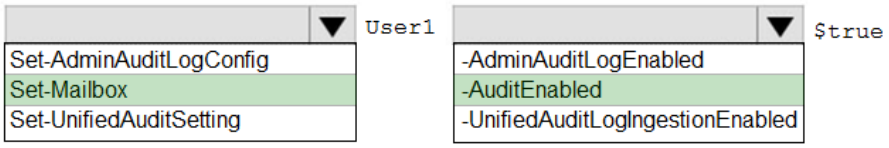
Hot Area:

Answer Area



Suggested Answer:

Answer Area



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 3 years, 6 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 13 times

Moderator Most Recent 2 years, 6 months ago

Correct, pretty straight forward.

upvoted 1 times

Question #5 *Topic 3*

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)

Suggested Answer: *E*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

Community vote distribution
E (100%)

Amir1909 11 months ago
Correct
upvoted 1 times

proxyma93 1 year, 7 months ago
Selected Answer: E
It's always PIM if you hear talking about time constraint
upvoted 1 times

JCkD4Ni3L 1 year, 8 months ago
Selected Answer: E
PIM is the correct answer (E).
upvoted 1 times

Startkabels 2 years ago
Selected Answer: E
Nobrainer E
upvoted 4 times

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.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-azure-ad-tenants

Community vote distribution
A (100%)

[Removed] Highly Voted 4 years, 5 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 27 times

STFN2019 Highly Voted 4 years, 5 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, you 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 9 times

Meebler Most Recent 1 year, 9 months ago
A. Deploy two servers that run Azure AD Connect, and then filter the users for each tenant by using attribute-based filtering.

This is the recommended solution because Azure AD Connect does not natively support synchronizing to multiple Azure AD tenants from a single Active Directory domain. To achieve the desired synchronization, you will need to deploy two separate Azure AD Connect servers. Each server will be responsible for synchronizing a subset of the users to one of the Azure AD tenants. You can use attribute-based filtering to specify which users will be synchronized to each tenant.
upvoted 1 times

Startkabels 2 years ago
Selected Answer: A
2 servers
upvoted 2 times

Tibo49100 2 years, 8 months 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 3 times

spg987 3 years, 4 months ago

In exam today

upvoted 2 times

Prates_BR 3 years, 8 months ago

Correct. A for sure!

upvoted 2 times

FableFa 4 years, 6 months ago

One AD Connect per destination tenant (excepted Staging server) - Answer A correct

upvoted 5 times

kazaki 4 years, 6 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 4 years, 6 months ago

But the question says that there are 2 tenants.

upvoted 25 times

lucidgreen 3 years, 9 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 has a mutually exclusive set of objects to process.

upvoted 5 times

Question #7 *Topic 3*

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.

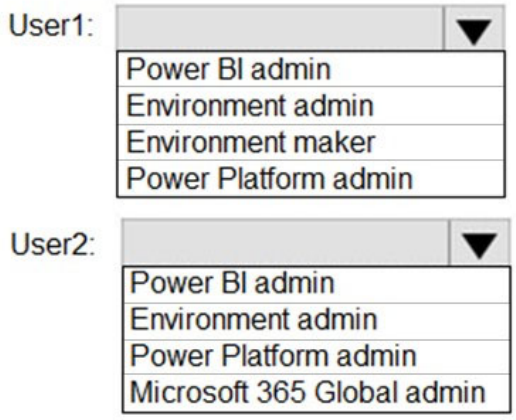
The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, select the appropriate options in the answer area.

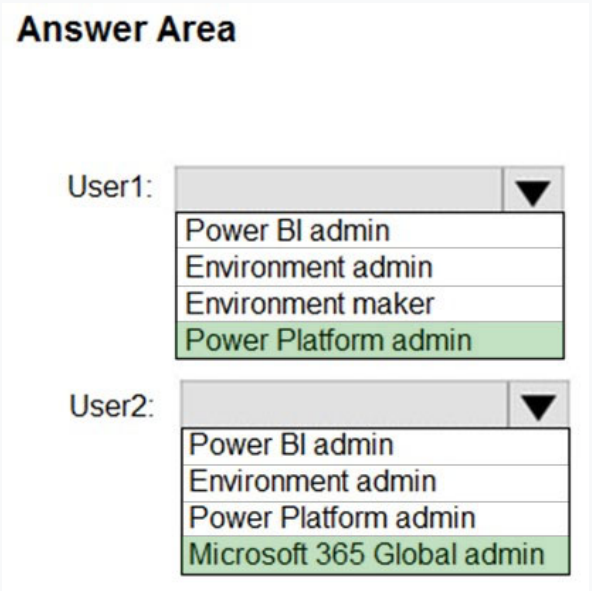
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Suggested Answer:



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

reastman66 Highly Voted 2 years, 1 month ago

I am think

1st one Environment Admin

2nd Microsoft Global Admin

upvoted 9 times

cscorrupt Highly Voted 2 years, 2 months ago

Unless they mean access to everything and all everyones made/does, an environment maker should be enough for full access.

ref: https://learn.microsoft.com/en-us/power-platform/admin/environments-overview
upvoted 6 times

BigDazza_111 Most Recent 1 year, 7 months ago
environment admin and 365 global admin
upvoted 1 times

vanr2000 1 year, 8 months ago
User1 - Environment Admin
https://learn.microsoft.com/en-us/power-platform/admin/environments-overview

User2 Global or Billing admin role in Microsoft 365
https://learn.microsoft.com/en-us/power-bi/enterprise/service-admin-purchasing-power-bi-pro
upvoted 2 times

steveofrobust 1 year, 9 months ago
I think:
- User1: Power Platform Admin
- User2: Power BI admin (has least privilege vs global admin and still can acquire and assign the Power BI license)
upvoted 2 times

DaDaDave 1 year, 5 months ago
Incorrect
https://learn.microsoft.com/en-us/power-platform/admin/use-service-admin-role-manage-tenant#service-administrator-permission-matrix
upvoted 1 times

One111 2 years ago
For environments with no Dataverse database, security roles can be assigned to individual users or groups from Azure AD. A user who has the Environment Admin role in the environment can take these steps.

If the environment has a Dataverse database, a user must be assigned the System Administrator role instead of the Environment Admin role for full admin privileges.

Environment Maker has no security roles permissions on db.
Environment Admn has security roles permissions on db.

https://learn.microsoft.com/en-us/power-platform/admin/database-security

Global admins and Power Platform admins can create environments and assign security groups and users.

https://learn.microsoft.com/en-us/power-platform/admin/create-environment

IMHO right answers are: 1. Environment Admin and 2. Global admin.
upvoted 4 times

Question #8 *Topic 3*

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

Suggested 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

Community vote distribution
A (71%) C (29%)

scottims Highly Voted 4 years, 2 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. When admins add apps to the private store, all employees in the organization can view and download the apps."
upvoted 29 times

Startkabels 2 years ago
People it is C and the above explanation is nonsense.
Yes when admin add apps all users can aquire but that's not the same as purchasing from Store for business.
Just read the rederred article: https://learn.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business#allow-users-to-shop
Viewing and downloading apps from the Store is something completely different as signing into Store for business and purchasing apps.
upvoted 7 times

DaDaDave 1 year, 5 months ago
Question is asking who can INSTALL that is everyone

As to who can PURCHASE that would be C, Purchasers and Basic Purchasers
upvoted 1 times

[Removed] Highly Voted 4 years, 5 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 21 times

PrinceVarghese 4 years, 3 months 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 the answer should be "C". Lets hope this is ON and hence the Purchasers and Basic Purchasers can purchase products and services from Microsoft Store.

upvoted 8 times

PrinceVarghese 4 years, 2 months ago

In my questionnaire it was "purchase". Looks "install" is a foolishness..

upvoted 5 times

maggie_priscilla Most Recent 1 year, 4 months ago

the question is identification of which user can install, and not just shop. The link https://learn.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business#allow-users-to-shop does not explain this aspect.

upvoted 1 times

thehighlandcow 1 year, 9 months ago

Selected Answer: C

As other people have suggested, answer is C.

https://learn.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business#allow-users-to-shop

upvoted 3 times

sehlohomoletsane 1 year, 9 months ago

Selected Answer: A

All users can install (there is a similar question in MS-101 it is QUESTION 32 Topic3)

upvoted 2 times

st2023 1 year, 10 months ago

Selected Answer: A

You can make an app available in your private store when you acquire the app, or you can do it later from your inventory. Once the app is in your private store, employees can claim and install the app.

we should focus on the "install" part.

https://learn.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

upvoted 2 times

DeLoc 1 year, 10 months ago

Selected Answer: C

In the Microsoft Store for Business, both the Purchaser and Basic Purchaser roles can install apps from the private store, but only the Purchaser role can also manage and purchase apps. If the Make everyone a Basic Purchaser option is set to Off, then users need to be explicitly added to the Purchaser or Basic Purchaser role to install apps from the private store.

upvoted 2 times

Startkabels 2 years ago

Selected Answer: C

C for Sure

upvoted 1 times

Benatha 2 years, 5 months ago

I will go for C.

Underline Install "from Microsoft" for business private store.

English is playing us here...

upvoted 1 times

Jkayx94 2 years, 12 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 by 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 3 years 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 me tomorrow, I will take my chances with A...
upvoted 6 times

us3r 3 years 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 6 times

davem90 3 years, 1 month 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 5 times

FreddyLao 3 years 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 your employees. They can browse the private store and install apps when needed.
upvoted 1 times

TimurKazan 3 years, 2 months ago

with these settings only Purchaser role assigned users can buy from Microsoft Store for Business
upvoted 1 times

xofowi5140 3 years, 2 months ago

Its is B
Source: https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business
upvoted 1 times

allesglar 3 years, 2 months ago

I believe that the wording "install" means purchase and therefore the answer is correct. View and download does not mean neither install nor purchase ;)
Answer is C
upvoted 1 times

PDR 3 years 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 set as available to users, group or everyone.

upvoted 2 times

lengySK 3 years, 4 months ago

if Private store...all users

upvoted 1 times

Question #9 *Topic 3*

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

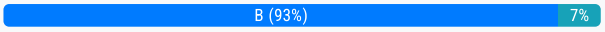
B. Records Management

C. Compliance Administrator

D. eDiscovery Manager

Suggested 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

Community vote distribution



examxe Highly Voted 5 years 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 answer
upvoted 36 times

[Removed] Highly Voted 4 years, 5 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 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
upvoted 18 times

donathon 4 years, 3 months 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 3 years, 5 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 2 times

DeLoc Most Recent 1 year, 10 months ago
Selected Answer: B
The "Records Management" role allows users to create, configure, and manage retention labels and policies.
upvoted 3 times

Startkabels 2 years ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#role-groups-in-the-defender-and-compliance-portals

Members can configure all aspects of records management, including retention labels and disposition reviews.

upvoted 2 times

Partylad 2 years, 2 months ago

States Which Role Group, there is no Records Management Role group, can create a new Role group and just add this Role but that's not what is asked so the given answer appears correct to me

upvoted 1 times

Partylad 2 years, 2 months ago

ignore this just found the role group for records management

upvoted 3 times

JhonnyBe 2 years, 2 months ago

Selected Answer: C

Correct answer

upvoted 1 times

mmraouf 2 years, 3 months 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 years, 3 months 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 2 times

ovd 2 years, 3 months 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 2 years, 4 months ago

least privilege is Records Management, so the answer is B.

upvoted 2 times

Sweethaven 2 years, 5 months 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 years, 5 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 2 times

RazielLycas 2 years, 10 months 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 2 years, 11 months ago

Records Management role is good enough to publish retention labels

upvoted 1 times

VictorPCS 2 years, 11 months ago

Selected Answer: B

Least privilege so should be B

upvoted 2 times

davem90 3 years, 1 month 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 3 years, 3 months ago

o grant permissions for this limited administration, we recommend that you add users to the Compliance Administrator admin role group.

Alternatively to using this default role, you can create a new role group and add the Retention Management role to this group. For a read-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 3 years, 3 months ago

The solution must use the principle of least privilege, B is the answer.

upvoted 3 times

Question #10 *Topic 3*

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.

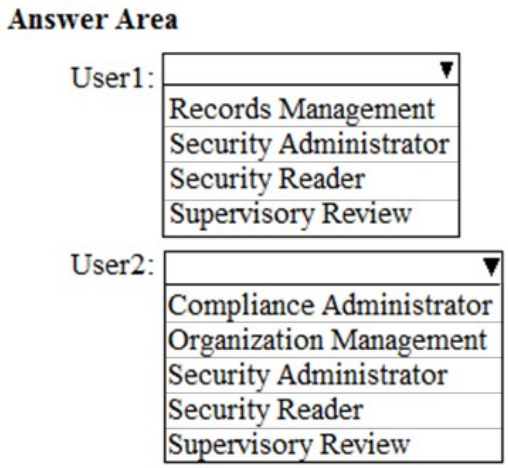
Name	Task
User1	Download all Security & Compliance reports.
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.

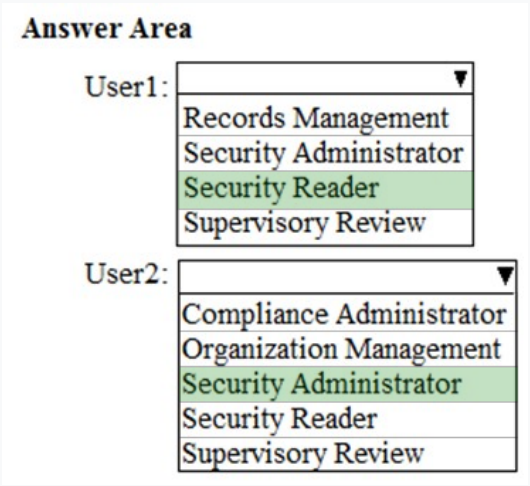
To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested 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 3 years, 11 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 security 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 40 times

test123123 Highly Voted 4 years, 11 months ago

Both are Security Administrator.
upvoted 15 times

minajahan 4 years, 10 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 3 years, 6 months ago
With my best respects your position about need to be revieved
upvoted 5 times

machinegf 2 years, 9 months ago
right, Global admin can also do that LOL.
upvoted 2 times

davem90 Most Recent 3 years, 1 month ago
Answer is correct! Security Reader & Security Administrator
upvoted 3 times

Rlcky 3 years, 3 months 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 3 years, 4 months ago
Both are Security Administrator.
upvoted 1 times

TimurKazan 3 years, 4 months ago
Following the principle of least privilege I would go with records management and security administrator.
upvoted 1 times

TimurKazan 3 years, 1 month ago
perhaps, security READER has less rights than records MANAGEMENT...
upvoted 5 times

Davidchercm 3 years, 4 months ago
security reader can download report :https://docs.microsoft.com/en-us/microsoft-365/compliance/download-existing-reports?view=o365-worldwide#:~:text=In%20general%2C%20global%20administrators%2C%20security,to%20Reports%20%3E%20Reports%20for%20download.
upvoted 3 times

Kepurikee 3 years, 5 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 4 times

melatocaroca 3 years, 6 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 3 years, 7 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 3 years, 11 months ago

i think it's an MS-101 exam question

upvoted 4 times

Takloy 3 years, 11 months ago

true, can't recallthis in the exam which i failed.lol

upvoted 2 times

mkoprivnj 4 years ago

3 & 3 for sure. Security Reader & Security Administrator!

upvoted 5 times

Prianishnikov 4 years ago

what is the correct answer?

upvoted 3 times

scottims 4 years, 2 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 4 years, 2 months ago

for user1, can it be record management ? (for Record Management :Members can manage and dispose record content.)

upvoted 1 times

[Removed] 4 years, 5 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 4 years, 5 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 4 years, 1 month ago

I just assigned the security reader role to a test user and successfully 'exported' a report.

upvoted 2 times

kev001 4 years, 1 month ago

Download existing reports
Important

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.

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.

Suggested 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

Community vote distribution
D (100%)

[Removed] Highly Voted 4 years, 5 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 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-linkspolicies#
policies-that-apply
upvoted 17 times

melatocaroca 3 years, 6 months ago
research department users so do not modify default, create a new one
upvoted 2 times

mkoprivnj Highly Voted 4 years ago
D for sure!
upvoted 5 times

trexar Most Recent 2 years, 9 months ago
Selected Answer: D
The complete path is https://security.microsoft.com/ -->
policies -->Policies & rules
Threat policies
Safe links
upvoted 3 times

Mike3033 3 years, 5 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

Jake1 4 years, 1 month 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=o365-worldwide

upvoted 3 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.	○	○

Suggested 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 5 years 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 indicates), then what data can you actually view with that permission?

upvoted 18 times

jabbrwcky 4 years, 12 months ago

My thoughts exactly.

upvoted 2 times

itmp 4 years, 7 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 19 times

[Removed] Highly Voted 4 years, 5 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 groups 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 15 times

donathon 4 years, 3 months ago

Agree too

upvoted 3 times

donb21 Most Recent 2 years, 4 months ago

Answer is Y Y Y

upvoted 1 times

melatocaroca 3 years, 6 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 3 years, 10 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 2 times

RNG60FR 3 years, 11 months ago

MS-101 Exam Question ?

upvoted 7 times

imEmi 3 years, 10 months ago

It is.

upvoted 3 times

Rstilekar 3 years, 11 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 4 years ago

Y, Y, Y for sure! ctfalci

upvoted 4 times

Carlos1787 4 years, 2 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 3 years, 10 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 4 years, 5 months ago

y n y no yes?

upvoted 1 times

Raj2020 4 years, 6 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 4 years, 6 months ago

Thanks for confirming, i went YNY

upvoted 3 times

fgdsgfdsa 4 years, 4 months 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-permissions

upvoted 1 times

asdkjhbfc 4 years, 7 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 4 years, 7 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 4 years, 9 months ago

How is the a MS-100 question, surely it must be MS-101?

upvoted 14 times

AlexanderSaad 4 years, 9 months ago

Yes
Yes
Yes

upvoted 3 times

Goofer 4 years, 10 months ago

Y - Y - Y

upvoted 7 times

Zaada 4 years, 10 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 4 years, 8 months ago

exactly!

upvoted 2 times

ExamStudy101 3 years, 5 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

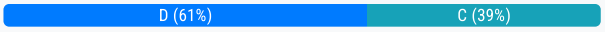
B. Security & Compliance data loss prevention (DLP) policies

C. Microsoft Azure Active Directory (Azure AD) conditional access policies

D. Microsoft Azure Active Directory (Azure AD) Identity Protection policies

Suggested 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

Community vote distribution



d3an Highly Voted 4 years, 11 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 30 times

Razuli 1 year, 10 months ago
Every time I get this error at work it is conditional access though. Confusing
upvoted 1 times

Logico 4 years, 2 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 10 times

DJHASH786 Highly Voted 5 years 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 30 times

Man1ak 3 years, 8 months ago
However in this case this error is clearly an MCAS error. Therefore it's D.
upvoted 1 times

STFN2019 4 years, 5 months ago
Yes I'd stick with conditional access as well
upvoted 3 times

Paolo2022 2 years, 1 month ago

That is 100% correct, Identity Protection policies are deprecated by now and admins are encouraged to implement the settings needed via Conditional Access.
See: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#identity-protection-policies
upvoted 3 times

melatocaroca 3 years, 6 months ago
C is the right answer

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access
upvoted 3 times

marco_aimi Most Recent 1 year, 4 months ago
no doubt guys, base requirement: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies:
*Block access
*Allow access
*Require multifactor authentication
upvoted 1 times

JCkD4Ni3L 1 year, 8 months ago
Selected Answer: C
Conditional Access is the correct answer, C.
upvoted 1 times

DeLoc 1 year, 10 months ago
Selected Answer: C
Both can be argued as valid. The answer "C. Microsoft Azure Active Directory (Azure AD) conditional access policies" is better than "D. Microsoft Azure Active Directory (Azure AD) Identity Protection policies" because it specifically mentions "something unusual about this sign-in" which suggests that the issue is related to sign-in activity and authentication. Azure AD conditional access policies can be used to define policies that control how and when users can access resources, including sign-in policies. These policies can be configured to block access if certain conditions are not met, such as sign-ins from unknown locations or devices, which could trigger the message described in the question. Azure AD Identity Protection policies, on the other hand, focus more on detecting and responding to identity-based threats, such as password spray attacks or brute-force attacks, and may not be directly related to the sign-in issue described in the question.
upvoted 2 times

steveofrobust 1 year, 10 months ago
Tried with ChatGPT, at first it told me the option C is correct. However, i told it i thought D is the correct answer and here what it answered me:

“I apologize for the confusion. The correct answer is D. Microsoft Azure Active Directory (Azure AD) Identity Protection policies.

When a user sees the message "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.", it is likely due to a risk detected by Azure AD Identity Protection policies.

Azure AD Identity Protection policies can block access to applications if the user's risk level is too high. This can be caused by factors such as a high number of failed sign-in attempts, sign-in attempts from a suspicious location or device, or evidence of malware on the user's device.

Therefore, the correct answer to the question is D. Microsoft Azure Active Directory (Azure AD) Identity Protection policies.” It os funny.
upvoted 1 times

juras 1 year, 11 months ago
Selected Answer: D
I see where people are getting confused it is not the location you want to confirm which would make the answer C it is the identity which needs confirmation
upvoted 1 times

jaysoft 2 years ago
Selected Answer: C
While Identity Protection also offers a user interface for creating user risk policy and sign-in risk policy, we highly recommend that you use Azure AD Conditional Access to create risk-based policies

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#identity-protection-policies
upvoted 1 times

Paolo2022 2 years, 1 month ago

Selected Answer: C

The answer here can only be C - as there's no such things as an Identity Protection Policy: Identity Protection is the service that gathers threat signals that are then used by other MS services, such as Conditional Access evaluations.
Or, in MS's own words: "The signals generated by and fed to Identity Protection, can be further fed into tools like Conditional Access to make access decisions, or fed back to a security information and event management (SIEM) tool for further investigation."
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
upvoted 3 times

WickedMJ 2 years, 2 months ago

Selected Answer: D

"D. Microsoft Azure Active Directory (Azure AD) Identity Protection policies" is the correct answer

Reference:
https://www.examtopics.com/discussions/microsoft/view/11784-exam-ms-101-topic-1-question-26-discussion/
upvoted 1 times

Cebsiej_28 2 years, 4 months 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 determine access.
upvoted 1 times

RenegadeOrange 2 years, 5 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 years, 5 months 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 access policy, it can be used for reporting purposes only as well. Ca only blocks
upvoted 2 times

aaron_roman 2 years, 5 months ago

Selected Answer: D

Identity protection policies is based in Conditional Access for configuration - however they form a different service. I hope MS is consistent to its engineering
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies
upvoted 2 times

DenisRossi 2 years, 6 months 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 3 times

TechMinerUK 2 years, 6 months 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 2 times

Stiobhan 2 years, 6 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

Question #14 *Topic 3*

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.	○	○

Suggested 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 4 years, 10 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 Group 1 . 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 40 times

[Removed] Highly Voted 4 years, 5 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, 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 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 22 times

jwfm Most Recent 1 year, 11 months ago

no,no,NO

I tested the User 3 question and when the Default Platform type policy is turn off iOS enrollment. DEM account (User 3) CANNOT enroll. After login on iOS during enrollment DEM account just like any other will get "Something went wrong" Error.

Also the question maybe outdated, since Old interface is 1 policy can be set to multiple Platform but now all the policy are by Platform type in different type. So just to recreate Policy 1, you cannot just create Policy 1, but create 3 different policy than can be same name or different name to allow the platform. So it is possible that when the question is written DEM is allow to bypass, but currently (Jan 22, 2023) DEM is Blocked from enrolling iOS device when the iOS Platform is BLOCKED.

upvoted 1 times

donb21 2 years, 4 months ago

I go with N N Y as user3 assign with device enroll manager

upvoted 1 times

RenegadeOrange 2 years, 5 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 2 times

DenisRossi 2 years, 6 months 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 3 times

DenisRossi 2 years, 6 months 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 3 times

Durden871 2 years, 10 months ago

Is this really MS-100?

upvoted 4 times

TimurKazan 3 years, 4 months 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 2 years, 11 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 set 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 2 years, 11 months 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 3 years, 6 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 you don't believe me , test it for yourself.
upvoted 3 times

bsldwp_2020 3 years, 7 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-priority
upvoted 1 times

lucidgreen 3 years, 10 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 3 years, 10 months ago
Otherwise, it is Yes, Yes, Yes.
upvoted 2 times

Andy555 3 years, 11 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 4 years ago
N, N, Y for sure. cfalci
upvoted 5 times

madsa 4 years, 1 month 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 to a DEM account, but number of devices that can be enrolled does apply to a DEM account.

upvoted 1 times

shark1 4 years, 6 months ago

No

No - higher priority wins

Yes - DEM roles guys!

upvoted 6 times

zmart 4 years, 6 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

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.	○	○

Suggested 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 4 years, 11 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 56 times

test123123 4 years, 11 months ago
Yes, No, No
Device 2 is not compliant, as btilocker is not running.
upvoted 1 times

WoneSix 4 years, 10 months ago
test123123 (and earlier, zzuk and vikaswins), the question doesn't say anything about blocking all non-compliant devices. User2 isn't affectede by the policy in question, nor is device2 as long as a non-affected user is using it.
upvoted 6 times

Moji1 4 years, 11 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

[Removed] Highly Voted 4 years, 5 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 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 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 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
upvoted 23 times

JCkD4Ni3L Most Recent 1 year, 8 months ago
YNY, answer is correct.
upvoted 1 times

sehlohomoletsane 2 years, 11 months ago
can someone please explain what the answer is?
upvoted 1 times

lucidgreen 3 years, 10 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 8 times

Andy555 3 years, 11 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] 3 years, 11 months ago
YNY - User 2 is not part of CA.
upvoted 3 times

mkoprivnj 4 years ago
Y - N - Y
upvoted 4 times

Pabanda 4 years, 6 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 4 years, 5 months ago
I think you're right.
upvoted 1 times

Jhill777 4 years, 7 months ago
Because every Azure admin is going to create these types of scenarios to confuse themselves.
upvoted 10 times

ChrisKon 4 years, 7 months ago
What is the correct answer?
upvoted 1 times

STFN2019 4 years, 5 months ago
Yes no yes
upvoted 5 times

itmp 4 years, 8 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 5 years, 3 months 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 it not to be considered - maybe I need to recreate in a lab
upvoted 1 times

Mendel 5 years, 3 months 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 5 years, 3 months ago

It is because user 2 is trying to access from device 2 which is affected by policy.

upvoted 1 times

zzuk01 5 years 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 4 years, 10 months ago

Device 2 (bitlocker turned off)- Policy 2 (requires bitlocker). Thats why

upvoted 1 times

mafevaso 4 years, 6 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 3 years, 9 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 4 times

Question #16 *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 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

Suggested Answer: *B*
The question states that ɔ€all the user account synchronizations completed successfullyɔ€. 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 4 years, 11 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 4 years, 10 months ago
Agreed, Sisko - not ideal, but it will work if the new rule is configured correctly.
upvoted 3 times

Marz Highly Voted 4 years, 11 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 3 years, 9 months ago
Answer is no. You need to modify the Filter
upvoted 3 times

[Removed] 4 years 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 4 years ago
Answer is NO.
upvoted 3 times

paddyh 4 years 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 is wrong with the failed accounts
upvoted 1 times

LuckyCricket 4 years, 1 month 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. Hence - 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 test 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 you should select Y.

upvoted 7 times

donathon 4 years, 2 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 4 years, 6 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 4 years, 8 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 4 years, 11 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 4 years, 10 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 rerun the wizard and add the OU to the list of synched OUs, but the answer does give another (more problemmatic) way of solving the issue.

upvoted 3 times

Dylan 5 years ago

I guess it would have reported issues if there was an AD related issues, makes sense now! Ignore please...

upvoted 2 times

Dylan 5 years ago

Why would this fix the 10 problematic accounts?

upvoted 3 times

Question #17 *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 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

Suggested Answer: *B*
The question states that ɔ€all the user account synchronizations completed successfullyɔ€. 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 4 years, 2 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 errors and further more it does not fix the issue where the OU are not included in the sync.
upvoted 11 times

forummj Most Recent 2 years, 3 months 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 to Azure AD" and "all the user account synchronizations completed successfully."
upvoted 1 times

forummj 2 years, 3 months ago
Scratch that. I've reread the question. Ignore the above comment.
upvoted 2 times

Ash473 3 years, 4 months ago
In exam today
upvoted 3 times

MartiFC 3 years, 5 months ago
Not for sure!
upvoted 2 times

mkoprivnj 4 years ago
No for sure!
upvoted 3 times

Question #18 *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 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

Suggested 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 4 years, 2 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 7 times

Ash473 Most Recent 3 years, 4 months ago
In exam today as multiple choice
upvoted 2 times

MartiFC 3 years, 5 months ago
No, because there are not any errors to sync.
upvoted 2 times

mkoprivnj 4 years ago
Answer is NO.
upvoted 2 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:

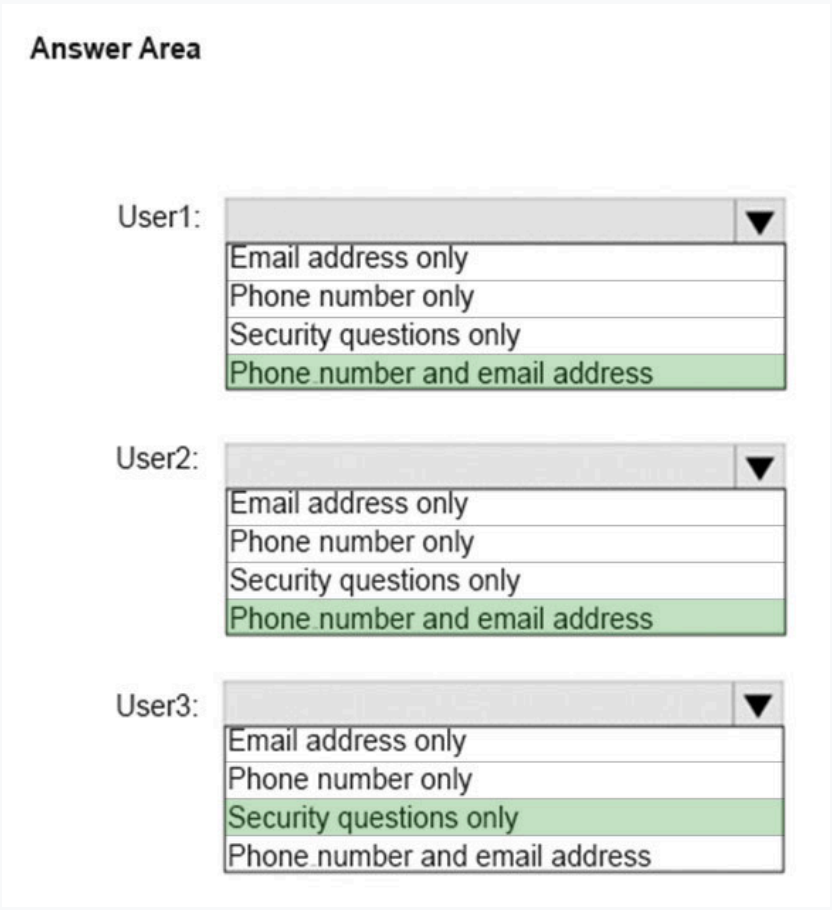
Answer Area

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

Suggested Answer:



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

BennyS Highly Voted 2 years, 10 months 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 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.
Source: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences
upvoted 6 times

Amir1909 Most Recent 11 months ago

Correct
upvoted 1 times

Moderator 2 years, 5 months ago

Still a valid question (July 30th 2022).
upvoted 4 times

melatocaroca 3 years, 6 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 3 years, 6 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 3 years, 7 months ago

exam question on 28May21

upvoted 4 times

F_M 3 years, 7 months ago

Provided answer is right!

upvoted 4 times

Question #20 *Topic 3*

HOTSPOT -

You have a Microsoft 365 subscription.

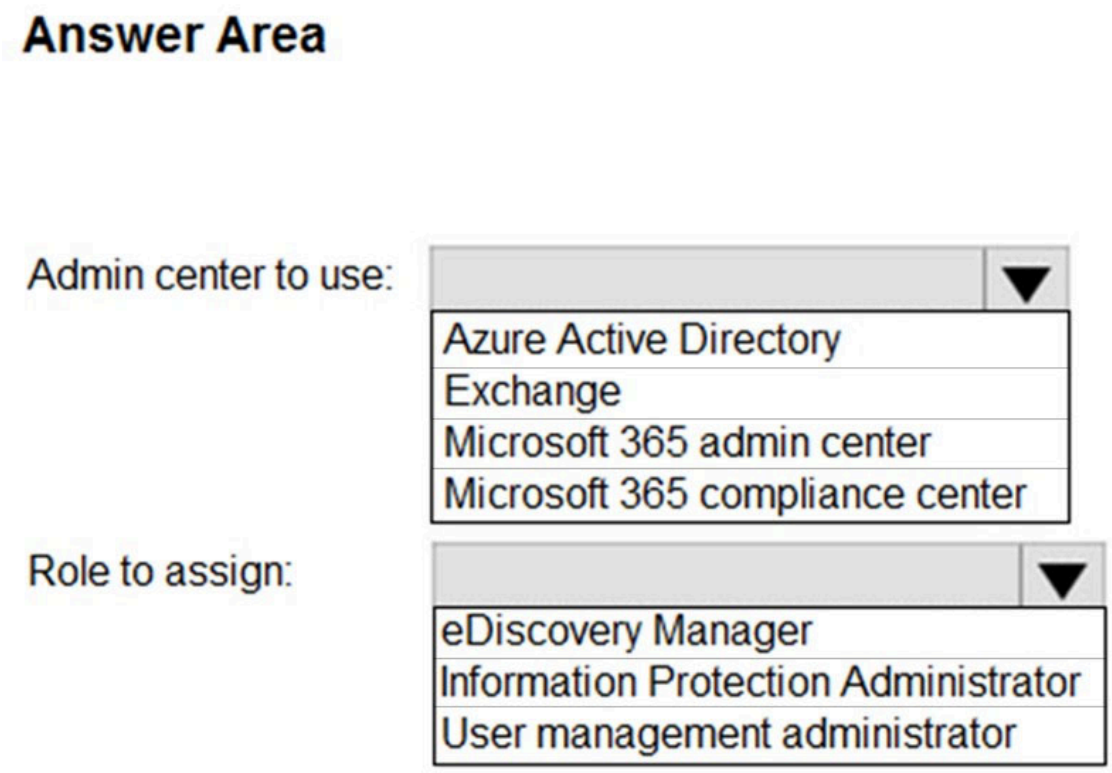
You need to provide an administrator named Admin1 with the ability to place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations.

The solution must use the principle of least privilege.

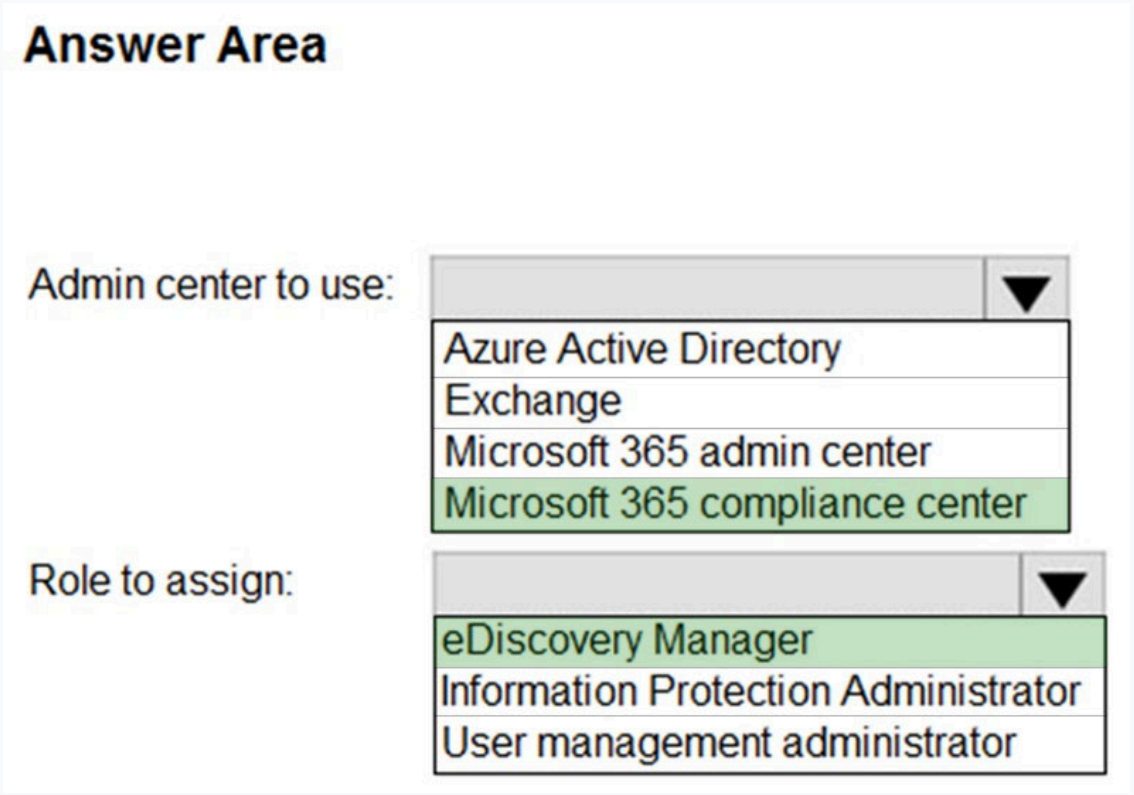
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



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 Highly Voted 2 years, 4 months 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 6 times

JCkD4Ni3L Most Recent 1 year, 8 months ago

Answers are correct.

upvoted 1 times

st2023 1 year, 10 months ago

for those who have not heard of a "hold", here hold is referring to legal hold on documents. This article explains it well:
https://www.exterro.com/basics-of-e-discovery/legal-hold

upvoted 2 times

Question #21 *Topic 3*

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.

Suggested 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

Amir1909 11 months ago
Correct
upvoted 1 times

m2L 1 year ago
Hello Guys, according to the link below, 8 hours is just the required time for the admin to activate the role if a user requests it.
For example: if User1 requests an admin role.
the PIM admin has 8 hours to activate the role for User1. 8 hours after the requests of User1 if the admin doesn't activate the role for him, the request will expire and User1 has to request again.
But if the admin activates the role for User1 within 8 hours, User1 will have 15 days to do his job. After 15 days he will lose the role.
https://learn.microsoft.com/fr-fr/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings
upvoted 1 times

st2023 1 year, 10 months ago
Based on these links and some testing I conclude A and B are correct
User Admin can:
1.reset password's of these roles:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords

2.delete these roles:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-perform-sensitive-actions

since exchange admin wasn't listed in the table I tested it myself.

-User admin is un-able to reset password for exchange admin(received the following message):
Exchange Admin 1 : 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

-User admin is un-able to delete exchange admin(received the following message):
Delete user failed
Couldn't delete this user. Please try again later.
upvoted 3 times

sehlohomoletsane 1 year, 10 months ago
AB is correct
upvoted 2 times

Question #22 *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 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

Suggested 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

sehlohomoletsane 1 year, 9 months ago
So basically the answer is YES in short
upvoted 1 times

JakeH 3 years, 1 month ago
In exam today
upvoted 3 times

junior6995 3 years, 3 months ago
Filtering is where you select the OU's to be synchronized with AAD.
upvoted 4 times

MartiFC 3 years, 5 months ago
If the sync is succesfully, then will see the filtering settings
upvoted 2 times

Question #23 *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 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

Suggested 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

Community vote distribution
A (100%)

saumade Highly Voted 5 years 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 35 times

itmp 4 years, 7 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 3 years, 11 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 3 years, 7 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 4 years, 9 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 4 years, 5 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 4 years, 1 month 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 26 times

originalwitness 4 years, 1 month ago

This makes much more sense than the other explanations. Tricky wording!

upvoted 4 times

Maroslaw 3 years, 6 months ago

Correct, tested on my E3

upvoted 2 times

JCkD4Ni3L Most Recent 1 year, 8 months ago

Selected Answer: A

Correct answer is A.
This should clean any doubt: https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-account-license-and-service-details-with-microsoft-365-powershell?view=o365-worldwide#to-view-services-for-a-user-account-1

upvoted 1 times

ARZIMMADAR 1 year, 11 months ago

Guys the Msol user cmdelt will only display the users who are licensed not what licenses they have. Answer is most definitely Azure portal, licenses blade.

upvoted 1 times

Cebsiej_28 2 years, 4 months ago

B is correct because Get-MsolUser cmd will only tell you if the user is licensed or not.

upvoted 1 times

Stiobhan 2 years, 7 months 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 4 times

KSvh53 2 years, 9 months 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're 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 see in Microsoft 365 Admin Center under that user.
upvoted 1 times

mikaiwhodakno 2 years, 6 months 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 2 years, 9 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 2 years, 6 months 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 3 years ago
tested - answer is A
upvoted 1 times

tf444 3 years ago
Get-MsolUser -All | where {$_.isLicensed -eq $true}.
upvoted 1 times

EaaGleee 3 years ago
Selected Answer: A
get-msoluser -UserPrincipalName abcd@example.com | select -ExpandProperty licenses | ft AccountSkuId
upvoted 1 times

Madball 3 years, 4 months 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 4 times

Fcnet 3 years, 5 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 3 years, 6 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 2 years, 11 months 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 3 years, 6 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 3 years, 7 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 that there is no way.

upvoted 1 times

mackypatio 3 years, 7 months ago

i meant powershell way, currently there is no way.

upvoted 1 times

mackypatio 3 years, 7 months ago

i stand corrected, (get-msoluser -userprincipalname user1@domain.com).licenses.servicestatus

upvoted 2 times

Razuli 3 years, 8 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 this on my tenant

upvoted 1 times

Question #24 *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 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

Suggested 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 3 years, 2 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 3 times

mkoprivnj 4 years ago
No for sure!
upvoted 1 times

melatocaroca 3 years, 6 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 4 years, 1 month 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 4 years, 2 months ago
B
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolaccountsku?view=azureadps-1.0
upvoted 1 times

Question #25 *Topic 3*

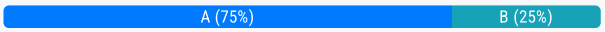
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer 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 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

Suggested 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.

Community vote distribution



Faheem2020 Highly Voted 4 years ago
I take back the earlier comment. You can do it from license blade.
upvoted 9 times

Faheem2020 Highly Voted 4 years 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 within the license that can be enabled for the users
upvoted 6 times

J0J0 3 years, 6 months ago
you're wrong. Definitely correct, but not the shortest path to check.
upvoted 5 times

Takloy 3 years, 11 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

JCkD4Ni3L Most Recent 1 year, 8 months ago
Selected Answer: A
From the license blade itself (at the root) = No
From the details of the subsection of license blade = Yes

It can be debated whether using the sublinks under the licence blade IS actually the license blade... so I would go with Yes on the technical aspect of it. After all "From the License blade" you are able to get the information you require, no ?
upvoted 1 times

m43s 2 years, 6 months ago
Selected Answer: A
correct is A

upvoted 1 times

Cebsiej_28 2 years, 8 months 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/licenses only.

upvoted 1 times

ARYMBS 2 years, 8 months 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 go for B. Either way this depends on how you understand a question.

upvoted 1 times

trexar 2 years, 9 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 3 years, 2 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 will see all the assigned Services.
Long way, but doable.

upvoted 4 times

josemariamr 3 years, 7 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 and 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 list of users, then click the user, etc.

upvoted 4 times

Razuli 3 years, 8 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 3 years, 8 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 3 years, 11 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 click 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 4 years ago

Yes for sure!

upvoted 1 times

mkoprivnj 4 years ago

NO is correct. Reference to Faheem2020's answer!

upvoted 1 times

cdsa 3 years, 11 months ago

Yes, Selecting the license will show the users assigned.

upvoted 2 times

MerryWeasel 3 years, 11 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 3 years, 11 months ago

He was wrong please, YES is correct. Please do your homework.

upvoted 2 times

jnecode 4 years, 3 months ago

Licenses blade then click the EO license and all users that have the license will show up. Correct Answer.

upvoted 1 times

AlexanderSaad 4 years, 9 months ago

From azure ad - licenses - you cannot see if the user is licenses for a single service only.

upvoted 1 times

AlexanderSaad 4 years, 8 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 4 years, 4 months ago

So is the answer correct or not? Is the "licenses blade" the same as the "user account -> licenses -> expand"?

upvoted 1 times

donathon 4 years, 2 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 4 years, 2 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

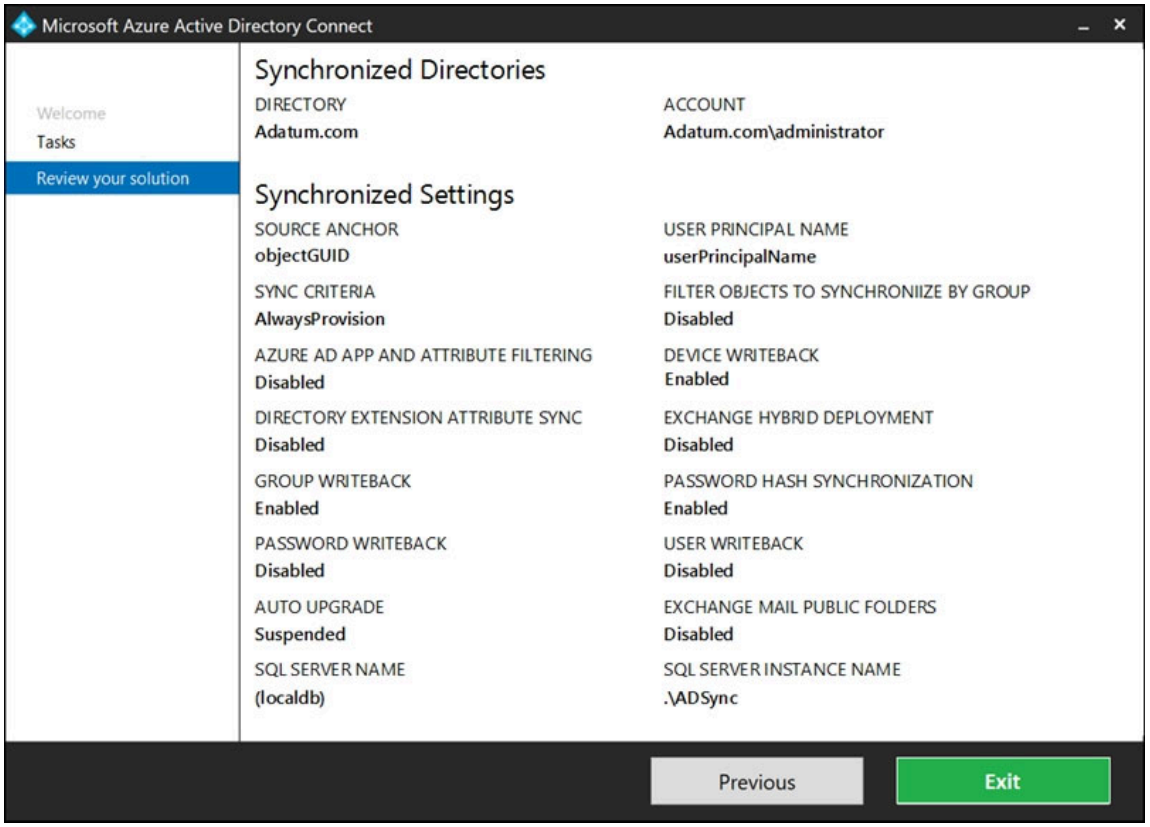
steven1 4 years, 11 months ago

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

Suggested Answer:

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**

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 3 years, 9 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 18 times

eknnob 3 years, 9 months ago
you are correct Security group will not sync
upvoted 19 times

LillyLiver 2 years, 11 months 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 setup. So the group won't be written back.

As I understand it anyway.
upvoted 1 times

RenegadeOrange 2 years, 5 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 10 times

Paolo2022 2 years, 1 month ago
Thanks for the link!

This makes it clear:
"There are two versions of group writeback. The original version is in general availability and is limited to writing back Microsoft 365 groups to your on-premises Active Directory instance as distribution groups. The new, expanded version of group writeback is in public preview and enables the following capabilities:
- You can write back Microsoft 365 groups as distribution groups, security groups, or mail-enabled security groups.
- You can write back Azure AD security groups as security groups."
upvoted 1 times

One111 2 years ago
Groups sync v2 can't be configured in Azure AD Connect, but only with PowerShell. Also, there is no way to check GroupWritebackV2 feature status in AADC.
upvoted 1 times

Eltooth Highly Voted 3 years, 8 months ago
Also group write back has specific requirements before only M365 groups can sync back...including Exchange Hybrid. Image shows that 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 10 times

One111 Most Recent 2 years ago
Groups sync v2 can't be configured in Azure AD Connect, but only with PowerShell. Also, there is no way to check GroupWritebackV2 feature status in AADC.

The new version is enabled on the tenant and not per Azure AD Connect client instance. Make sure that all Azure AD Connect client instances are updated to a minimal build of Azure AD Connect version 2.0 or later if group writeback is currently enabled on the client instance.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback-v2
upvoted 1 times

Mage10 2 years, 1 month ago

answer is correct,"Use Azure AD Connect to write cloud groups, including security groups, back to your on-premises Active Directory. With this preview, yo managed in the cloud.06 Jul 2022"
https://www.google.com/search?q=can+security+group+in+azure+ad+sync+back+on+prem&rlz=1C1SQJL_enZA856ZA856&oq=can+security+group+in+azure+ad+sync+back+on+prem&aqs 8

upvoted 2 times

amitsharma170490 2 years, 3 months ago

Now you can writeback Azure AD security Groups to On-premise AD: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback-v2

upvoted 2 times

One111 2 years ago

But it can't be configured or viewed in AADC, it can only be accomplished in PowerShell.

upvoted 1 times

rajeshrengasamy 2 years, 3 months 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 2 times

One111 2 years ago

But it can't be configured or viewed in AADC, it can only be accomplished in PowerShell.

upvoted 1 times

Contactfornitish 2 years, 5 months ago

1. Only O365 groups sync, not security groups
2. Device writeback enabled so device would sync

upvoted 1 times

charat 2 years, 7 months 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 2 years, 7 months 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, then you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange present in your on-premises Active Directory.

upvoted 1 times

BoxGhost 2 years, 8 months 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 2 years, 10 months 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 3 years 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 3 years, 2 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 comment are welcome
upvoted 1 times

fofo1960 3 years, 2 months ago
But the Microsoft 365 Group are written back, so Security group wont be Synced down to AD
upvoted 1 times

Davidchercm 3 years, 4 months ago
is the answer for the device showing correct ?
upvoted 2 times

junior6995 3 years, 3 months ago
For the security group, definitely not syncing, for the computers, I'd go for not syncing as well.
upvoted 2 times

Greyexam 3 years, 6 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 3 years, 7 months ago
MS-100 Exam question on 28May21
upvoted 2 times

PlumpyTumbler 3 years, 7 months ago
MS-101 question anyway.
upvoted 1 times

Goseu 3 years, 8 months ago
Groups writeback enables customers to leverage cloud groups for their hybrid needs. If you use the Microsoft 365 Groups feature, then you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange present in your on-premises Active Directory.
upvoted 1 times

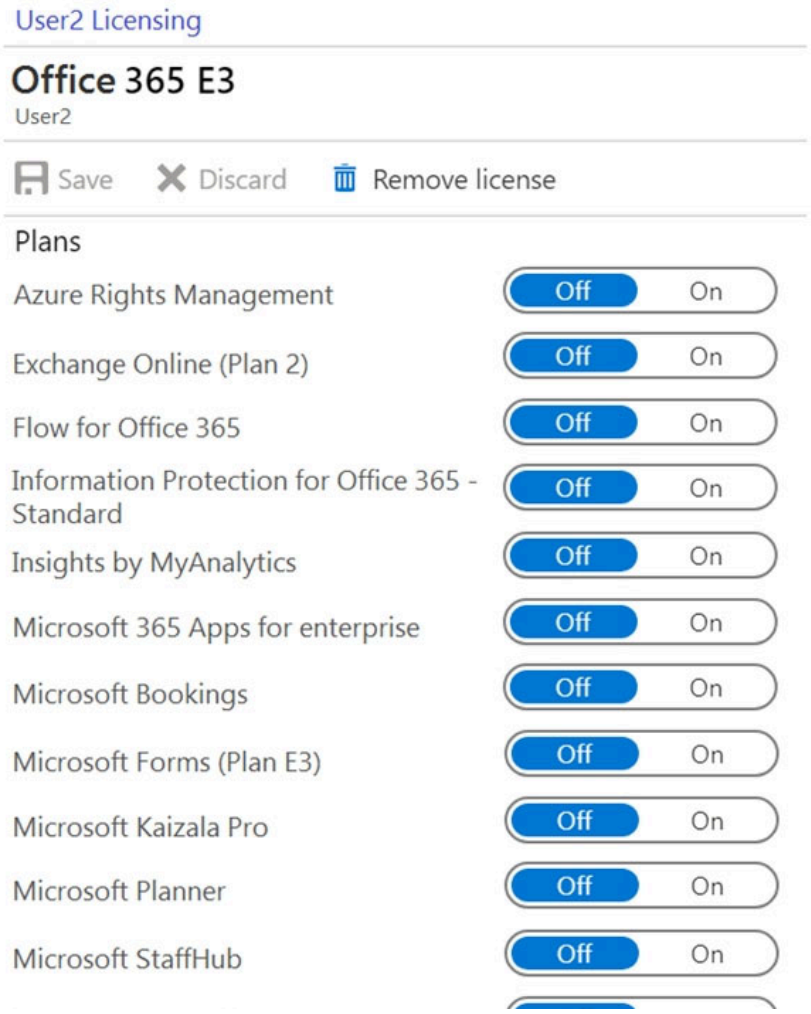
HOTSPOT -

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

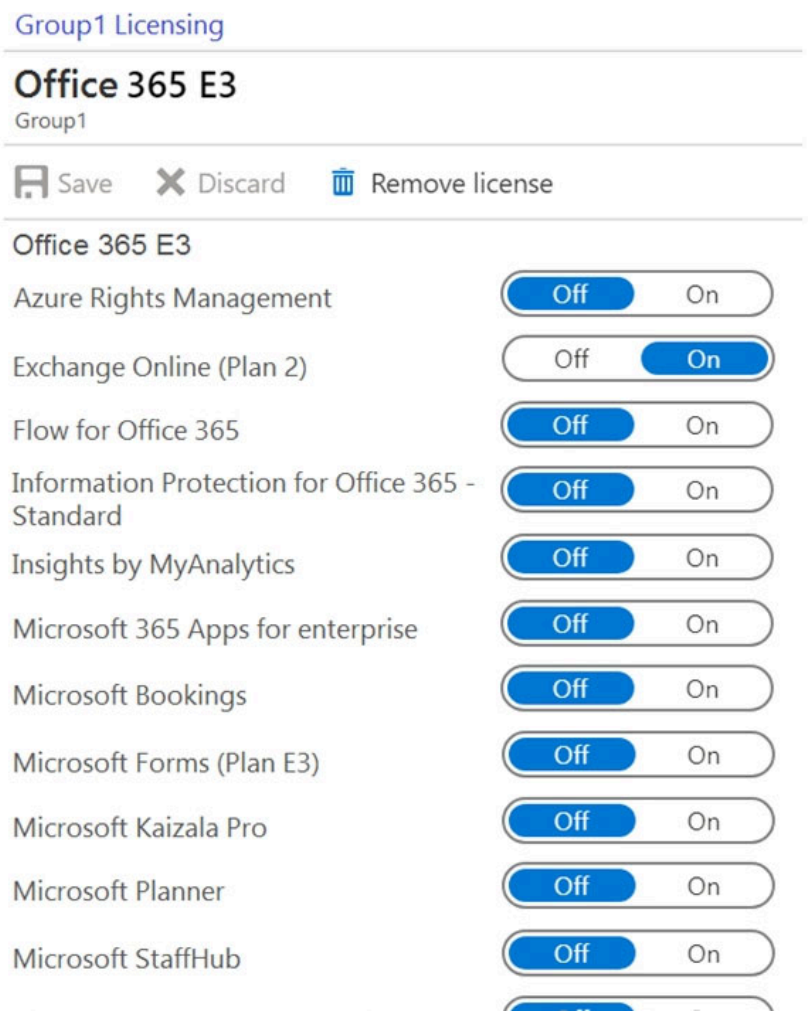
Name	Usage location	Membership
User1	*Not set*	Group1
User2	United States	Group2
User3	United States	*Not applicable*

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.	○	○

Suggested 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 3 years, 6 months ago
Tested this in my Azure demo environment. Y,N,N is correct
upvoted 12 times

davem90 Highly Voted 3 years 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 8 times

vanr2000 Most Recent 1 year, 8 months ago
For me they're N/N/N

Without user location, you cannot assign a license.
upvoted 3 times

One111 1 year, 3 months ago
Only manually, if you user group based licensing IT will be applied.
upvoted 1 times

One111 2 years ago
Some features in Office 365 are not allowed in certain countries and Microsoft determines this with the help of UsageLocation attribute. This attribute is required.

How to user could be using Exchange without Usagelocation andmsExchUsageLocation?
upvoted 1 times

Cheekypoo 2 years, 5 months ago
Was in my exam today 05/08/22.
upvoted 3 times

Contactfornitish 2 years, 5 months 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 2 times

tejb 3 years, 3 months 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 3 years, 3 months 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 3 years, 4 months ago
it was in my exam
upvoted 2 times

john_gros 3 years, 5 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 3 years, 4 months ago
Check again, Exchange is set to "ON"
upvoted 2 times

jjong 3 years, 3 months ago
its not all ON for group 1... u're seeing it wrongly.. like me. :)
upvoted 1 times

dmillion 3 years, 8 months ago
user2 have the "sharepoint online" selected in the exhibition. not showing in this screenshot.
upvoted 3 times

chaoscreater 3 years, 6 months ago
But not Exchange Online, so answer is still correct.
upvoted 3 times

Eltooth 3 years, 8 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 3 years, 9 months ago
No/No/No
User1 should fail to assign a license because the usage location is Not set.
upvoted 3 times

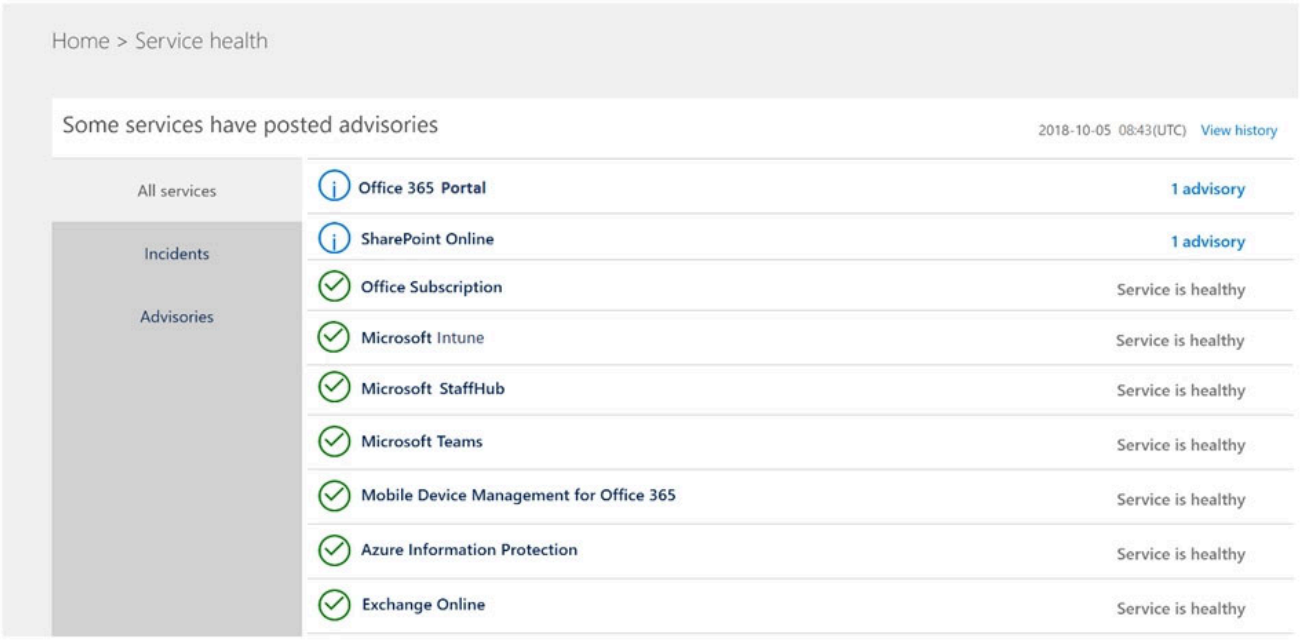
syswiz85 3 years, 8 months ago
incorrect, if a usage location is NOT set, it will inherit a location from the group instead.
upvoted 10 times

BGM_YKA 3 years, 7 months ago
Location is set with Group membership for that License. Therefore user1 is licensed. Without seeing Sharepoint licensing I believe it is beset to assume not licensed. My answer would be Y/N/N
upvoted 5 times

Question #28 *Topic 3*

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

Suggested 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

Community vote distribution

D (77%) B (18%) 5%

Mike3033 Highly Voted 3 years, 5 months ago

The role is actually 'Service Support Administrator'

upvoted 13 times

mic88 3 years, 3 months 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, 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, see About admin roles."

upvoted 2 times

Everlastday Highly Voted 1 year, 12 months ago

Was on Exam 03.01.2023

upvoted 7 times

JCkD4Ni3L Most Recent 1 year, 8 months ago

Selected Answer: D

D is correct.
If any doubt: https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide#how-to-check-service-health
upvoted 1 times

JamesWilliams 1 year, 9 months ago

Selected Answer: B

s usuários que têm a função "Leitor do Centro de Mensagens" no Microsoft SharePoint Online podem visualizar os avisos para investigar problemas de integridade do serviço
upvoted 1 times

trexar 2 years, 9 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 4 times

jage01 2 years, 9 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 4 times

trexar 2 years, 10 months ago

Selected Answer: D

'Service Support Administrator has access to microsoft.azure.serviceHealth/allEntities/allTasks
upvoted 3 times

trexar 2 years, 10 months ago

Selected Answer: C

Service support administrator have access to microsoft.azure.serviceHealth/allEntities/allTasks
upvoted 1 times

sliix 2 years, 10 months 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 5 times

MEC123 2 years, 11 months 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 see 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 2 times

dumpmaster 2 years, 11 months ago

Selected Answer: B

I guess is B: http://shortcutshari.com/o365-update-new-feature-message-center-reader-role/

upvoted 3 times

Claire91 3 years ago

D for me

Given answer is correct (ish)
Service Administrator is also known as Service Support Administrator

upvoted 2 times

Claire91 3 years ago

https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide

upvoted 1 times

fofo1960 3 years, 2 months ago

Why not Message Center reader ?

upvoted 2 times

Jubei612 3 years, 2 months ago

The users administer. That is the key word to help identify the right answer.

upvoted 1 times

MDLima 3 years, 2 months 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 would 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 3 years, 3 months ago

If we follow the least privilege principle the Message Center reader will be more appropriated

upvoted 4 times

Ash473 3 years, 4 months ago

was in exam today

upvoted 2 times

Question #29 *Topic 3*

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

Suggested 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

Community vote distribution
A (100%)

Eltooth Highly Voted 3 years, 8 months ago
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions
upvoted 7 times

dumpmaster Highly Voted 2 years, 11 months 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 5 times

Amir1909 Most Recent 11 months ago
A is correct
upvoted 1 times

Amir1909 11 months ago
A is correct
upvoted 1 times

Oval61251 2 years, 1 month ago
Key word review, so Security Reader would apply
upvoted 1 times

tejb 3 years, 3 months ago

Permissions
Identity Protection requires users be a Security Reader, Security Operator, Security Administrator, Global Reader, or Global Administrator in order to access.

Source: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
upvoted 2 times

fko1978 3 years, 3 months ago
review (=not change) so, Security reader: View all Identity Protection reports and Overview blade
upvoted 3 times

TimurKazan 3 years, 4 months ago
so I would go with Global Admin. User Administrator has nothing to do with Azure Identity Protection
upvoted 1 times

Turak64 3 years, 4 months ago
"The solution must use the principle of least privilege."
upvoted 2 times

TimurKazan 3 years, 3 months ago
it is actually the least possible privilege to perform such tasks from this list of given roles
upvoted 1 times

Azreal_75 3 years, 2 months ago
It isn;t, see role descriptions here: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions
upvoted 3 times

Luiza 3 years, 6 months ago
B. User administrator

"Review" is not "Read"
upvoted 1 times

TimurKazan 3 years, 4 months ago
Correct. but in this case it should be Security Administrator
upvoted 1 times

junior6995 3 years, 7 months ago
Should I consider "Review" and "Read" the same?
upvoted 1 times

airairo 3 years, 7 months ago
This is in ms 101
upvoted 1 times

LouahZA 3 years, 4 months ago
i had this on my first go on ms-100
upvoted 4 times

Question #30 *Topic 3*

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.

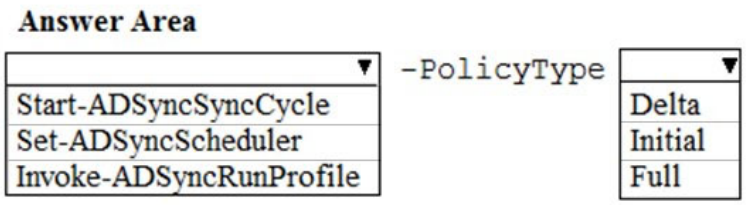
You automate the creation of 100 new user accounts.

You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

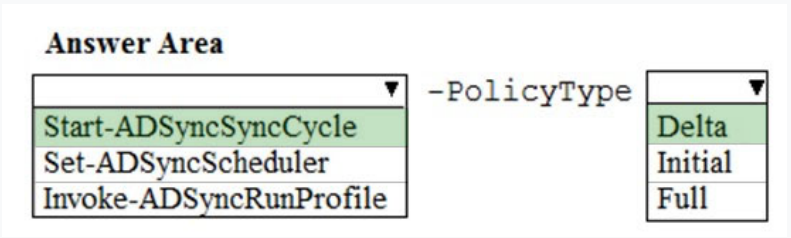
Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested 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 4 years ago

syncsync cycle + delta is correct!

upvoted 13 times

Amir1909 Most Recent 11 months ago

Correct

upvoted 1 times

Everlastday 1 year, 12 months ago

On Exam 03.01.2023

upvoted 4 times

jjong 3 years, 3 months ago

came out today on my exam on 27-sep-21

upvoted 3 times

Ash473 3 years, 4 months ago

in exam today

upvoted 4 times

melatocaroca 3 years, 6 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 4 times

Alvaroll 4 years, 3 months ago
2-13 https://www.examtopics.com/exams/microsoft/ms-100/view/12/
upvoted 2 times

saasaa 4 years, 6 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

Suggested 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

Community vote distribution
B (100%)

lusis987 Highly Voted 4 years, 10 months ago
If AD can access all 3 forests - enough with one server that syncs everything.
upvoted 18 times

[Removed] Highly Voted 4 years, 5 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 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
upvoted 15 times

donathon 4 years, 3 months 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, you 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

Amir1909 Most Recent 11 months ago
B is correct
upvoted 1 times

st2023 1 year, 10 months ago
➪https://learn.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-forests-single-azure-ad-tenant
➪https://learn.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-forests-multiple-sync-servers-to-one-azure-ad-tenant
➪https://learn.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#staging-server
upvoted 1 times

Cheekypoo 2 years, 5 months ago
Was in my exam today 05/08/22.
upvoted 2 times

charat 2 years, 7 months ago

Selected Answer: B

In exam on 05/22.

upvoted 5 times

JakeH 3 years, 1 month ago

In exam today

upvoted 1 times

melatocaroca 3 years, 6 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 2 times

lucidgreen 3 years, 10 months ago

You can only have one AD Connect server active per tenant. So B.

upvoted 4 times

lucidgreen 3 years, 9 months ago

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

upvoted 1 times

mkoprivnj 4 years ago

B for sure!

upvoted 2 times

kazaki 4 years, 6 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 of 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

mmdcert 4 years, 9 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 of 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 4 years, 9 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 4 years, 10 months ago

Should be A. You can only have 1 ADConnect for forest

upvoted 3 times

WoneSix 4 years, 10 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 4 years, 10 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 to synch to two tenants.

upvoted 4 times

AADapson 4 years, 1 month ago

You can have One Active ADConnect and another one in staging mode. You can't have two active ADConnect

upvoted 1 times

Question #32 *Topic 3*

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.

Suggested 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 4 years ago
C for sure. From AD modify city attribute!
upvoted 13 times

lucidgreen 3 years, 8 months ago
Yes, you're modifying the user in AD, not the cloud.
upvoted 5 times

syswiz85 3 years, 8 months ago
100% correct
upvoted 3 times

Amir1909 Most Recent 11 months ago
C is correct
upvoted 1 times

Amir1909 11 months ago
Correct
upvoted 1 times

MomoLomo 3 years, 4 months ago
on ms-100
upvoted 1 times

MartiFC 3 years, 5 months ago
C is correct. The change have to from AD on-premises

upvoted 3 times

venwaik 3 years, 5 months ago

Got the question on 19th of July 2021

upvoted 2 times

RAJULROS 3 years, 7 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

Suggested Answer: *B*

Community vote distribution

[Removed] Highly Voted 4 years 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 just 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 check the box for west.contoso.com.
upvoted 21 times

DesertStorm Highly Voted 3 years, 6 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 10 times

michszym 3 years, 5 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 3 times

vanr2000 Most Recent 1 year, 8 months ago
Selected Answer: A
If you added or removed domains in your forest after you installed Azure AD Connect, you also have to update the filtering configuration.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#domain-based-filtering

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom#domain-and-ou-filtering
upvoted 1 times

Exam99111 1 year, 9 months ago
A. Yes
This solution should meet the goal of syncing the new domain west.contoso.com to the Azure AD tenant. By running the setup wizard on the Azure AD Connect server in contoso.com and including the west.contoso.com domain, the necessary configuration and synchronization rules should be set up to ensure that the new domain is synchronized to Azure AD

upvoted 1 times

gills 1 year, 10 months ago

Selected Answer: B

This is only a sub domain. Not a new domain.

upvoted 2 times

suvittech 1 year, 11 months ago

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#single-forest-single-azure-ad-tenant

upvoted 1 times

donb21 2 years, 4 months ago

personally i think this should go with A

upvoted 1 times

DenisRossi 2 years, 6 months ago

Selected Answer: A

Just run the wizard

upvoted 1 times

Mea988 2 years, 10 months ago

Selected Answer: A

Wizard automates everything. A

upvoted 3 times

vnet1 2 years, 11 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 3 times

VictorPCS 2 years, 11 months ago

Selected Answer: B

Running the wizard again should do the job

upvoted 2 times

kanag1 2 years, 11 months 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 4 times

jkklim 3 years ago

answer is yes

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

upvoted 3 times

tejb 3 years, 3 months ago

Answer is NO. Need to rerun the AAD Connect wizard with "Refresh Schema" option

upvoted 4 times

Chipper 3 years, 3 months ago

it states that AD connect is already deployed and syncing with the Azure Tenant "An Azure AD Connect server is deployed to contoso.com. Azure AD Connect syncs to an Azure Active Directory (Azure AD) tenant."

So shouldn't the answer be A?

upvoted 3 times

TimurKazan 3 years, 3 months 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 3 years, 6 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 3 years, 6 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

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

Suggested 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

Community vote distribution
AC (100%)

VP11 Highly Voted 4 years, 9 months ago
The Group writeback feature does not handle security groups or distribution groups.
upvoted 25 times

hufflepuff 2 years, 2 months ago
This is no longer correct - In AD Connect V2 all are supported.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback-v2
upvoted 10 times

kerberos99 1 year, 11 months ago
Still in Public Preview…
upvoted 2 times

sovis29088 Highly Voted 3 years, 2 months ago
This question conflicts with a previous one a page or two back where the correct answer indicated that an AzureAD security group would 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 17 times

BigDazza_111 Most Recent 1 year, 7 months ago
Selected Answer: AC
correct 'There are two versions of group writeback. The original version is in general availability and is limited to writing back Microsoft 365 groups to your on-premises Active Directory instance as distribution groups. The new, expanded version of group writeback is in public preview and enables the following capabilities:

You can write back Microsoft 365 groups as distribution groups, security groups, or mail-enabled security groups.
You can write back Azure AD security groups as security groups.
All groups are written back with a group scope of Universal.
You can write back groups that have assigned and dynamic memberships.'
upvoted 1 times

JCkD4Ni3L 1 year, 8 months ago
Selected Answer: AC

Well, at the time of the writing of this question the answer was A & C, now it is A,B,C,D and E. Since we can only choose 2, have to answer the question in a more legacy context, thus A and C.

upvoted 1 times

RenegadeOrange 2 years, 5 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 13 times

Paolo2022 2 years, 1 month ago

That didn't use to be the case, that's why the mix of old questions, assuming the limitation to O365 groups, and new ones with a broader sync scope can lead to confusion.

See the link provided in other comments already:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-group-writeback-v2

upvoted 1 times

bill1982 2 years, 5 months 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 written 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 AD Connect.

You can now configure Azure AD groups to writeback using the Azure AD Admin portal, Graph Explorer, and PowerShell.

upvoted 4 times

trexar 2 years, 9 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, then you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange present in your on-premises Active Directory.

upvoted 1 times

Boeroe 2 years, 10 months 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 3 years 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, then you can have these groups represented in your on-premises Active Directory. This option is only available if you have Exchange present in your on-premises Active Directory.

upvoted 1 times

tf444 3 years 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 3 years ago
IF the 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.
in another Q in exam topic.
upvoted 1 times

JakeH 3 years, 1 month ago
In exam today
upvoted 1 times

fofo1960 3 years, 2 months ago
Tested, and One A & C are correct, Security or Dist groups wont be written back.
upvoted 3 times

Eltooth 3 years, 8 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 3 years, 11 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

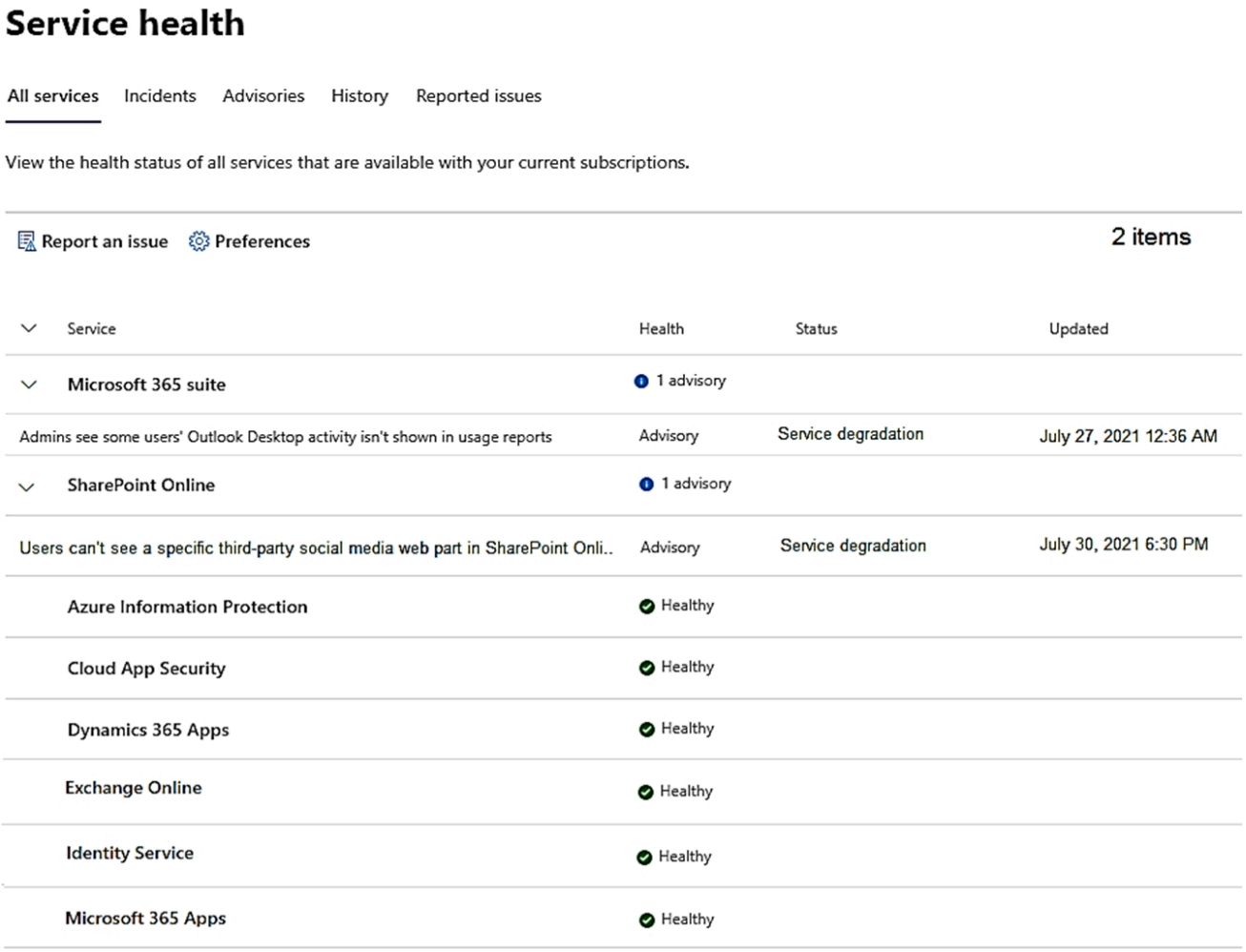
mkoprivnj 4 years ago
A & C for sure!
upvoted 3 times

phvogel 4 years, 2 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 is required). Writeback only works with Office 365 groups.
upvoted 4 times

Question #35 *Topic 3*

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

Suggested 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

Community vote distribution

D (100%)

n0t_a_good_t1m3 2 years, 1 month ago

on exam as of three days ago

upvoted 4 times

EliasMartinelli 2 years, 2 months ago

Selected Answer: D

D is correct

upvoted 1 times

boxojunk 2 years, 3 months 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

Question #36 *Topic 3*

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

Suggested 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/

Community vote distribution
C (100%)

Eltooth Highly Voted 3 years, 8 months ago
C - https://docs.microsoft.com/en-us/sharepoint/hybrid/accounts-needed-for-hybrid-configuration-and-testing
upvoted 11 times

sohopros Most Recent 2 years, 2 months ago
MS-100 question still relevant on 10/21/22
upvoted 3 times

charat 2 years, 7 months ago
Selected Answer: C
Good question. C is the answer
upvoted 2 times

RazielLycas 2 years, 10 months 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 3 years, 4 months ago
on ms-100
upvoted 2 times

PlumpyTumbler 3 years, 7 months ago
This is on MS-101.
upvoted 2 times

Question #37 *Topic 3*

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.

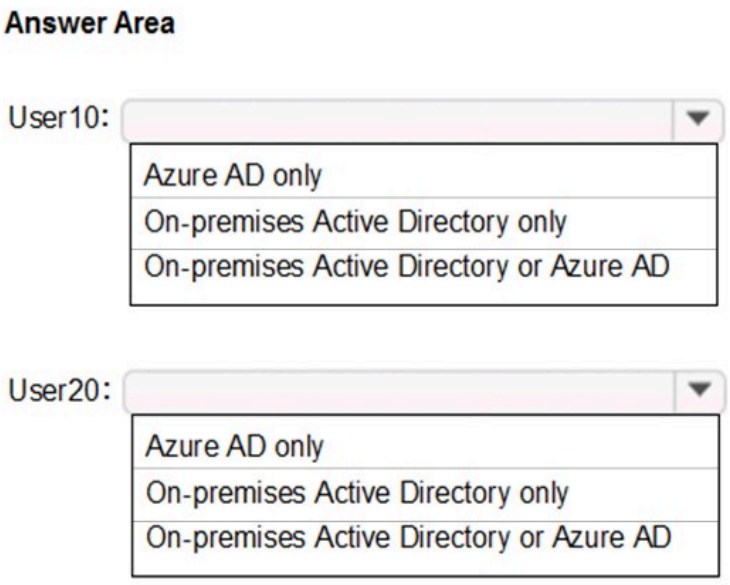
You create a new user named User10 on-premises and a new user named User20 in Azure AD.

You need to identify where an administrator can reset the password of each new user.

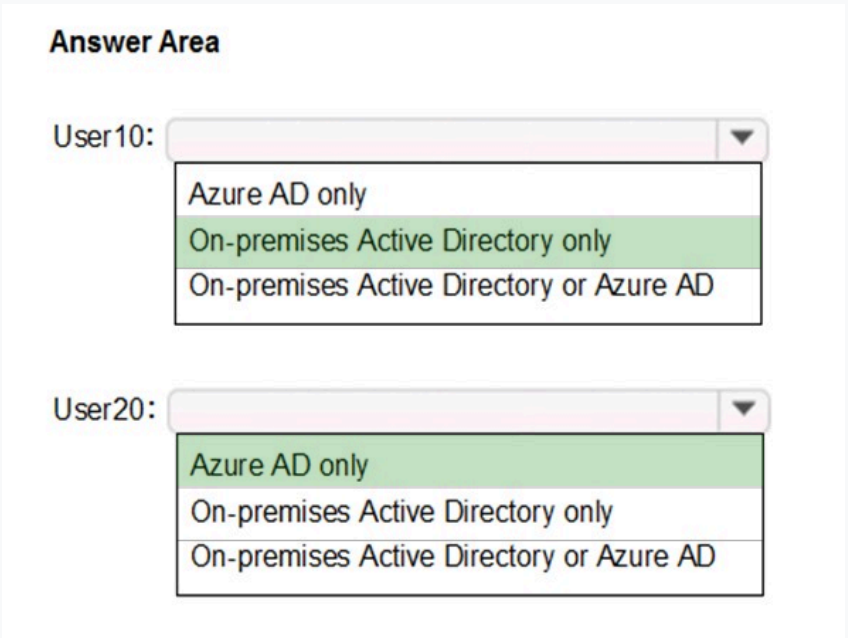
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested 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 3 years, 8 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 back the on-premise credentials, so this is not a viable solution. Answers provided are 100% correct without a doubt.

upvoted 10 times

Amir1909 Most Recent 11 months ago

Correct
upvoted 1 times

Moderator 2 years, 4 months ago
Question still valid (30th July 2022).
upvoted 1 times

n0t_a_good_t1m3 2 years, 1 month ago
On exam as of two days ago
upvoted 3 times

tcmaggio 3 years, 1 month ago
I will stand with given answer BUT, imho, the Admin COULD reset password either using AD (hash sync) or AzAd. Of course, AzAd would be the better way: Yes! But the question says: where you CAN, not which would be the better way to do so.
upvoted 4 times

TimurKazan 3 years, 4 months 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 3 times

TimurKazan 3 years, 4 months ago
Sorry, User10 - AD only, since password writeback is disabled
upvoted 17 times

Ash473 3 years, 4 months ago
in exam today
upvoted 2 times

chan2013 3 years, 8 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 3 years, 8 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 3 years, 6 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.

Suggested 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

[Removed] Highly Voted 4 years, 5 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 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
upvoted 21 times

DavidSapery Highly Voted 4 years, 6 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 the users' UPN suffixes.
upvoted 13 times

Amir1909 Most Recent 11 months ago
B is correct
upvoted 1 times

KennethYY 1 year, 5 months ago
maybe outdate, even the UPN is not routable DNS, Azure AD connect still can sync, just cannot SSO
upvoted 1 times

mikl 3 years, 9 months ago
Think "B. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix." is correct.
upvoted 2 times

Parvezg 3 years, 10 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 4 years ago
B. add contoso.com as a UPN suffix
upvoted 2 times

ExamTopic 4 years, 7 months ago

https://docs.microsoft.com/en-us/office365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization

upvoted 5 times

Question #39 *Topic 3*

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"}
```

Suggested 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 3 years, 7 months ago
incorrect syntax - should be Set-AzureADUserLicense -AssignedLicenses "
upvoted 5 times

F_M 3 years, 6 months ago
And Get-ADUser -All -Filter "Department eq 'Temp'"
upvoted 1 times

chaoscreater 3 years, 6 months ago
That's for onprem, not AAD
upvoted 1 times

F_M 3 years, 6 months ago
Sorry, Get-AzureADUser -All -Filter "Department eq 'Temp'"
upvoted 1 times

emanresu Highly Voted 2 years, 8 months 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 5 times

Wojer Most Recent 3 years 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 3 years, 2 months ago
B is right if Get-MsolUser and Set-MsolUserLicense have been used.
upvoted 2 times

lafcow 3 years, 4 months 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 3 years, 4 months ago
Actually there are no correct answers listed... "TimurKazan: should be B, but instead of ""-addlicenses" there must be "-assignedlicenses""
upvoted 1 times

TimurKazan 3 years, 4 months ago
should be B, but instead of ""-addlicenses" there must be "-assignedlicenses"
upvoted 4 times

melatocaroca 3 years, 6 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 3 years, 7 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.

Suggested 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

Amir1909 11 months ago
E is correct
upvoted 1 times

Wojer 3 years 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 3 years, 1 month ago
In exam today
upvoted 2 times

junior6995 3 years, 3 months 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 and outbound.
upvoted 2 times

Eggsamine 3 years, 2 months 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 2 years, 6 months 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 when AD Connect reaches out to Azure to gets an update.

upvoted 2 times

maikelb 3 years, 7 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

Suggested 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 4 years, 7 months ago
Smartcard is the key word.
upvoted 22 times

[Removed] Highly Voted 4 years, 5 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 17 times

Solo96 Most Recent 1 year, 8 months ago
A is more valid now. Password hash and seamless SSO supports Smart cards:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#comparing-methods
upvoted 1 times

NHaikes 2 years, 5 months 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 3 years, 6 months ago
Update the reference link:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 1 times

mkoprivnj 4 years ago

B for sure! ctfalci

upvoted 3 times

HLBJani 4 years, 7 months ago

Right link:

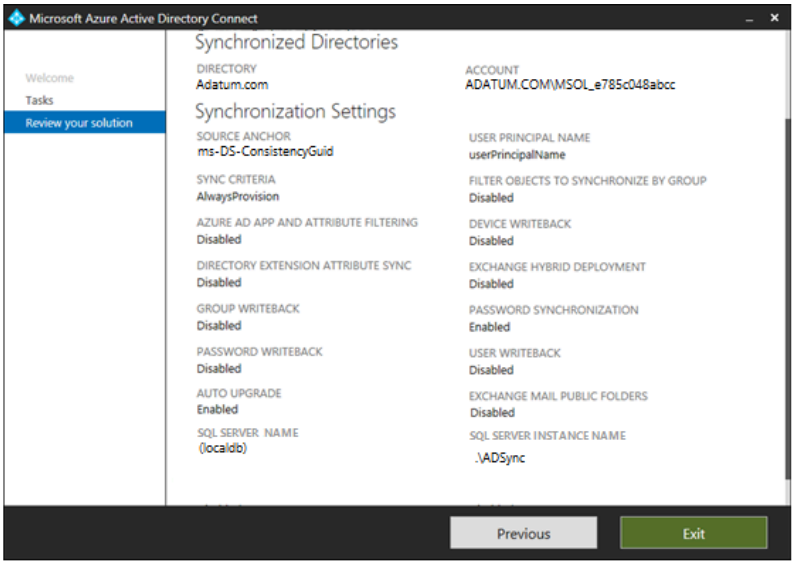
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 4 times

Question #42 *Topic 3*

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.	○	○

Suggested 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 3 years, 2 months 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 12 times

One111 1 year, 3 months ago

Yes - you can reset password,but it will be overide next synchronization by AADC.

No - only AADC for synced accounts.

Yes - usage location can be set both ADDS and AAD.

upvoted 1 times

Amir1909 Most Recent 11 months ago

Yes

Yes

Yes

upvoted 1 times

gills 1 year, 10 months ago

It depends on if you can or you should.

So being an IT system for operations, the answers should be if we should. We can change the password but it will be over written in the next sync.

So answer is NNY

upvoted 2 times

n0t_a_good_t1m3 2 years, 1 month ago

On exam as of three days ago

upvoted 4 times

ARYMBS 2 years, 8 months ago

YNY

Yes you can reset password on AAD but it will never sync - disabled password writeback.

upvoted 1 times

Karvon 2 years, 7 months ago

Not right. It displays that the setting is handled by your on premise. N N Y

upvoted 5 times

raugustine 2 years, 1 month ago

Incorrect, the provided answer is Correct.

N

N

Y

upvoted 2 times

Wojer 3 years 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 2 times

joergsi 2 years, 11 months ago

The question is not saying, but the image does!

upvoted 3 times

JakeH 3 years, 1 month ago

In exam today

upvoted 2 times

zacmzee 3 years, 3 months 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 4 times

emilianogalati 3 years, 3 months 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 then 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 3 times

Comp_technician 3 years, 7 months ago
NO - YES - NO
upvoted 1 times

melatocaroca 3 years, 6 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 will overwrite the Azure AD change,
upvoted 7 times

subbuhotmail 3 years, 4 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 2 times

gkp_br 3 years, 7 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 3 years, 6 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 3 years, 6 months ago
Sorry, but you are wrong. Test this and see it.
upvoted 1 times

Turak64 3 years, 4 months 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 3 years, 6 months ago
How about you read your own comment below, which proved my point?
upvoted 3 times

gkp_br 3 years, 7 months ago
bu the password will not be sync with on-premises Active Directory.
upvoted 2 times

wonap 3 years, 8 months ago
In my opinion
1 Yes (writeback enabled)
2 No
3 Yes
upvoted 1 times

sadsadweqr23424dsdqweqwe 3 years, 8 months ago
Password writeback disabled
upvoted 16 times

One111 2 years ago
You can reset password on Azure for synced identities (no matter what sufix is being used), but it t won't be synchronized back to onprem AD (until password writeback is enabled) and will be overwrite in next sync cycle.
upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).

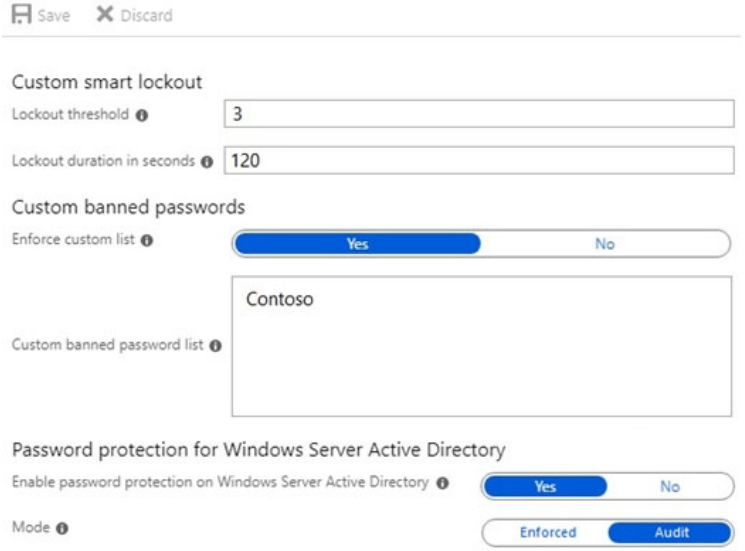
You have users in contoso.com as shown in the following table.

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.	○	○

Suggested Answer:

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.	○	○

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 3 years, 8 months ago
The policy is in Audit mode. So it isn't enforced. Passwords can be whatever they want.
upvoted 11 times

Scooter454 3 years, 8 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 14 times

charat 2 years, 7 months 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

ColmTheMeanie Most Recent 1 year, 10 months ago
This has irritated me so i worked it out.
1, N - there's straightforward if you know these policies.
2, Y - Here's why below
Each banned password that's found in a user's password is given one point.
Each remaining character that is not part of a banned password is given one point.
A password must be at least five (5) points to be accepted.
C0nt0s0 normalised to contoso = 1
Complex - C=0 O=0 M=1 P=1 L=1 E=1 X=1 1=1 2=1 3=1 so it's a score of 9 so it's OK
3, Y - You can see without going too much into it 1=1 2=1 3=1 that's 3 already then 1 point for contoso that's 4 and the "MyPassword" it's a point for every letter not in contso

Pretty sure that's right. Audit still applies if it's including and on prem AD
upvoted 1 times

ColmTheMeanie 1 year, 10 months ago
and the reference https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#how-are-passwords-evaluated
upvoted 1 times

TechMinerUK 2 years, 6 months 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 they 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 3 times

[Removed] 2 years, 8 months 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 source. 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 password list.

URL talks, when user Change ou Reset password, if it already set User1 don't need to change their password

upvoted 1 times

[Removed] 2 years, 8 months 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 2 years, 9 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 to a 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 4 times

Ltgoldman 2 years, 3 months 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 3 years, 1 month 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-mode

upvoted 1 times

AGill 3 years 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 only takes effect at a password change or set operation - not sign in.

upvoted 2 times

JakeH 3 years, 1 month ago

In exam today

upvoted 2 times

[Removed] 3 years, 3 months 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 will only be logged.

upvoted 3 times

Davidchercm 3 years, 4 months 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 3 years, 9 months ago

So, What is the question? lol

upvoted 1 times

Scooter454 3 years, 8 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

Question #44 *Topic 3*

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.	○	○

Suggested 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 3 years, 8 months ago

Group owner = Reviewer. User 3 is not a group owner, and therefor, not a reviewer.

upvoted 12 times

Moderator Most Recent 2 years, 5 months ago

Still a valid question (July 30th 2022).

upvoted 4 times

Ash473 3 years, 4 months ago

in exam today

upvoted 2 times

Question #45 *Topic 3*

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:

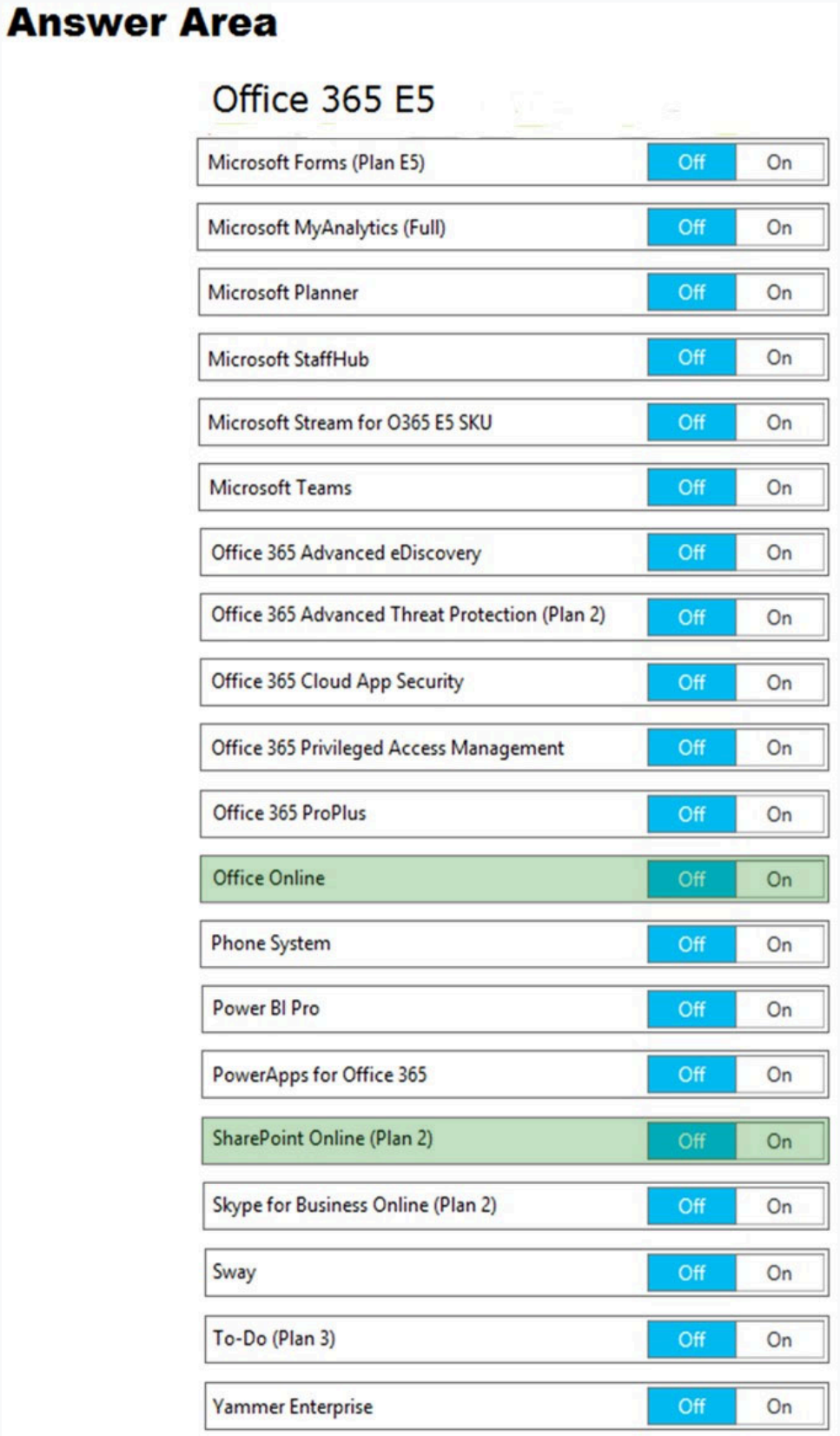
Answer Area

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

Suggested Answer:

Answer Area



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 3 years, 8 months ago

It's actually "Office for the web" not "Office online"

upvoted 20 times

MDol Highly Voted 2 years, 11 months ago

Answers are correct. You need the have a storage location for the documents, otherwise you can't create a new document.

upvoted 5 times

hufflepuff Most Recent 2 years, 2 months ago

Tested adding Office for Web - "To Assign a license that contains 'Office for the Web', you must also assign one of the following service plans: SharePoint (Plan1)". I assume SharePoint (Plan 2) would therefore also apply.

Answer: "Office for Web" (previously Office Online?) & "SharePoint (Plan 2)"

upvoted 2 times

Stiobhan 2 years, 7 months 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 5 times

TashaGirl 2 years, 11 months 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

Wojer 3 years 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 3 years, 1 month ago

why is share point needed

upvoted 2 times

JEricThomas610 3 years ago

According to the explanation, you need a place to store the documents online. Kind of a tricky question.

upvoted 5 times

Question #46 *Topic 3*

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

Suggested 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

Community vote distribution
A (100%)

lucidgreen Highly Voted 3 years, 8 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 26 times

lucidgreen 3 years, 8 months ago
And by standby, I mean staging mode.
upvoted 25 times

Cheekypoo Most Recent 2 years, 5 months ago
Was in my exam today 05/08/22.
upvoted 4 times

Sh1rub10 2 years, 7 months 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.

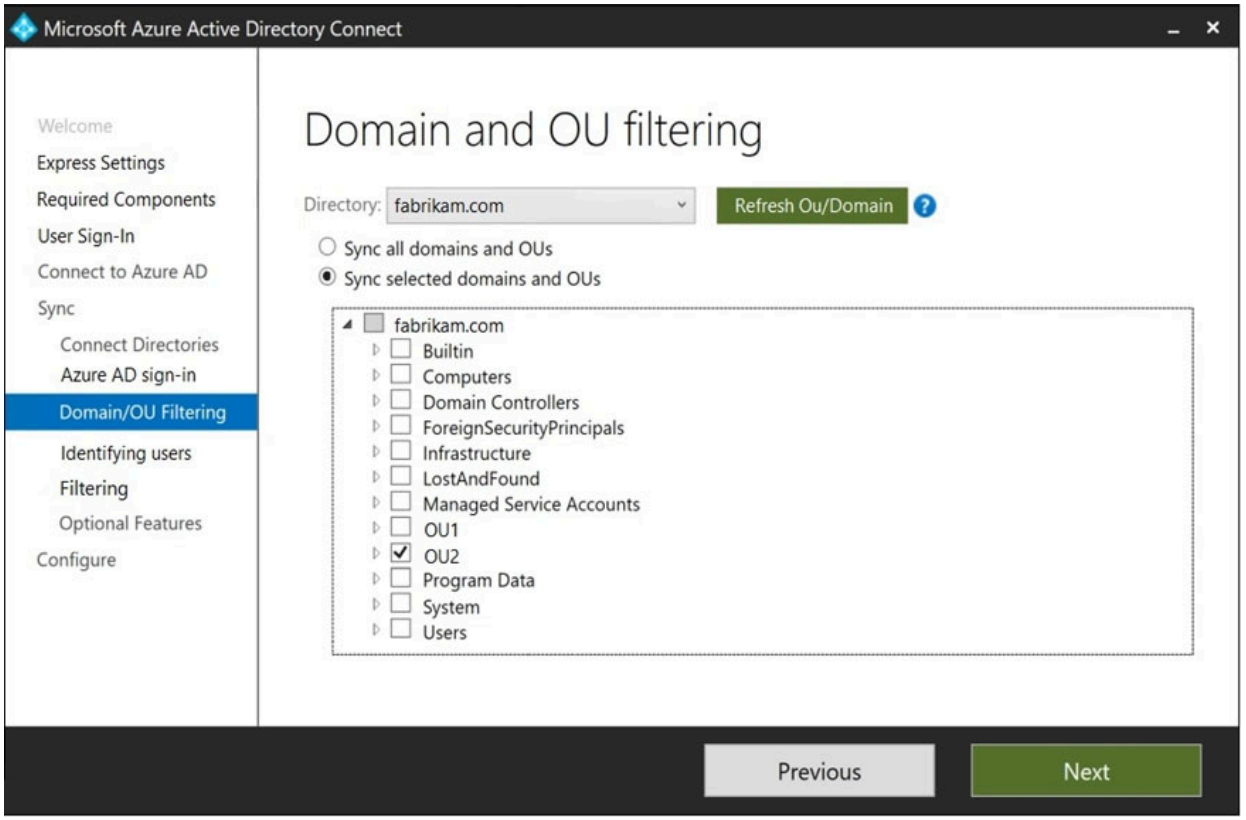
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group – Global	OU1
User3	User	OU2
Group2	Security Group – Global	OU2

The groups have the members shown in the following table.

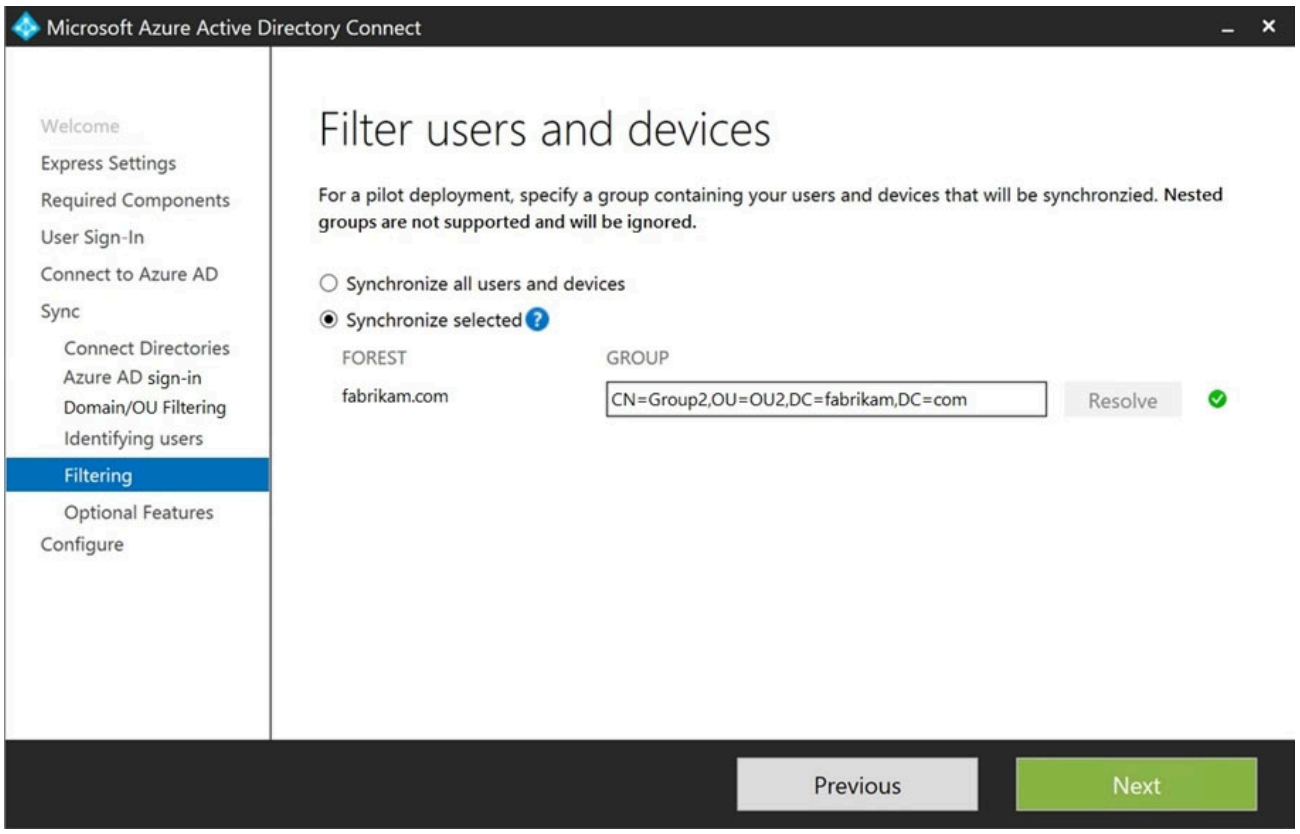
Group	Members
Group1	User1
Group2	User2, User3, Group1

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.	○	○

Suggested 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 3 years, 7 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 11 times

RenegadeOrange 2 years, 5 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 2 times

Nilz76 Highly Voted 2 years, 9 months ago
This question was in my exam on 06/April/2022. I passed.
upvoted 6 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

Cheekypoo 2 years, 5 months ago
Was in my exam today 05/08/22.
upvoted 2 times

fofo1960 3 years 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 3 years ago
i thought that security groups are not syncronized...
upvoted 1 times

PDR 3 years 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 14 times

Jeff8989 2 years, 11 months ago
Thanks!
upvoted 1 times

Pietras123 2 years, 1 month ago
Actually it is no longer valid. Now also security and distribution synchronize
upvoted 3 times

JakeH 3 years, 1 month ago
In exam today
upvoted 1 times

gonick 3 years, 3 months ago
In exam last week
upvoted 3 times

Question #48 *Topic 3*

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

Suggested 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 3 years, 4 months 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 16 times

manis73 Highly Voted 2 years, 6 months ago
Terrible question
upvoted 9 times

Jo696 Most Recent 2 years, 6 months 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 3 times

JakeH 3 years, 1 month ago
In exam today
upvoted 3 times

emolnes85 3 years, 5 months ago
Trick question
upvoted 5 times

Question #49 *Topic 3*

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.

Suggested 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/

Community vote distribution
A (100%)

AlfredHK Highly Voted 4 years, 9 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 27 times

[Removed] Highly Voted 4 years, 5 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

[Removed] 4 years, 5 months ago
Answer A
upvoted 7 times

donathon 4 years, 3 months ago
The user writeback preview feature was removed in the August 2015 update to Azure AD Connect. If you have enabled it, then you should disable this feature. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-preview

upvoted 2 times

Amir1909 Most Recent 11 months ago

A is correct

upvoted 1 times

Cebsiej_28 2 years, 4 months 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 3 times

Cheekypoo 2 years, 5 months ago

Was in my exam today 05/08/22.

upvoted 1 times

Rudelke 2 years, 5 months 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 using Azure PS module on domain controller.

upvoted 2 times

TechMinerUK 2 years, 6 months 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 are "Get-AzureADUser and Set-AzureADUser cmdlets" which will not work for administrating an on-prem AD

upvoted 1 times

charat 2 years, 7 months ago

On Exam 05/22/22. Great qustion.

upvoted 2 times

jill44 2 years, 11 months ago

A&D both are correct, but for 100 users I go with D.

upvoted 1 times

Ibraheem 2 years, 8 months 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 right command would have been GetADuser for on-premises.

upvoted 2 times

tf444 3 years ago

A&C both are correct, however, for 100 users, C is more reasonable!

upvoted 1 times

JakeH 3 years, 1 month ago

In exam today

upvoted 3 times

lucidgreen 3 years, 9 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 9 times

Razuli 3 years, 8 months ago

always appreciate your comments lucidgreen

upvoted 3 times

lucidgreen 3 years, 10 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 best 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 3 times

mkoprivnj 4 years ago

A for sure!

upvoted 5 times

mikerss 4 years, 7 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 4 years, 7 months ago

Not D. unless it says Get-ADuser and Set-ADuser rather than Get-AzureADUser & Set-AzureADuser. You need to modify on-premises AD accounts!

upvoted 10 times

Jokke71 4 years, 9 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.

Suggested 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

Community vote distribution
D (100%)

jkklim Highly Voted 3 years 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 6 times

Amir1909 Most Recent 11 months ago
D is correct
upvoted 1 times

Davidchercm 2 years, 11 months ago
Selected Answer: D
D is correct
upvoted 3 times

JakeH 3 years, 1 month ago
In exam today
upvoted 2 times

densyo 3 years, 6 months ago
https://answers.microsoft.com/en-us/msoffice/forum/msoffice_o365admin-mso_dirservices/directory-synchronization-part-2-using-idfix-to/6f09c9d7-8b6e-4d6b-aa0c-630dd2904460
upvoted 3 times

adaniel89 3 years, 7 months ago
You need to ensure the UPN of the users AD accounts are correct. i.e not .local UPN.
upvoted 1 times

chaoscreater 3 years, 6 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. Sync issues are 99% related to attributes.
upvoted 12 times

PDR 3 years 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 but 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 ـ€"DomainName contoso.com ـ€"SupportMultipleDomain command.

B. From Windows PowerShell, run the New-MsolFederatedDomain ـ€"SupportMultipleDomain -DomainName contoso.com command.

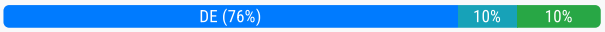
C. From Windows PowerShell, run the New-MsolFederatedDomain -DomainName adatum.com command.

D. From Windows PowerShell, run the Update-MSOLFederatedDomain ـ€"DomainName contoso.com ـ€"SupportMultipleDomain command.

E. From the federation server, remove the Microsoft Office 365 relying party trust.

Suggested Answer: *AE*
When the Convert-MsolDomaintoFederated ـ€"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 ـ€"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.

Community vote distribution



lucidgreen Highly Voted 3 years, 8 months ago
Convert-MsolDomaintoFederated is for changing the configuration to federated. Update-MsolDomaintoFederated is for making changes.
I'm going say D and E.
upvoted 26 times

michszym 3 years, 6 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 3 years, 6 months ago
D and E
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365
upvoted 7 times

papaaj Most Recent 1 year, 7 months ago
Option D is the correct answer
upvoted 1 times

Blagojche 1 year, 8 months ago
The correct actions to perform before running the Azure AD Connect wizard to configure the adatum.com Active Directory domain for federated authentication are:

C. From Windows PowerShell, run the New-MsolFederatedDomain -DomainName adatum.com command.
E. From the federation server, remove the Microsoft Office 365 relying party trust.

Explanation:

Option A is incorrect because it references the contoso.com domain, not the adatum.com domain that needs to be configured.

Option B is incorrect because it creates a new federated domain for the contoso.com domain, not the adatum.com domain that needs to be configured.

Option C is correct because it creates a new federated domain for the adatum.com domain, which is necessary for federated authentication.

Option D is incorrect because it references the contoso.com domain, not the adatum.com domain that needs to be configured.

Option E is correct because the Microsoft Office 365 relying party trust needs to be removed from the federation server before configuring the adatum.com domain for federated authentication.

Therefore, the correct answers are C and E.
upvoted 1 times

trexar 2 years, 9 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 years, 5 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 3 times

Paolo2022 2 years, 1 month ago

This link says it all - D&E, thanks RenegadeOrange!

What you're looking for to answer the question is described in this section: https://learn.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 1 times

trexar 2 years, 9 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 3 times

RazielLycas 2 years, 10 months 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 have to remove the Office365 object from ADFS
upvoted 4 times

[Removed] 2 years, 11 months ago

Selected Answer: DE

similar question in Measureup.com , D& E were the answer

upvoted 2 times

joergsi 2 years, 11 months ago

Selected Answer: BD

For me

1. = D

2. = B

upvoted 1 times

joergsi 2 years, 11 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 2 years, 11 months 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 2 years, 11 months 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 2 years, 11 months 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 3 times

fofo1960 2 years, 11 months ago

Selected Answer: DE

Agree with Lucidgreen

upvoted 3 times

FumerLaMoquette 2 years, 12 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 3 years, 3 months 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 5 times

Linux09 3 years, 3 months 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 3 years, 3 months 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 3 years, 4 months ago
I think D E
upvoted 1 times

Question #52 *Topic 3*

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

Suggested 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 3 years, 6 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 least privilege
Owner SharePoint related
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
upvoted 9 times

Question #53 *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 -
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.

Suggested 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

Mahammad 1 year, 9 months ago
Service Support Administrator is correct. Check this link:
https://learn.microsoft.com/en-US/azure/active-directory/roles/permissions-reference#service-support-administrator
upvoted 1 times

DeLoc 1 year, 10 months ago
The Service Support Admin role in Microsoft 365 only allows users to view the service health dashboard and the Microsoft 365 message center. It does not provide the ability to create Microsoft support requests. To create support requests, users need to be assigned the Global Administrator, Billing Administrator, or Service Administrator roles. In this case the service administrator role.
upvoted 1 times

Question #55 *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 -
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.

Suggested 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'.

One111 Highly Voted 2 years ago
Microsoft for enterprise apps (formally Office online) subscription is required to use Word Online.
To save for also SharePoint Online P1 or P2 is required.
MyApps dashboard is available to everyone in organization.
upvoted 5 times

Question #56 *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 -
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.

Suggested 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.

Kees1990 1 year, 11 months ago
you can do this from AAD too.
Find user, remove checkmark "account enabled" click save
upvoted 1 times

iptbee 2 years ago
1- admin.microsoft.com
2- Active users
3- select the user
4- “Block sign-in”
Blocking doesn't stop the account from receiving email and it doesn't delete any data.
upvoted 1 times

Question #57 *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 -
You need to create a group named Group2. Users who are added to Group2 must be licensed automatically for Microsoft Offline 365.

Suggested 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

Hanan1234 1 year, 11 months ago
step 6 can be ignored
upvoted 2 times

sehlohomoletsane 1 year, 8 months ago
what kind of license should i select if i may ask?
upvoted 1 times

Question #58 *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 -
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.

Suggested 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

Paolo2022 2 years, 1 month ago
I wonder what constraints the requirement would entail: "The solution must minimize the number of licenses assigned to users."

Anyone with an idea about this? For now the answer provided (BIlling Administrator) seems straightforward to me.
upvoted 1 times

Kees1990 1 year, 11 months ago
yes. billing adm. is correct. no license (E3 or E5 or whatever) required for the user to do this task.
upvoted 1 times

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.

Suggested 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

BigDazza_111 1 year, 7 months ago
Helpdesk administrator also. Cannot change GA password
upvoted 1 times

st2023 1 year, 10 months ago
The question does not specify "least privilege" and only mentions global admin.
if the question identifies "user", as (no admin role) users then "Password admin" is the answer.
User Admin could be an option here.
However, the question is not clear enough therefore, we can assume it is asking for least privilege.
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords
upvoted 1 times

Question #61 *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 -
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.

Suggested 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.

BigDazza_111 1 year, 7 months ago
correct. no longer 'permissions' blade. It under Roles --> admin roles etc
upvoted 1 times

ago_inline 1 year, 11 months ago
There is where I found these settings: Exchange Admin Center>Roles>Admin Roles>Add role group>Give it a name>search for the roles to add: "Mailbox Import Export" and "Mail Recipients" and check each one > add members > click "add role group" button
upvoted 2 times

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

Suggested 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 Highly Voted 2 years, 5 months ago

Was in my exam today 05/08/22.

upvoted 5 times

Amir1909 Most Recent 11 months ago

Correct

upvoted 1 times

BigDazza_111 1 year, 7 months ago

box 1- answer 1 and 3. Box 2 is correct - this description from azure user admin role - microsoft.directory/users/manager/update

Update manager for users

upvoted 1 times

Blagojche 1 year, 8 months ago

Apology, by mistake I posted my answer here for

Question 3, Topic 8

Admin 1 and Admin 3 Only

Service Health

upvoted 1 times

Blagojche 1 year, 8 months ago

This is very weird that all comments are not tested:

You can view Microsoft 365 incidents in the Microsoft 365 admin center. Here's how:

Sign in to the Microsoft 365 admin center using your admin credentials.

In the left navigation pane, click on the Health tab.

Under the Service health section, you can view the current status of your services, incidents, advisories, and planned maintenance events.

To view more details about an incident, click on the incident and you will be taken to the Service health page for that specific incident.

The "Security Reader" and "Security Administrator" roles can view the "Incidents" section in the Microsoft 365 admin center. From the provided roles A and C

upvoted 1 times

Moderator 2 years, 6 months ago

Correct answers given.

upvoted 3 times

itmaster 2 years, 8 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 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%20Admi

upvoted 1 times

itmaster 2 years, 8 months ago

sorry this comment is for Q62 not for this Question

upvoted 1 times

trexar 2 years, 8 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 2 years, 8 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 3 years, 1 month ago

In exam today

upvoted 4 times

M19 3 years, 3 months 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 2 times

Ash473 3 years, 4 months ago

IN exam today

upvoted 1 times

itstudy369 3 years, 6 months ago

Password Administrator CAN'T modify user attribute fields

upvoted 1 times

itstudy369 3 years, 6 months ago

Reset password only user1

upvoted 1 times

itstudy369 3 years, 6 months ago

Sorry, reset password user 1 and 3.

upvoted 4 times

melatocaroca 3 years, 7 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 4 times

melatocaroca 3 years, 6 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 all 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 users.

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

upvoted 7 times

Question #63 *Topic 3*

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.

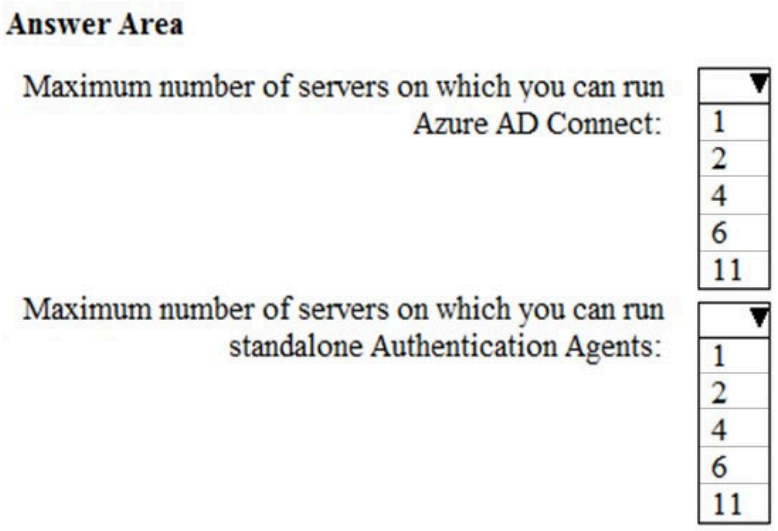
You are evaluating the implementation of pass-through authentication and seamless SSO. Azure AD Connect will NOT be in staging mode.

You need to identify the redundancy limits for the planned implementation.

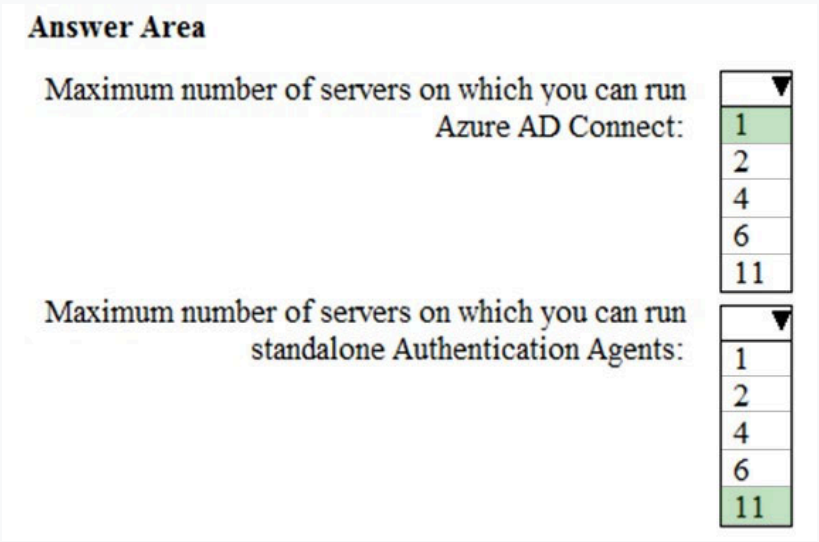
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested 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 5 years, 1 month 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 16 times

lucidgreen 3 years, 8 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 4 times

Turak64 3 years, 3 months ago
Is an Auth Agent an Azure Connect server?
upvoted 1 times

Goofer Highly Voted 4 years, 11 months ago
One Azure AD Connect server.
Max 40 PTA servers
upvoted 12 times

Mr01z0 3 years, 7 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 your tenant. There is a system limit of 40 Authentication Agents per tenant."
upvoted 1 times

melatocaroca Most Recent 3 years, 6 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 3 years, 7 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 3 years, 3 months 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 5 times

mkoprivnj 4 years ago
1 & 11 is correct. Only one AAD connect per server if staging not configured!
upvoted 3 times

[Removed] 4 years, 5 months ago
double question again
upvoted 2 times

Alvaroll 4 years, 3 months ago
2-9 https://www.examtopics.com/exams/microsoft/ms-100/view/11/
upvoted 2 times

Question #64 *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: 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

Suggested Answer: *B*

Kipperson Highly Voted 3 years, 7 months ago

B - You would also need to add the custom doing in the 365 Portal

upvoted 8 times

Jo696 Most Recent 2 years, 6 months 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 2 times

Question #65 *Topic 3*

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

Suggested 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 3 years, 9 months ago

It is possible to create a guest user without a User Administrator.
Therefore, guest creation is possible for all users.
upvoted 9 times

adaniel89 3 years, 8 months ago
correct!

All users can create guest user accounts, so should be User 1,2.3 &4
upvoted 7 times

melatocaroca 3 years, 6 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 6 times

J0J0 3 years, 6 months ago
But technically, once invite has been accepted it will create a guest user account. so by inviting, you can create guest account and that is considering the default settings.
upvoted 4 times

allesglar 3 years, 1 month ago
exactly and this is why it is wrong. You cannot "create" the guest user to your preference, just replicate the default behavior.
The answer is imo correct.
upvoted 6 times

alex_p 2 years, 9 months ago
Please, explain how can you create Guest Users without inviting them?
upvoted 3 times

marckinez 3 years, 5 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 3 years, 5 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 in AzureAD, inviting just sends the create request to the AzureAD internal authority, which creates the guest user for you. the effect is the same, but the means are quite different.
upvoted 5 times

mitsios96 3 years, 3 months ago
Invite is different than create
upvoted 7 times

Paolo2022 2 years, 1 month ago
No, it is not.
See: https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal#add-a-new-guest-user-in-azure-ad

Still, not all users can invite externals. See the same article:
https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal#prerequisites
upvoted 1 times

vicentsp84 Highly Voted 3 years, 7 months ago
1,2,3 & 4, https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide default settings
upvoted 7 times

Chetithy Most Recent 2 years, 3 months ago
I'm not sure how noone has referenced this: https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-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 3 times

Claire91 2 years, 5 months 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 2 years, 6 months ago
Correct answers given.
upvoted 3 times

itmaster 2 years, 8 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
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%20Admi
upvoted 2 times

Ogabs 2 years, 10 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 2 years, 11 months 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 3 times

Moderator 2 years, 5 months ago
Correct, great link.
upvoted 1 times

tf444 3 years 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 3 years 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 3 years 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 3 years, 1 month ago
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

upvoted 1 times

Jcbrow27 3 years, 1 month 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 3 years, 1 month 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 3 years, 3 months 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 creating a guest user?

upvoted 2 times

Chipper 3 years, 3 months 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 User 2 so I agree with the answer that it is User 2 for both drop downs.

upvoted 1 times

TimurKazan 3 years, 4 months 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 3 years, 1 month ago

incorrect

upvoted 1 times

lengySK 3 years, 4 months ago

If they mean "invite" same as create guest user then anyone in the organization can create guest account. https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide

upvoted 1 times

Question #66 *Topic 3*

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.

Suggested 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

Community vote distribution
A (100%)

james1 Highly Voted 3 years, 10 months ago
Yep A for sure
upvoted 10 times

Startkabels Most Recent 2 years, 1 month ago
Selected Answer: A
Nobrainer A
upvoted 1 times

SkullRage 2 years, 2 months ago
This is the correct link: https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection
upvoted 1 times

trexar 2 years, 9 months ago
Selected Answer: A
Yes. A
upvoted 1 times

joergsi 2 years, 11 months ago
Answer (A):
AZURE AD => Security => Authentication Methods | Policies => Password Protection => Custom banned password list
upvoted 3 times

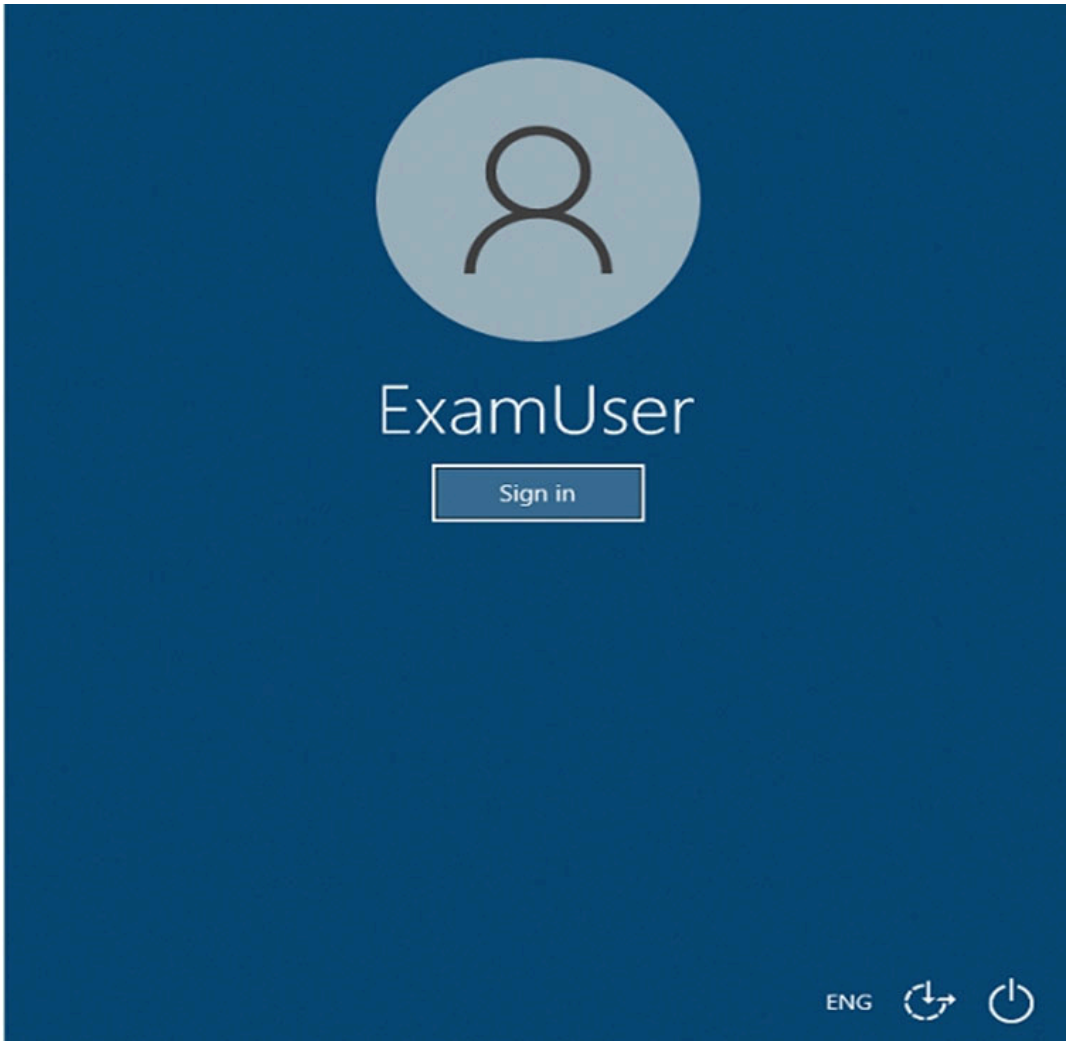
DaBummer 3 years, 3 months ago
it is A!
upvoted 2 times

Ahema 3 years, 4 months 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.

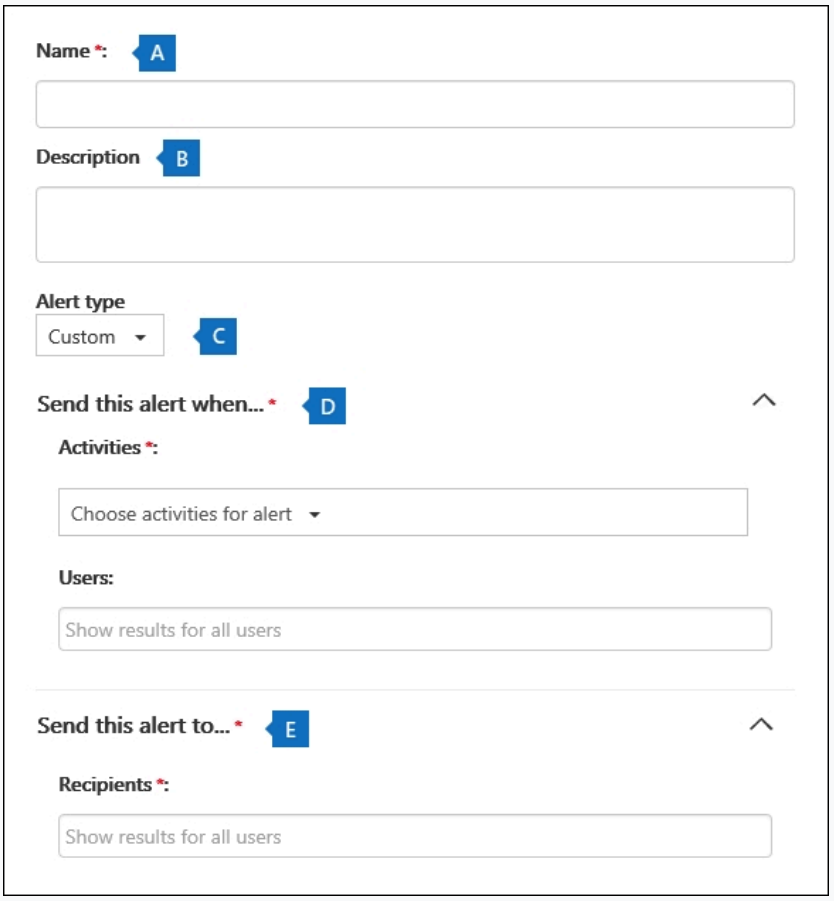
Lab information -
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@admin.onmicrosoft.com
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.

Suggested 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

gills 1 year, 10 months ago
This is now in the Purview portal.
https://compliance.microsoft.com/alertpoliciesv2?
upvoted 1 times

Startkabels 2 years, 1 month ago
Compliance Center > Alerts > New alert policy
upvoted 3 times

Paolo2022 2 years ago
Yes, it can be done from the Compliance admin center, too:
Policies > Alerts > New Alert Policy > (Category doesn't matter) > "Granted mailbox permission".
upvoted 6 times

Downstar 2 years, 1 month ago
This tutorial is outdated. Protection.office.com isn't in use anymore.

Just go to compliance.microsoft.com
Policies > Alert > Alert Poicies > + New alert Policy > fill in name etc. Choose for activity is "Granted mailbox permission" and user: User is xxx an setup the email of who to alert
upvoted 4 times

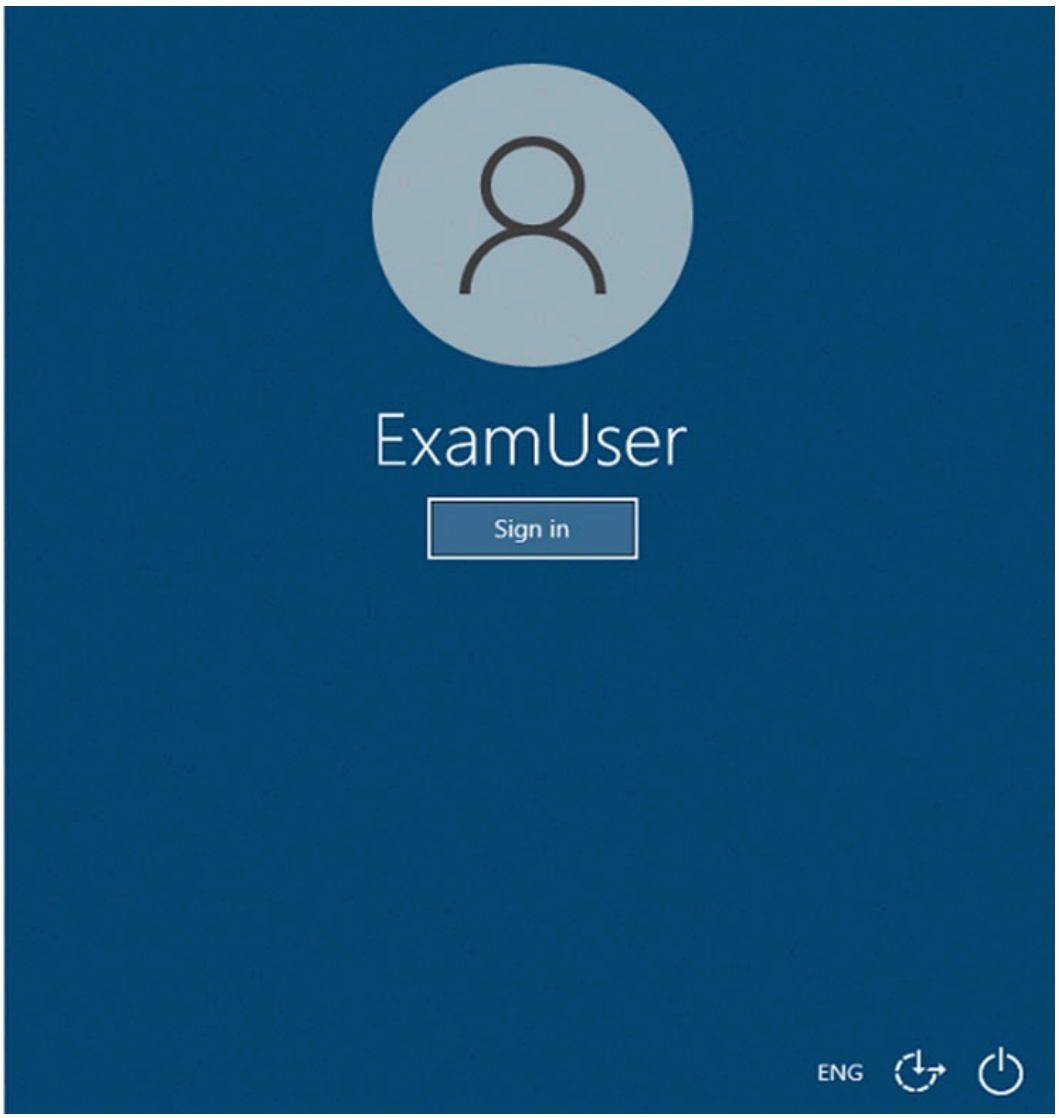
hufflepuff 2 years, 2 months ago
Security Admin Center -> Policies & Rules -> Alert policy -> New Alert Policy.
upvoted 4 times

Paolo2022 2 years, 1 month ago
Yes, thanks for testing!
To be very, very precise this is where you have to be:
Security Admin Center -> Email & Collaboration -> Policies & Rules -> Alert policy -> New Alert Policy -> (Category doesn't matter) -> "Granted mailbox permission".
upvoted 3 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 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.

Suggested 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 ɹ€Set user passwords to expire after a number of daysɹ€ is ticked.
6. Enter 180 in the ɹ€Days before passwords expireɹ€ field.
7. Click the 'Save changes' button.

StudyBM Highly Voted 2 years, 2 months ago

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 Org settings option.
3. Click on Security and Privacy.
4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled ɹ€Set user passwords to expire after a number of daysɹ€ is ticked.
6. Enter 180 in the ɹ€Days before passwords expireɹ€ field.
7. Click the 'Save changes' button.

upvoted 6 times

Downstar Most Recent 2 years, 1 month ago

This is correct

upvoted 1 times

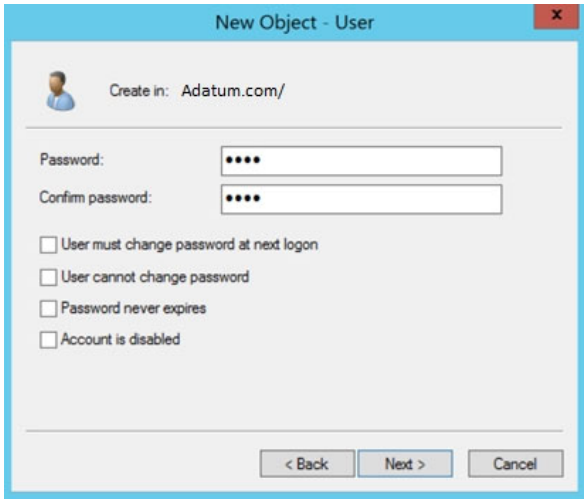
Question #69 *Topic 3*

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.	○	○

Suggested 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

TheWallPTA Highly Voted 3 years, 9 months ago
Should this not be YNN?
On-prem Password policy should apply...
upvoted 29 times

BoxGhost 2 years, 8 months ago
I think cloud password expiration for a synced account would be ignored unless you enable a specific feature. So I would be inclined to 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 5 times

adaniel89 Highly Voted 3 years, 7 months ago
There is no second exhibit! How can you guys answer this question ?
upvoted 28 times

Bobalo 3 years, 5 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, that already tells you a lot about the possible answers.
upvoted 1 times

Amir1909 Most Recent 11 months ago
- Yes
- No
- No
upvoted 1 times

Meebler 1 year, 9 months ago
If password writeback is disabled, the password policies in Azure AD and on-premises Active Directory will be enforced independently.

By default, the Azure AD password policy requires users to change their passwords every 90 days. However, if you have a hybrid environment and are synchronizing passwords from on-premises Active Directory to Azure AD, the on-premises password policy will apply to your users. In this case, the password expiration period will be determined by your on-premises Active Directory policy settings, not by Azure AD.

If you want to enforce a consistent password expiration policy for both on-premises and cloud users, you should configure the password policies in both environments to have the same settings.
upvoted 1 times

Everlastday 1 year, 12 months ago
On Exam 03.01.2023
upvoted 4 times

Moderator 2 years, 4 months ago
Valid question (30th July 2022).
upvoted 3 times

Moderator 2 years, 5 months ago
Still a valid question (July 30th 2022).
upvoted 1 times

Contactfornitish 2 years, 5 months 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 2 years, 6 months 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) the 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 2 years, 8 months ago

1.y
2.n
3.n Express installation just perform PHS it means just send the hash.

upvoted 1 times

KSvh53 2 years, 10 months ago

Where is the 2nd photo? I believe it is missing, which is very important for understanding the question....

upvoted 1 times

Durden871 2 years, 10 months 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, passwords 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 2 years, 10 months 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 is set to 90 days in AzureAD, the policy doesn't apply to accounts synchronized from AD DS unless the enforced cloud password policy is applied.

Really hate this question.

upvoted 2 times

Durden871 2 years, 10 months 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 AD 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 policy 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 for exhibit 2, who knows?
upvoted 3 times

Storm 2 years, 12 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 3 times

jkklim 3 years 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 3 years, 4 months 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 3 years, 4 months ago
YNY.

Password is by default set on 90 days before expiration and with a reminder 14 days before.
upvoted 2 times

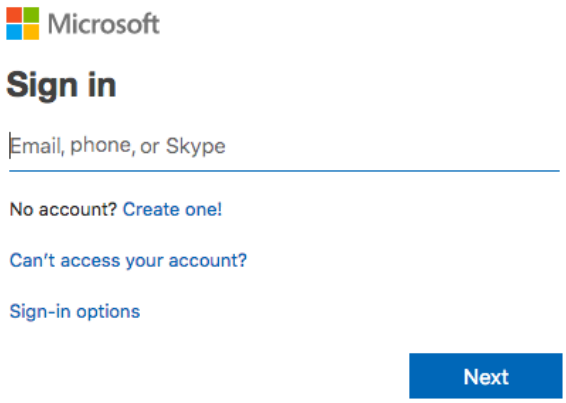
emilianogalati 3 years, 3 months ago
Also YNN if you consider writeback is disabled.
upvoted 2 times

AZalan 3 years, 5 months ago
Y,N,N.
There is no password Writeback & by default Password expiration policy is disabled on MS365 admin center. Microsoft recommendation is to have strong password with no expiration policy.
upvoted 3 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.

Suggested 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.

Hanan1234 1 year, 10 months ago

To ensure that you can grant permissions to the Managers group, the group needs to be a Security Group.

upvoted 1 times

hubran 1 year, 11 months ago

This is not about roles assignment, it is only about permissions. So a regular security group

upvoted 1 times

DogusB 2 years, 2 months ago

The question states "The solution must ensure that you can grant permissions to Managers." I would use the Azure Active Directory admin center and then ensure the 'Azure D roles can be assigned to the group' is enabled when creating the group.

upvoted 4 times

Paolo2022 2 years ago

This is also possible from the MS 365 admin center. During group creation there is a step called "Settings", in which you can check a box called "Allow admin roles to be assigned to this group". That obviously does the trick as well.

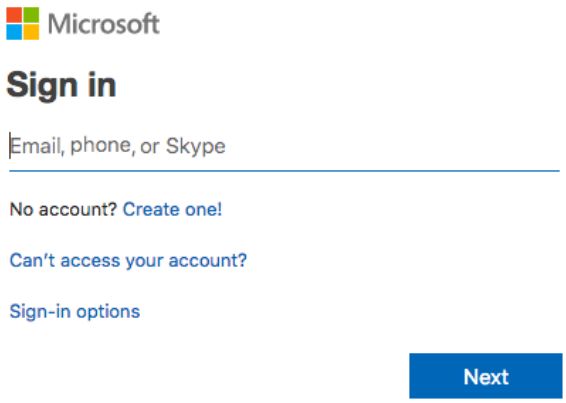
upvoted 2 times

Question #71 *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 -



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.

Suggested 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.

SkullRage Highly Voted 2 years, 1 month ago

1. Go to https://compliance.microsoft.com or Go to https://admin.microsoft.com
2. In the left navigation pane, select Compliance.
3. In the left navigation pane, select Communication Compliance.
4. Click the '+Create policy' -> 'Custom Policy' button to create a new policy.
5. Give the policy a name such as 'Joni Sherman' and click Next.
6. In the 'Users and reviewers' section, at 'Supervised Users and Groups' select Joni Sherman from the users list
7. At Reviewers select Lee Gu from the users list and click Next.
8. Deselect the 'Teams', 'Skype for Business Conversations' and 'Yammer' checkboxes leaving only the 'Exchange' checkbox ticked and click Next.
9. Under 'Communication Direction', deselect Inbound & Internal leaving only Outbound selected
10. In the 'Review Percentage' section, enter 50 and click Next.
11. Click Next.
13. On the 'Review your settings' page, check the settings are correct the click the Finish button to create the policy.

upvoted 21 times

Oval61251 2 years, 1 month ago

THANK YOU!!

upvoted 3 times

fessebook Most Recent 1 year, 8 months ago

Office 365 E3 is needed to create a communication compliance policy.

upvoted 1 times

[Removed] 2 years ago

It seems to be in communication compliance under Purview now.

upvoted 3 times

yawb 2 years ago

This can now be located in Microsoft Purview Portal (direct link: https://compliance.microsoft.com/supervisoryreview?viewid=Policies)
Create a custom policy

upvoted 1 times

Oval61251 2 years, 1 month ago

This seems to have changed where can it be found now?

upvoted 1 times

renrenren 2 years, 2 months ago

Now as known as Communication compliance

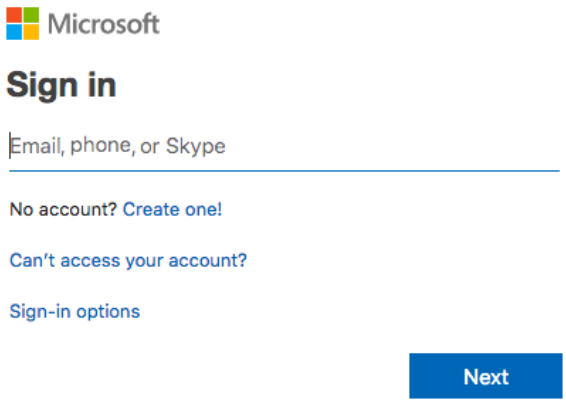
upvoted 3 times

Question #72 *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 -



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.

Suggested 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 ɔ€Set user passwords to expire after a number of daysɔ€ is ticked.
6. Enter 60 in the ɔ€Days before passwords expireɔ€ field.
7. Enter 10 in the ɔ€Days before a user is notified about expirationɔ€ field.
8. Click the 'Save changes' button.

johnyb Highly Voted 2 years, 3 months ago
At the moment I can't see the option for reminding the password expiration.
upvoted 7 times

OscarGir 2 years, 3 months ago

Agree, I don't see this option

upvoted 3 times

hufflepuff 2 years, 3 months ago

Tested and I only see "Days before passwords expire", no reminder options.

upvoted 3 times

Kees1990 Highly Voted 1 year, 11 months ago

i found this: Set-MsolPasswordPolicy -ValidityPeriod 60 -NotificationDays 10

upvoted 5 times

fessebook Most Recent 1 year, 8 months ago

Password expiration notifications are no longer supported in the Microsoft 365 admin center and Microsoft 365 apps.
https://learn.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide

upvoted 2 times

Hanan1234 1 year, 11 months ago

Tested:

1- navigate to 365 admin center

2- settings > org setting > security and privacy

3- password expiration policy

upvoted 3 times

Question #73 *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: 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

Suggested 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

Community vote distribution
B (100%)

SinghG Highly Voted 4 years, 4 months ago
This is incorrect. Right answer is to run the AAD Connect setup wizard to include the newly created sub-domain.
upvoted 38 times

kuuser Highly Voted 4 years, 4 months ago
Is this really true? I thought you should only have one AD Connect server per tenant!
upvoted 21 times

Razuli 3 years, 7 months ago
Exactly, you can't have more than one per tenant
upvoted 9 times

Contactfornitish Most Recent 2 years, 5 months ago
Selected Answer: B
There is only one Azure AD Tenant, for which AAD Connect already deployed. How can one chose A?
upvoted 3 times

Contactfornitish 2 years, 5 months ago
Selected Answer: B
Can't be A
upvoted 1 times

Rudelke 2 years, 5 months 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 AAD 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 years, 5 months ago

Selected Answer: B

Incorrect A.

upvoted 1 times

mikaiwhodakno 2 years, 6 months 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. AD connect is already deployed in the root domain which can see all child domains. Therefore re-running the wizard and adding the new child domain to sync is the correct answer.

upvoted 1 times

BoxGhost 2 years, 8 months 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 goal 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 3 years, 1 month ago

In exam today

upvoted 1 times

Creations 3 years, 4 months ago

There is no "active mode " we only have staging mode setting

upvoted 1 times

Nasser 3 years, 4 months ago

It is impossible to do that because one Azure Connect server can be active at a time.

upvoted 1 times

Carlo5 3 years, 6 months ago

"set AD Connect to active mode", I think it is the key word.

upvoted 3 times

melatocaroca 3 years, 7 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 3 years, 6 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 3 years, 7 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 tenant.

upvoted 3 times

egdeeptha 3 years, 7 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 sync is the correct answer.

upvoted 2 times

Mlt1865 3 years, 7 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 3 years, 8 months ago

No way. NO

upvoted 3 times

Mujja 2 years, 7 months ago

So, not a No = Yes?

upvoted 1 times

Question #74 *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: 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

Suggested 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

[Removed] Highly Voted 4 years 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 the 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 3 years ago
1AAD 1ADDC, rerun the wizard, and include the new domain.
there is no other option.
upvoted 1 times

MerryWeasel 3 years, 11 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 3 years, 11 months ago
typo: *AADC
upvoted 1 times

melatocaroca 3 years, 6 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 wizard 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 3 years, 6 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 5 times

melatocaroca 3 years, 6 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 4 years ago
No for sure!
upvoted 3 times

phvogel 4 years, 2 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