



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



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

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 Services (AD DS) domain named contoso.com.

You need to identify which server is the PDC emulator for the domain.

Solution: From Active Directory Domains and Trusts, you right-click Active Directory Domains and Trusts in the console tree, and then select Operations Master.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

Community vote distribution

B (100%)

 **VinoTee** Highly Voted 3 years, 2 months ago

1. Right-click on the domain
  2. Click Operations Masters
  3. Click the PDC tab to view the server holding the PDC master role
- upvoted 27 times

 **tenob34120** Most Recent 2 weeks, 4 days ago

**Selected Answer: B**

hgghhghg

upvoted 1 times

 **SDK76** 3 months ago

**Selected Answer: B**

Made a mistake below: admin delete my earlier post.

The Operations Master roles can be view via ADU&C – these include the RID, PDC and Infrastructure roles.

PS:

Get-ADDomain | Select-Object RIDMaster

Get-ADDomain | Select-Object PDCEmulator

Get-ADDomain | Select-Object InfrastructureMaster

The Domain Naming Master role can be view by AD Domains and Trusts

Get-ADForest | Select-Object DomainNamingMaster.

Note: The Schema Master role can viewed by AD Sites and Services

Get-ADForest | Select-Object SchemaMaster - you can register the Schema snap-in. Run>regsvr32 schmmgmt.dll. Then go MMC > File > ADD> AD Schema.

Points: All 5 roles start out on the initial DC: 2 roles are forest wide, 3 domain level. You only have one writable copy of the Domain/Schema roles in your forest.

upvoted 1 times

 **SDK76** 3 months ago

**Selected Answer: B**

The Operations Master roles can be view via ADU&C – these include the RID, PDC and Infrastructure roles.

PS:

Get-ADDomain | Select-Object RIDMaster

Get-ADDomain | Select-Object PDCEmulator

Note: The Schema Master role can viewed by AD Sites and Services

Get-ADForest | Select-Object SchemaMaster

The Domain Naming Master role can be view by AD Domains and Trusts

Get-ADForest | Select-Object DomainNamingMaster.

upvoted 1 times

🗲️ 👤 **Vinopanda** 5 months, 1 week ago

**Selected Answer: B**

This Solution will not meet the goal

upvoted 1 times

🗲️ 👤 **stonwall12** 5 months, 4 weeks ago

**Selected Answer: B**

Answer: No.

The solution does not meet the goal because Active Directory Domains and Trusts management console is used for managing forest-wide operations masters (FSMO) roles, specifically the Domain Naming Master and Schema Master, not the PDC Emulator role.

upvoted 1 times

🗲️ 👤 **rafacne** 7 months ago

**Selected Answer: B**

B is the correct

upvoted 1 times

🗲️ 👤 **boyihi9432** 11 months, 3 weeks ago

B is the correct answer .

upvoted 1 times

🗲️ 👤 **wilsont8** 1 year, 1 month ago

**Selected Answer: B**

B. This is the correct answer.

upvoted 1 times

🗲️ 👤 **Roy\_zuniga** 1 year, 5 months ago

B is the one.

upvoted 1 times

🗲️ 👤 **pass601** 2 years ago

B is CORRECT ANSWER

upvoted 1 times

🗲️ 👤 **syu31svc** 2 years, 3 months ago

**Selected Answer: B**

It's not Active Directory Domains and Trusts but Active Directory Users and Computers

Answer is No

upvoted 4 times

🗲️ 👤 **wyvern8888** 2 years, 3 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/find-servers-holding-fsmo-role>

upvoted 1 times

🗲️ 👤 **Goofer** 2 years, 5 months ago

**Selected Answer: B**

You see the Operations Master not the PDC emulator

upvoted 2 times

🗲️ 👤 **iel** 2 years, 6 months ago

B Correct:

Open AD User and Account

Right click and select Operation Master

upvoted 3 times

  **nefaxto** 3 years, 1 month ago

**Selected Answer: B**

B Correct

upvoted 2 times



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com.

You need to identify which server is the PDC emulator for the domain.

Solution: From a command prompt, you run netdom.exe query fsmo.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: A**

*Community vote distribution*

A (100%)

  **SDK76** 3 months ago

**Selected Answer: A**

PS:

Get-ADDomain | Select-Object RIDMaster



Get-ADDomain | Select-Object PDCEmulator

Get-ADDomain | Select-Object InfrastructureMaster

Get-ADForest | Select-Object SchemaMaster

Get-ADForest | Select-Object DomainNamingMaster

upvoted 1 times



  **stonwall12** 5 months, 4 weeks ago

**Selected Answer: A**

Answer: Yes


Running "netdom query fsmo" from a command prompt will identify the PDC emulator role holder for the domain.

upvoted 1 times

  **pass601** 6 months, 3 weeks ago

A is CORRECT ANSWER

upvoted 1 times

  **syu31svc** 9 months, 2 weeks ago

**Selected Answer: A**

This is the correct answer

upvoted 1 times

  **STFN2019** 1 year ago

The correct command is netdom query fsmo, ref: <https://activedirectorypro.com/how-to-check-fsmo-roles/>

upvoted 1 times

  **JohnO1971** 1 year, 2 months ago

**Selected Answer: A**

Tested it on a Windows 10 laptop and it returns the correct results, answer should be A

upvoted 2 times

  **WMG** 1 year, 4 months ago

**Selected Answer: A**

Correct answer .Netdom.exe, c:\windows\system32. You can use "netdom" or "netdom.exe", and the "query FSMO" will list all FSMO roles, including which server is the PDC.

upvoted 3 times

  **josepedroche** 1 year, 5 months ago

**Selected Answer: A**

netdom.exe exits

Use ++Netdom.exe+++ to reset machine account passwords of a Windows Server domain controller

upvoted 2 times

🗨️ 👤 **plmmmsg** 1 year, 5 months ago

answer is correct. it can be run with .exe

upvoted 2 times

🗨️ 👤 **AmineHZ** 1 year, 6 months ago

correct

upvoted 3 times

🗨️ 👤 **panthermc** 1 year, 6 months ago

the correct answer is false. there are no .exe at the end. To get the fsmo you need to run "netdom query fsmo" in CMD.

upvoted 3 times

🗨️ 👤 **panthermc** 1 year, 6 months ago

Ok, after rereading the question I found it to be true. My bad. it can be run with the .exe also.

upvoted 3 times

🗨️ 👤 **ET42** 1 year, 7 months ago

No, there is no .exe after netdom

upvoted 2 times

🗨️ 👤 **Jandegroot09** 1 year, 7 months ago

Incorrect. I was thinking the same but I tested it with netdom.exe and that's also working.

upvoted 1 times

🗨️ 👤 **panthermc** 1 year, 6 months ago

I could not get the .exe to run. I had to run "netdom query fsmo" in CMD to get the results. So I am guessing this one should be false.

upvoted 2 times

🗨️ 👤 **nefaxto** 1 year, 7 months ago

**Selected Answer: A**

Yes, it's Correct A

upvoted 3 times

🗨️ 👤 **Arpan\_kumar\_roy** 1 year, 7 months ago

Correct

upvoted 3 times

You have an on premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant. You plan to implement self-service password reset (SSPR) in Azure AD. You need to ensure that users that reset their passwords by using SSPR can use the new password resources in the AD DS domain. What should you do?

- A. Deploy the Azure AD Password Protection proxy service to the on premises network.
- B. Run the Microsoft Azure Active Directory Connect wizard and select Password writeback.
- C. Grant the Change password permission for the domain to the Azure AD Connect service account.
- D. Grant the impersonate a client after authentication user right to the Azure AD Connect service account.

**Correct Answer: B**

Community vote distribution



B (100%)

 **Lazylinux**  3 years, 1 month ago

**Selected Answer: B**

B Is correct

upvoted 9 times

 **stonwall12**  5 months, 4 weeks ago

**Selected Answer: B**

Answer: B, Password writeback.

Password writeback enables bidirectional password synchronization between on-premises AD DS and Azure AD, which is essential for SSPR functionality.

upvoted 1 times

 **bipinmikeeyis** 7 months ago

**Selected Answer: B**

Enable Password Writeback:

Password writeback allows password changes made in the cloud (via SSPR) to be written back to the on-premises AD DS directory in real time.

This feature ensures that the updated passwords are synchronized to the on-premises environment.

You can enable password writeback using either Microsoft Azure AD Connect or Azure AD Connect cloud sync.

When users change or reset their passwords using SSPR in the cloud, the updated passwords are also written back to the on-premises AD DS environment.

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-writeback>

Guide: <https://sites.google.com/view/learnmicrosoftcomenustrainingm/home>

upvoted 3 times

 **SIAMIANJI** 9 months, 1 week ago

**Selected Answer: B**

Enable Password Writeback:

Password writeback allows password changes made in the cloud (via SSPR) to be written back to the on-premises AD DS directory in real time.

This feature ensures that the updated passwords are synchronized to the on-premises environment.

You can enable password writeback using either Microsoft Azure AD Connect or Azure AD Connect cloud sync.

When users change or reset their passwords using SSPR in the cloud, the updated passwords are also written back to the on-premises AD DS environment.

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-writeback>

upvoted 2 times

 **ESAJRR** 1 year, 8 months ago

**Selected Answer: B**

B. Run the Microsoft Azure Active Directory Connect wizard and select Password writeback.

upvoted 1 times

 **Firdaus1996** 1 year, 9 months ago



B is correct

upvoted 1 times

  **pass601** 2 years ago

B is CORRECT ANSWER



upvoted 1 times

  **syu31svc** 2 years, 3 months ago

**Selected Answer: B**



B is correct as supported by provided link

upvoted 1 times

  **plmmsg** 2 years, 12 months ago

writeback is correct

upvoted 3 times

  **AmineHZ** 3 years ago

B is correct

upvoted 2 times

  **Arpan\_kumar\_roy** 3 years, 1 month ago

Correct

upvoted 3 times

## HOTSPOT -

Your network contains an Active Directory Domain Services (AD DS) forest named contoso.com.

You create the resources shown in the following table.

Name	Type	Member of	In organizational unit (OU)
User1	User	None	Contoso.com\OU1
User2	User	Group1	Contoso.com\OU1
User3	User	Group1	Contoso.com\OU2
Group1	Group	None	Contoso.com\OU1
Comp1	Client computer	Group1	Contoso.com\OU2

You create the Group Policy Objects (GPOs) shown in the following table.

Name	Linked to
GPO1	OU1
GPO2	OU2

You configure the Group Policy Preferences shown in the following table.

GPO	Setting
GPO1	Computer Configuration: Add a shortcut named Link1 to the desktop User Configuration: Add a shortcut named Link2 to the desktop
GPO2	Computer Configuration: Add a shortcut named Link3 to the desktop User Configuration: Add a shortcut named Link4 to the desktop

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
If User1 signs in to Comp1, a shortcut named Link4 will appear on the computer's desktop.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Comp1, a shortcut named Link2 will appear on the computer's desktop.	<input type="radio"/>	<input type="radio"/>
If User3 signs in to Comp1, a shortcut named Link2 will appear on the computer's desktop.	<input type="radio"/>	<input type="radio"/>



Correct Answer:

#### Answer Area

Statements	Yes	No
If User1 signs in to Comp1, a shortcut named Link4 will appear on the computer's desktop.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Comp1, a shortcut named Link2 will appear on the computer's desktop.	<input checked="" type="radio"/>	<input type="radio"/>
If User3 signs in to Comp1, a shortcut named Link2 will appear on the computer's desktop.	<input type="radio"/>	<input checked="" type="radio"/>

  **Webcatman** Highly Voted 7 months, 4 weeks ago



I setup the lab and the result is NYN.  
upvoted 9 times

  **enley2000** Most Recent 2 weeks, 3 days ago

Definitely is YYN.  
There is no mention that loopback processing is enabled. So user policy will be the priority in the case of conflict. But there is no conflict, because the shortcuts are different. So user policy and computer policy will apply.  
upvoted 1 times

  **eea3f8d** 1 week, 1 day ago

for the 1st question its No, because When user1 sing in to computer1 only user configuration will be applied from GP01 , computer configuration will be dropped from GP01, for GP02 user configuration will be dropped and computer config will apply therefore user1 in computer 1 will see only link2 and link3  
upvoted 1 times

  **stonwall12** 5 months, 4 weeks ago

Answer: NYN

For User1:


User1 is not a member of any group  
Comp1 is in OU2 which links to GP02  
GP02 would apply Link4, but User1 is in OU1  
Therefore, Link4 will NOT appear (No)

For User2:



User2 is a member of Group1 and is in OU1  
GP01 applies to OU1 and adds Link2 for user configuration  
Therefore, Link2 WILL appear (Yes)

For User3:

User3 is in OU2 and is a member of Group1  
While in OU2 (which has GP02), the Link2 is from GP01 which is linked to OU1  
Therefore, Link2 will NOT appear (No)  
upvoted 1 times

  **mainesketch** 5 months, 3 weeks ago

Should be NNN ... Comp config will always override User config  
The GPO are linked to OUs not groups  
upvoted 2 times

  **stonwall12** 5 months, 2 weeks ago

Mm, correct!

The answer is NNN:

- Computer configuration settings override user configuration settings
- Since Comp1 is in OU2, GP02's computer configuration (Link3) will override any user configuration settings (Link2 or Link4) regardless of which user logs in.

upvoted 2 times

🗨️ 👤 **Neuch** 5 months, 2 weeks ago

There's no override because it's not the same shortcut/config

NYN for me

upvoted 2 times

🗨️ 👤 **igather0** 8 months, 2 weeks ago

Think NYN

upvoted 4 times

🗨️ 👤 **Ksk08** 8 months, 2 weeks ago

Sorry it should be YNY

upvoted 1 times

🗨️ 👤 **Ksk08** 8 months, 2 weeks ago

should be YNN.

upvoted 2 times

🗨️ 👤 **Ksk08** 7 months, 2 weeks ago

YNN is confirm

upvoted 2 times

🗨️ 👤 **nazw1** 7 months ago

what is the correct answer?

upvoted 1 times

🗨️ 👤 **Ksk08** 8 months, 2 weeks ago

Answer is YNY

upvoted 1 times

🗨️ 👤 **Ksk08** 8 months, 2 weeks ago

Sorry should be NNN

upvoted 1 times

🗨️ 👤 **mainesketch** 5 months, 3 weeks ago

Should be NNN ... Comp config will always override User config

upvoted 1 times

🗨️ 👤 **Neuch** 5 months, 2 weeks ago

No, the comp config override user config only if you use loopback processing

NYN for me

upvoted 2 times

DRAG DROP -

You create a new Azure subscription.

You plan to deploy Azure Active Directory Domain Services (Azure AD DS) and Azure virtual machines.

You need to ensure that the virtual machines can join to Azure AD DS.

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

Select and Place:

### Actions

Modify the settings of the Azure virtual network.

Install the Active Directory Domain Services role.

Install Azure AD Connect.

Create an Azure virtual network.

Create an Azure AD DS instance.

Run the Active Directory Domain Service installation Wizard.

### Answer Area



Correct Answer:

### Actions

Install the Active Directory Domain Services role.

Install Azure AD Connect.

Run the Active Directory Domain Service installation Wizard.

### Answer Area

Create an Azure virtual network.

Create an Azure AD DS instance.

Modify the settings of the Azure virtual network.



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance>

Justin0020 Highly Voted 1 year, 3 months ago

Correct answer

1. Create Virtual Network
2. Create AD DS instance, because in the wizard you have to select virtual network to deploy it on
3. Modify the DNS server settings in the Virtual Network/Subnets

upvoted 21 times

stonwall12 Most Recent 5 months, 4 weeks ago



Answer:

1. Create an Azure virtual network
2. Create an Azure AD DS instance
3. Modify the settings of the Azure virtual network



1. Create an Azure virtual network - This is the foundational step that provides the network infrastructure where your Azure AD DS and VMs will reside.

2. Create an Azure AD DS instance - After the virtual network is in place, you deploy the managed domain service within it. This step provisions the domain controllers as managed VMs in your virtual network.

3. Modify the settings of the Azure virtual network - After Azure AD DS is deployed, you need to update the DNS settings of the virtual network to use the DNS servers provided by the managed domain. This ensures that VMs in the virtual network can resolve and join the domain.

<https://learn.microsoft.com/en-us/entra/identity/domain-services/tutorial-create-instance>

upvoted 2 times

  **syu31svc** 9 months, 1 week ago

Given answer is correct as supported by link provided

upvoted 3 times

  **Lu5ck** 1 year ago

MS like to ask step by step in perspective of powershell or script.

<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance>

upvoted 3 times

## HOTSPOT -

You have an Azure Active Directory Domain Services (Azure AD DS) domain.

You create a new user named Admin1.

You need Admin1 to deploy custom Group Policy settings to all the computers in the domain. The solution must use the principle of least privilege.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Hot Area:

### Answer Area

Add Admin1 to the following group:

AAD DC Administrators
Domain Admins
Group Policy Creator Owners

Instruct Admin1 to apply the custom Group Policy settings by:

Creating a new Group Policy Object (GPO) and linking the GPO to the domain
Modifying AADDC Computers GPO
Modifying the default domain GPO

### Correct Answer:

#### Answer Area

Add Admin1 to the following group:

AAD DC Administrators
Domain Admins
Group Policy Creator Owners

Instruct Admin1 to apply the custom Group Policy settings by:

Creating a new Group Policy Object (GPO) and linking the GPO to the domain
Modifying AADDC Computers GPO
Modifying the default domain GPO

### Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy> <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou>

 **nefaxto** Highly Voted 1 year, 7 months ago

AAD DC Administrators

Modifying AADDC Computers GPO

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy>

The GPO can be linked on UO not to the domain

upvoted 31 times

 **olnn** Highly Voted 1 year, 8 months ago

bad:

1 ok

but

2 creating a new GPO

upvoted 13 times

🗨️ 👤 **Josty** 1 year, 4 months ago

the group policy can't be linked to the domain only to a OU -> so Modifying AADDC Computers GPO is the correct one

upvoted 6 times

🗨️ 👤 **stonwall12** Most Recent 5 months, 4 weeks ago

Answer:

1. AAD DC Administrators
2. Create a new GPO linked to domain

1. This is the required group for managing Group Policy in Azure AD DS.
2. While you can modify the built-in GPOs (AADDC Users and AADDC Computers), creating a custom GPO provides better management and control and is the recommended approach as per Microsoft documentation for implementing custom policies.

<https://learn.microsoft.com/en-us/entra/identity/domain-services/manage-group-policy>

upvoted 3 times

🗨️ 👤 **tanoj** 8 months, 1 week ago

deploy custom Group Policy settings to all the COMPUTERS in the domain.

Answer : SO when you create a new gpo and link to the domain it will be applied to both users and computers. As it is required only for the computers in the domain you need to modify the existing Computers GPO which is the fit answer.

upvoted 1 times

🗨️ 👤 **syu31svc** 9 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy>

A user account that's a member of the Azure AD DC administrators group in your Azure AD tenant (Before you begin)

hese built-in GPOs can be customized to configure specific group policies on your managed domain. Right-select one of the GPOs, such as AADDC Computers GPO, then choose Edit.... (Open the Group Policy Management Console and edit an object)

Answer is correct

upvoted 2 times

🗨️ 👤 **Lu5ck** 1 year ago

Keyword is ADDS. Not on-on-premises DS or hybrid. Therefore, the only option is ADDS admin and AD GPO.

upvoted 3 times

🗨️ 👤 **Lu5ck** 1 year ago

AADDS. Missed out the A. :D

upvoted 5 times

🗨️ 👤 **giver** 1 year, 4 months ago

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy> -- clearly shows

upvoted 2 times

🗨️ 👤 **giver** 1 year, 4 months ago

Given is Correct.

upvoted 2 times

🗨️ 👤 **dapkor** 1 year, 5 months ago

Is a custom GPO thats requested.

1. = AADDC Admin
2. Creating a new gpo <--

upvoted 3 times

**DRAG DROP -**

Your network contains a single domain Active Directory Domain Services (AD DS) forest named contoso.com. The forest contains a single Active Directory site.

You plan to deploy a read only domain controller (RODC) to a new datacenter on a server named Server1. A user named User1 is a member of the local

Administrators group on Server1.

You need to recommend a deployment plan that meets the following requirements:

- ⇒ Ensures that a user named User1 can perform the RODC installation on Server1
- ⇒ Ensures that you can control the AD DS replication schedule to the Server1
- ⇒ Ensures that Server1 is in a new site named RemoteSite1

Uses the principle of least privilege

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

Select and Place:

**Actions****Answer Area**

Instruct User1 to run the Active Directory Domain Services installation Wizard on Server1.

Create a site and a subnet.

Create a site link.

Pre-create an RODC account.

Add User1 to the Contoso\Administrators group.

**Correct Answer:****Actions****Answer Area**

Create a site link.

Add User1 to the Contoso\Administrators group.

Create a site and a subnet.

Pre-create an RODC account.

Instruct User1 to run the Active Directory Domain Services installation Wizard on Server1.



Box 1.

We need to create a site and subnet for the remote site. The new site will be added to the Default IP Site Link so we don't need to create a new site link. You configure the replication schedule on the site link.

Box 2.

When we pre-create an RODC account, we can specify who is allowed to attach the server to the prestaged account. This means that the User1

does not need to be added to the Domain Admins group.

Box3.

User1 can connect the RODC to the prestaged account by running the AD DS installation wizard.

Reference:

<https://mehic.se/2018/01/02/how-to-install-and-configure-read-only-domain-controller-rodc-2016/>

  **edykss**  1 year, 3 months ago

Given answer is correct.

upvoted 12 times

  **tfulanchan**  10 months, 1 week ago

Question#31 Topic 1 is the same except that "Ensures that you can control the AD DS replication schedule to the Server1" is not mentioned. The answers for these two questions are different and confusing.

upvoted 6 times



  **ppardav**  1 month, 1 week ago

If you want to control the replication between sites you need to create a different site link

so the solution should be :

- 1) Pre-Create RODC account
- 2) Create Site link
- 3) Create a site and subnet

upvoted 1 times



  **stonwall12** 5 months, 4 weeks ago

Answer:

1. Create a site and subnet
2. Pre-create an RODC account
3. Instruct User1 to run the Active Directory Domain Services

Creating the site and subnet first establishes the network foundation needed for RODC replication. Pre-creating the RODC account next ensures security by configuring password replication policies and permissions before installation. Finally, having User1 run the AD DS installation wizard leverages their local admin rights to complete the deployment in the properly prepared environment.

upvoted 3 times

  **syu31svc** 9 months, 1 week ago

Answer is correct and link given supports it

upvoted 2 times

Your network contains an Active Directory Domain Services (AD DS) domain. The network also contains 20 domain controllers, 100 member servers, and 100 client computers.

You have a Group Policy Object (GPO) named GPO1 that contains Group Policy preferences.

You plan to link GPO1 to the domain.

You need to ensure that the preference in GPO1 apply only to domain member servers and NOT to domain controllers or client computers. All the other Group

Policy settings in GPO1 must apply to all the computers. The solution must minimize administrative effort.

Which type of item level targeting should you use?

- A. Domain
- B. Operating System
- C. Security Group
- D. Environment Variable

**Correct Answer: B**

Community vote distribution

B (67%)



C (33%)

  **kijken**  2 years, 8 months ago

Nothing is mentioned about OS. Domain controllers can have the same OS.

I would do it based on C

upvoted 12 times


  **kijken** 2 years, 8 months ago

I want to correct this answer, I did some testing, and the operating system option has a computer role option in it. You can set that to member server. So this is a valid option.

Security group is also possible, but requires more overhead. You should always choose the best option. Same for D, which would also be a possibility. Domain is rubbish

So B is correct

upvoted 21 times

  **boapaulo** 1 year, 6 months ago

Option B, "Operating System," would not be the best choice in this case because it would apply the preference to all computers running the specified operating system, not just member servers. This means that the preference would also apply to domain controllers and client computers that are running the same operating system, which is not in line with the requirement.

In contrast, Security Group item-level targeting allows for more granular control, allowing you to apply the preference only to member servers, regardless of the operating system they are running. This meets the requirement to apply the preference only to member servers and not to domain controllers or client computers. Furthermore, it minimizes administrative effort.

upvoted 1 times

  **sardonique** 1 year, 2 months ago

you're in the wrong direction. it takes time to create a group with all the servers needed, especially if these server are spread around many OUs, whereas it takes only 7 objects to configure within the "Operating Systems" option: one for each major release of Windows Server:

2003,2003r2,2008,2008r2,2012,2012r2,2022, it allows you to specify "domain member"


upvoted 2 times

  **keniel**  1 week, 6 days ago

**Selected Answer: B**

OS targeting specify DC from memeber server

upvoted 1 times

  **lxxxnnnnx** 2 months, 4 weeks ago

**Selected Answer: C**

Item-level targeting in Group Policy Preferences (GPP) allows applying settings only to specific objects that meet certain criteria.

upvoted 1 times

🗨️ 👤 **Kumar\_ram\_** 3 months, 2 weeks ago

**Selected Answer: B**

Option Description

Product The product name of the operating system.

Edition The edition of the product such as Enterprise, Standard, or Web.

Release The release of the product. If the desired service pack does not appear in the list, type the full name of the service pack in the box (for example, Service Pack 3).

Computer role The role of the computer. A computer that is running Windows has one of three roles:

Workstation: A domain-joined computer that is running any release of Windows® 7, Windows Vista®, or Windows XP.

Member Server: A domain-joined computer that is running any release of Windows Server® 2008 R2, Windows Server 2008, or Windows Server 2003.

Domain Controller: A computer running any release of Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 that hosts Active Directory® directory service for the domain.

upvoted 1 times

🗨️ 👤 **thomasemr** 4 months, 4 weeks ago

**Selected Answer: B**

B because is possible choice in Computer Role on Targeting Editor, if Member Server or Domain Controller

upvoted 1 times

🗨️ 👤 **Mustapha\_Hadrich** 5 months, 3 weeks ago

**Selected Answer: C**

I would say security groups because domain controllers and member server could have the same os

upvoted 2 times

🗨️ 👤 **stonwall12** 5 months, 4 weeks ago

Answer: C, Security Group.

This solution allows you to target Group Policy preferences to specific computers by adding the member servers to a dedicated security group.

IT IS NOT OPERATING SYSTEM:

Operating System targeting isn't ideal because server environments often run a mix of Windows Server versions simultaneously (like Server 2019 and 2022). This would require creating and maintaining multiple OS-specific targeting rules, increasing complexity and administrative overhead compared to the simpler approach of using a security group.

upvoted 1 times

🗨️ 👤 **nonoelptirobo** 4 months, 1 week ago

actually there is a specific role section in the item level OS targeting :

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789189\(v=ws.11\)#operating-system-targeting](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789189(v=ws.11)#operating-system-targeting)

The role of the computer. A computer that is running Windows has one of three roles:

Workstation: A domain-joined computer that is running any release of Windows® 7, Windows Vista®, or Windows XP.

Member Server: A domain-joined computer that is running any release of Windows Server® 2008 R2, Windows Server 2008, or Windows Server 2003.

Domain Controller: A computer running any release of Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 that hosts Active Directory® directory service for the domain.

trick question as "least complex" would be that (creating / adding computers to a sec group is being a step to do to every new server created )

upvoted 1 times

🗨️ 👤 **Midoria** 7 months, 1 week ago

Operating System Targeting includes a Computer Role option, which allows you to specify whether the preference applies to Domain Controllers, Member Servers, or Workstations. By selecting Member Server, you can easily apply the preference to only member servers, avoiding the need to manually manage security groups.

Why this works better:

It avoids the additional step of creating or maintaining a security group.

It minimizes administrative effort by leveraging built-in functionality. B

upvoted 2 times

🗨️ 👤 **AB164** 7 months, 3 weeks ago

This is not a clear answer, who can explain please ?

upvoted 1 times

🗳️ 👤 **Ksk08** 8 months ago

Answer is c

upvoted 1 times

🗳️ 👤 **TTC000** 8 months, 4 weeks ago

**Selected Answer: C**

Explanation:

You need to apply the Group Policy Object (GPO) only to member servers, while excluding domain controllers and client computers.

The most efficient way to do this with minimal administrative effort is by using Security Group targeting.

You can place all the member servers into a security group, and then apply the GPO preference specifically to that group.

This approach ensures that only the specified member servers receive the GPO preference, without impacting domain controllers or client computers.

This method provides a granular way of controlling which machines the policy applies to.

upvoted 1 times

🗳️ 👤 **syu31svc** 9 months, 1 week ago

**Selected Answer: B**

"apply only to domain member servers and NOT to domain controllers or client computers"

From the link

Computer role The role of the computer. A computer that is running Windows has one of three roles:

Workstation: A domain-joined computer that is running any release of Windows® 7, Windows Vista®, or Windows XP.

Member Server: A domain-joined computer that is running any release of Windows Server® 2008 R2, Windows Server 2008, or Windows Server 2003.

Domain Controller: A computer running any release of Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 that hosts Active Directory® directory service for the domain.

B is correct

upvoted 3 times

🗳️ 👤 **boapaulo** 1 year, 6 months ago

Option B, "Operating System," would not be the best choice in this case because it would apply the preference to all computers running the specified operating system, not just member servers. This means that the preference would also apply to domain controllers and client computers that are running the same operating system, which is not in line with the requirement.

In contrast, Security Group item-level targeting allows for more granular control, allowing you to apply the preference only to member servers, regardless of the operating system they are running. This meets the requirement to apply the preference only to member servers and not to domain controllers or client computers. Furthermore, it minimizes administrative effort.

upvoted 2 times

🗳️ 👤 **JPO2021** 10 months, 4 weeks ago

Option B "Operating System"

\*An Operating System targeting item allows a preference item to be applied to computers or users only if the processing computer's operating system's product name, release, edition, or computer role matches those specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the operating system's product name, release, edition, or computer role does not match those specified in the targeting item.

\*[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v=ws.11))

upvoted 2 times

🗳️ 👤 **linuxlinuxmint** 1 year, 1 month ago

# Définition des rôles que vous souhaitez filtrer

\$roles = @("DHCP", "DNS") # Ajoutez d'autres rôles au besoin

# Filtrer les serveurs ayant des rôles spécifiques

\$serveursAvecRoles = Get-WmiObject Win32\_ServerFeature | ? { \$\_.Name -in \$roles } | Select-Object PSComputerName

# Filtrer les serveurs sans rôles spécifiques

\$serveursSansRoles = Get-WmiObject Win32\_ServerFeature | ? { \$\_.Name -notin \$roles } | Select-Object PSComputerName

# Afficher les résultats

Write-Host "Serveurs avec des rôles spécifiques (\$roles) :"



\$serveursAvecRoles

Write-Host "Serveurs sans des rôles spécifiques (\$roles) :"

\$serveursSansRoles

upvoted 1 times

🗉 👤 **sardonique** 1 year, 2 months ago

As always the question has an ambiguous interpretation. If you have a security group that already contains all the desired computer objects, this solution is the faster. however you cannot assume that. so you would need to create a group and put all the servers as members of the group. you can achieve that using powershell pretty quickly. in my opinion the "Operating System" option is the way to go since it allows to filter by role: "Any", "Member Server" and "Domain Controller", so you would need to add a few rows (7 from 2003 to 2022) such as OS is server 2003 family, OS is server 2003R2 family, OS is server 2008 family .... and for each one of these you would choose the role "Member Server".

upvoted 3 times

🗉 👤 **rasmart** 1 year, 2 months ago

**Selected Answer: C**

This seems to be the most effective approach. You could create a security group that includes all the member servers and then target this group with the GPO. This method is precise and allows you to have full control over which servers are affected by the GPO. It requires some initial setup to create and populate the security group, but it minimizes ongoing administrative effort as the group membership dictates the GPO application.

upvoted 1 times

🗉 👤 **SanMan\_NZ** 1 year, 4 months ago

**Selected Answer: B**

OS targeting is correct only because there is an item under OS targeting called 'Computer Role' which has options to select 'Workstation', Member Srv' or 'Domain Controller.' Answer B is works and the easiest way to achieve the objective.

upvoted 3 times

🗉 👤 **Mustapha\_Hadrich** 5 months, 3 weeks ago

unless you use wmi filter like

Select \* from Win32\_ComputerSystem where DomainRole < 4

the easiest way is by security groups

upvoted 1 times

## DRAG DROP -

You deploy a new Active Directory Domain Services (AD DS) forest named contoso.com. The domain contains three domain controllers named DC1, DC2, and DC3.

You rename Default-First-Site-Name as Site1.

You plan to ship DC1, DC2, and DC3 to datacenters in different locations.

You need to configure replication between DC1, DC2, and DC3 to meet the following requirements:

- ⇒ Each domain controller must reside in its own Active Directory site.
- ⇒ The replication schedule between each site must be controlled independently.
- ⇒ Interruptions to replication must be minimized.

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

Select and Place:

**Actions**

Create a connection object between DC1 and DC2.

Create an additional site link that contains Site1 and Site2.

Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3.

Create a connection object between DC2 and DC3.

Remove Site2 from DEFAULTIPSITELINK.

**Answer Area****Correct Answer:****Actions**

Create an additional site link that contains Site1 and Site2.

Remove Site2 from DEFAULTIPSITELINK.

**Answer Area**

Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3.

Create a connection object between DC1 and DC2.

Create a connection object between DC2 and DC3.



prepper666 Highly Voted 3 years ago

Answer is wrong, nothing to do with Connection objects. To control Inter-site replication, configure the IPSITELINK properties and schedule. KCC generates connection objects and takes replication details from the site link. Correct answer is:

1. create 2 additional sites and move DC2 and DC3.
2. Create and additional site link between site 2 and site 3 (does this first so as not to disrupt site 1 and site 2)

3. remove Site 2 from Default sitelink (leaving site 1 and 3 to replicate. by default site-link Bridging is enabled so 1 to 2 and 1 to 3 bridges the link between 2 and 3)

upvoted 32 times

  **lukiduc9625** 2 years, 9 months ago

1. Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3 - After this step Site2 and Site3 are linked to each other and to Site1 by DEFAULTSITELINK and in both new sites "automatically generated" connection objects will be created

2. Create an additional site link between site 2 and site 3 - but such action is not mentioned in available actions set. There is only "Create and additional site link between Site1 and Site2". I'm not sure, that adding Site1 and Site2 to new site link will disrupt replication between these sites. I don't think so. After this step:

- Site1 is linked to Site2 by DEFAULTSITELINK and NewSiteLink

- Site1 is linked to Site3 by only DEFAULTSITELINK

- Site2 is linked to Site3 by only DEFAULTSITELINK

3. remove Site 2 from DEFAULTSITELINK - After this step:

- Site1 is linked to Site2 by only NewSiteLink

- Site1 is linked to Site3 by only DEFAULTSITELINK

- Site2 is not directly linked to Site3 - replication must go through Site1

Two first requirements are fulfilled. But whether interruptions to replication is minimized? hmmm

upvoted 6 times

  **MR\_Eliot** 1 year, 9 months ago

I agree with this approach

upvoted 1 times

  **lukiduc9625** 2 years, 9 months ago

I'm not sure - there is no action "Create and additional site link between site 2 and site 3"

upvoted 4 times

  **GoforiT21** 3 years ago

Thanks for your take on this! Would you have a source to document that approach?

upvoted 1 times

  **AnonymousJhb** 2 years, 11 months ago

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/creating-a-site-link-design>

upvoted 1 times

  **loulouka**  3 years ago


Correct order is

1) create two additional sites

2) create an additional site link that contains site1 & site 2

3) Remove site2 from default sitelink

upvoted 14 times

  **stonwall12**  5 months, 4 weeks ago

Answer:



1. Create two additional site links and move DC2/DC3

2. Create an additional site link that contains Site1 and Site2

3. Remove Site2 from DEFAULTSITELINK

This sequence works because the Knowledge Consistency Checker (KCC) automatically handles connection objects based on site links, with site-link bridging enabled by default. Creating sites first ensures proper infrastructure, adding the new site link maintains replication paths, and removing Site2 from the default link completes the topology while preserving replication through bridging between Site1-to-Site2 and Site1-to-Site3. This approach meets all requirements: each DC has its own site, replication schedules can be controlled independently through site links, and interruptions are minimized through proper topology design.

upvoted 1 times

  **Midoria** 7 months, 1 week ago

Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3.

Reason: Each domain controller must reside in its own site. Creating Site2 and Site3 and moving the domain controllers ensures proper placement and organization for replication.

Create an additional site link that contains Site1 and Site2.

Reason: By creating a new site link, you establish an independent replication path between Site1 (DC1) and Site2 (DC2) with its own schedule.

Remove Site2 from DEFAULTIPSITELINK.

Reason: Removing Site2 from the default site link ensures that it no longer uses the default replication path, which would otherwise conflict with the custom site link created in Step 2. This step helps maintain independent replication control.

upvoted 2 times

🗨️ 👤 **sardonique** 1 year, 2 months ago

the 3 DCs were in the same site, and replicated between themselves (intrasite) regardless of the default sitelink. so when you create new sites, the default sitelink comes into play and so the default site link along with the setting "site-link Bridging" enabled by default can guarantee communication between sites. I assume that the creation of connection objects is some sort of redundancy so the interruptions to replication get minimized? if you remove the site2 from the default sitelink, you won't have anymore the mesh topology between the 3 sites, reducing the number of paths available for replication, which appears to be in contrast to the requirement to minimize interruptions

upvoted 1 times

🗨️ 👤 **pass601** 2 years ago

Correct order is

- 1)create two additinal sites
- 2)create an additinal site link that contains site1 & site 2
- 3)Remove site2 from defaultipsitelink

upvoted 2 times

🗨️ 👤 **syu31svc** 2 years, 3 months ago

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/creating-a-site-link-design>

Whenever you add sites to a newly created site link, determine if the site being added is a member of other site links, and change the site link membership of the site if needed. For example, if you make a site a member of the Default-First-Site-Link when you initially create the site, be sure to remove the site from the Default-First-Site-Link after you add the site to a new site link. If you do not remove the site from the Default-First-Site-Link, the Knowledge Consistency Checker (KCC) will make routing decisions based on the membership of both site links, which may result in incorrect routing.

Answer is

- 1) Create additional sites (Each domain controller must reside in its own Active Directory site)
- 2) Create site link contains 1 and 2
- 3) Remove 2 from DEFAULTIPSITELINK

upvoted 4 times

🗨️ 👤 **sardonique** 1 year, 2 months ago

agree, so Site2 can replicate to site 3 thanks to site 1 being on both links, however removing site2 from the default link removes a replication path, so if the S1 has a network issue, S2 will not be able to replicate with S3

upvoted 1 times

🗨️ 👤 **Lu5ck** 2 years, 6 months ago

Basically, all the DCs are created under "Site1" and shipped out.

1. Obviously, since all these DCs are now in different locations, they need to be placed in their own site. So, now we got Site1, Site2, Site3.
2. They want the "replication schedule" to be controlled "independently". You control this timing via "site link". At this moment, all the 3 site are dumped into "defaultipsitelink". So, what you need to do is create a site link for each of them like "site1-to-site2" and "site1-to-site3".

So, the answer is....

1. Create 2 additional sites for DC2 and DC3
2. Create a new site link
3. Remove one site from the default site link

Site/subnet is like node in a topology

Site link is the communication between the nodes.

So, DC can be geographically placed in different locations thus you are given the options to customize the communications between these sites through site link.

upvoted 2 times

🗨️ 👤 **johosofat** 2 years, 7 months ago

Same answer but trying to make it more clear -

1. DC1, Dc2, Dc3
  2. Rename Default site to Site1(dc1)
  3. Create sites 2 and 3. -Add DC2 to site2 Add DC3 to site3
  4. Add new site link to site 1 and 2
  5. Remove site 2 from the default site link (now 1 and 3 are left)
- upvoted 1 times

  **joehoesofat** 2 years, 8 months ago

New Multi-site setup- create site 2 and 3 and rename default site to site1

1. DC1, Dc2, Dc3
  2. Rename Default site to Site1(dc1)
  3. Add DC2 to site2 Add DC3 to site3
  4. Add site link new to site 1 and 2
  5. Remove default site link from site 2
- upvoted 2 times

  **lukiduc9625** 2 years, 9 months ago

Hi, I think in same manner, but in my opinion one should first remove Site2 from DefaultSiteLink and afterwards Create an additional site link between Site2 and Site3.

upvoted 1 times

Your network contains an Active Directory Domain Services (AD DS) forest named contoso.com. The root domain contains the domain controllers shown in the following table.

Name	FSMO role
DC1	Domain naming master
DC2	RID master
DC3	PDC emulator
DC4	Schema master
DC5	Infrastructure master

A failure of which domain controller will prevent you from creating application partitions?



- A. DC1
- B. DC2
- C. DC3
- D. DC4
- E. DC5

**Correct Answer: A**

Community vote distribution

A (95%)

5%

 **Pandaguo**  3 years, 1 month ago

**Selected Answer: A**

Initial replication and connectivity requirements

This FSMO role holder is only active when the role owner has inbound replicated the configuration NC successfully since the Directory Service started.

Domain members of the forest only contact the FSMO role holder when they update the cross-references. DCs contact the FSMO role holder when:

Domains are added or removed in the forest.

New instances of application directory partitions on DCs are added. For example, a DNS server has been enlisted for the default DNS application directory partitions.



<https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-roles#domain%20naming>

upvoted 11 times

 **AvoKikinha** 3 years, 1 month ago

Correct!

upvoted 4 times

 **Ahmedali70x**  2 months, 2 weeks ago

**Selected Answer: D**

DC4 (Schema Master)

If DC4 (Schema Master) fails, you will not be able to create application partitions, as this FSMO role is responsible for managing schema updates, including those for application partitions.

upvoted 1 times

 **stonwall12** 5 months, 4 weeks ago

**Selected Answer: A**

Answer: A, DC1

If DC1 were to fail, any operations requiring the Domain Naming Master role, including creating application partitions, would be impossible until either:

- DC1 is restored to service, or
  - The Domain Naming Master role is transferred to another domain controller
- upvoted 1 times

🗨️ 👤 **syu31svc** 9 months, 1 week ago

**Selected Answer: A**

A for answer as supported by link given

Domain naming master FSMO role

The domain naming master FSMO role holder is the DC responsible for making changes to the forest-wide domain name space of the directory, that is, the Partitions\Configuration naming context or LDAP://CN=Partitions, CN=Configuration, DC=<domain>. This DC is the only one that can add or remove a domain from the directory. It can also add or remove cross references to domains in external directories.

Initial replication and connectivity requirements

This FSMO role holder is only active when the role owner has inbound replicated the configuration NC successfully since the Directory Service started.

Domain members of the forest only contact the FSMO role holder when they update the cross-references. DCs contact the FSMO role holder when:

Domains are added or removed in the forest.

New instances of application directory partitions on DCs are added. For example, a DNS server has been enlisted for the default DNS application directory partitions.

upvoted 2 times

🗨️ 👤 **ESAJRR** 1 year, 8 months ago

**Selected Answer: A**

A. DC1

upvoted 1 times

🗨️ 👤 **ahmadano** 2 years, 11 months ago

A is correct

upvoted 2 times

🗨️ 👤 **Unitec** 3 years ago

Correcto

upvoted 3 times

🗨️ 👤 **AvoKikinha** 3 years, 1 month ago

**Selected Answer: A**

Correct!

upvoted 3 times

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains the objects shown in the following table.

Name	Type
User1	User
Group1	Universal security group
Group2	Domain local security group
Computer1	Computer

You plan to sync contoso.com with an Azure Active Directory (Azure AD) tenant by using Azure AD Connect.

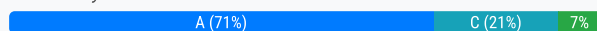
You need to ensure that all the objects can be used in Conditional Access policies.

What should you do?

- A. Select the Configure Hybrid Azure AD join option.
- B. Change the scope of Group1 and Group2 to Global.
- C. Clear the Configure device writeback option.
- D. Change the scope of Group2 to Universal.

**Correct Answer: A**

Community vote distribution



**edykss** Highly Voted 2 years, 9 months ago

Given answer is correct.

upvoted 11 times

**Itkiller** 4 months, 3 weeks ago

This one was tough!

Seen about 10 installations, none of them had the option,

the options comes AFTER you configured AD Connect, open it again to configure it. This will allow devices to be synced to Azure AD.

@13:08

<https://www.youtube.com/watch?v=ohFGjg7-cr4>

Domain Local groups are not synced, they are ignored, so it must be set to universal.

So yeah, 2 options here: whats worse, missing 1 group that may not be able to convert to Universal or all your devices, Go with A!

upvoted 1 times

**syu31svc** Highly Voted 2 years, 3 months ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-compliant-device>

Answer is A

upvoted 6 times

**e489b39** Most Recent 1 month ago

**Selected Answer: A**

To register computer 1

upvoted 1 times

**ScKn** 1 month, 3 weeks ago

**Selected Answer: D**

It should be the D

Azure AD Connect only syncs Universal groups from on-prem AD

Global and Domain Local groups are not synced unless they're Universal.



Conditional Access policies require groups to be available in Azure AD.

So, if Group2 is not Universal, it won't be in Azure AD – and therefore unusable in Conditional Access.

upvoted 1 times

🗨️ **monishhk** 11 months, 1 week ago

**Selected Answer: A**

This question is valid

Exam date - 27-07-2024

upvoted 2 times

🗨️ **boapaulo** 1 year, 7 months ago

Why do not D?

To ensure that all objects can be used in Conditional Access policies, you must change the scope from Group2 to Universal

Universal security groups can be used anywhere in the forest domain, and can include global users and groups from any domain in the forest.

Therefore, changing the scope of Group to Universal will allow it to be used in Conditional Access policies

Also, it's important to remember that to use Conditional Access, you need an Azure AD Premium license. Azure AD Premium licenses also include features that allow you to change passwords in the cloud and write the changes to your on-premises AD DS

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad>

<https://learn.microsoft.com/en-us/entra/identity/domain-services/tutorial-configure-password-hash-sync>

upvoted 1 times

🗨️ **fran199** 2 years, 1 month ago

**Selected Answer: A**

A... Given answer is correct.

upvoted 1 times

🗨️ **SuradjBajaj** 2 years, 4 months ago

Correct!

Hybrid Azure AD join needs to be configured to enable Computer1 to be used in Conditional Access Policies. Synchronized users, universal groups and domain local groups can be used in Conditional Access Policies.

upvoted 1 times

🗨️ **ant\_12** 2 years, 5 months ago

Hybrid Azure AD join Allows computer accounts in the on-premises AD DS forest to register with Azure AD. Configuring this option allows you to use features including conditional access in Azure.

Thomas, Orin. Exam Ref AZ-800 Administering Windows Server Hybrid Core Infrastructure (3570357) (p. 63). Pearson Education. Kindle Edition.

upvoted 5 times

🗨️ **Lu5ck** 2 years, 6 months ago

**Selected Answer: C**

The concept of "writeback" is "Azure-to-onPremises". Hybrid Azure join on the other hand is "onPremises-to-Azure". "Conditional access" is a azure feature, not available on premises. Thus, to access such feature, it has to be "azure-to-onPremise" aka writeback.

upvoted 3 times

🗨️ **Lu5ck** 2 years, 6 months ago

Reading it again, C say "<Clear> the Configure device writeback option" but we need to enable it. Therefore, A is the only sensible answer. sorry about this.

upvoted 9 times

🗨️ **[Removed]** 2 years, 8 months ago

I think the correct answer is C.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-options>

"Device writeback: Device writeback is used to enable Conditional Access based on devices to AD FS (2012 R2 or higher) protected devices"

<https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-device-based-conditional-access-on-premises>

"The following per-requisites are required before you can begin with on-premises conditional access.

To enable device write-back for on premises conditional access "

upvoted 4 times

Your network contains a multi-site Active Directory Domain Services (AD DS) forest. Each Active Directory site is connected by using manually configured site links and automatically generated connections.

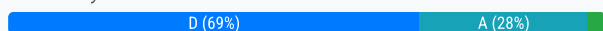
You need to minimize the convergence time for changes to Active Directory.

What should you do?

- A. For each site link, modify the replication schedule.
- B. For each site links, modify the site link costs.
- C. Create a site link bridge that contains all the site links.
- D. For each site link, modify the options attribute.

**Correct Answer: D**

Community vote distribution



**igymo** Highly Voted 2 years, 8 months ago

Correct Answer is D. when you configure manual site link replication schedule is already setup to 15 minute replication cycle you can not lower more down. so only option left is to change link site option attribute for use notify setting  
upvoted 13 times

**Rasto02** 9 months ago

the correct answer would be 'For each manually created connection object modify the options attribute.' to lower the replication interval, but it is NOT. (Then the only correct options left is A (which is 15 min replication interval)  
upvoted 1 times

**Judith1969** Most Recent 1 week, 4 days ago

**Selected Answer: A**

ChatGPT said it  
upvoted 1 times

**axelbest** 1 month, 1 week ago

**Selected Answer: A**

Change the replication schedule is the most straightforward answer.  
upvoted 2 times

**ScKn** 1 month, 3 weeks ago

**Selected Answer: A**

D is not the simplest or most effective method to reduce convergence time between sites  
upvoted 1 times

**Ahmedali70x** 2 months, 2 weeks ago

**Selected Answer: C**

C. Create a site link bridge that contains all the site links.

Site Link Bridges: Site link bridges allow for automatic replication between all sites by connecting site links in a transparent manner. This ensures that replication occurs in the most efficient manner, without needing to manually define replication paths for every possible connection.  
upvoted 1 times

**axelbest** 1 month, 1 week ago

Disagree.

Site link bridges are used when you have non-transitive IP connections between sites (e.g., spokes connected to a hub, but spokes can't directly communicate). By default, site link bridging is enabled and handles transitivity. You only manually create them in specific, complex scenarios. Creating a site link bridge generally doesn't directly minimize convergence time. It's more about ensuring connectivity and replication can occur across non-fully meshed networks. If your sites are already connected, a bridge won't necessarily speed up the replication process itself.  
upvoted 1 times

**atheerahmadd** 4 months, 1 week ago

**Selected Answer: D**

its definitely not A because its only control (WHEN) replication happens. but dose not reduce convergence time

upvoted 1 times

🗨️ **Midoria** 5 months, 2 weeks ago

**Selected Answer: A**

D. Modify the options attribute:

The options attribute is used for specific advanced configurations (e.g., enabling or disabling compression). It does not affect replication frequency or convergence time.

upvoted 1 times

🗨️ **stonwall12** 5 months, 4 weeks ago

**Selected Answer: D**

Answer: D, options attribute.

Modifying the options attribute for each site link will minimize Active Directory replication convergence time through optimizing inter-site replication settings.

upvoted 1 times

🗨️ **Rasto02** 9 months ago

**Selected Answer: A**

Correct is A.. D states: . For each site link, modify the options attribute. It clearly states 'site link', not 'manually created connection object'. Based on the link below, for InterSite replication relationship the 'options' attribute is not inherited down to connection objects (domain controller level). "if it's a manual connection object, it will NOT inherit the Options value from the Site Link object. You're going to have to enable change notifications directly on the manually created connection object".

upvoted 1 times

🗨️ **neilkraftmann** 10 months, 2 weeks ago

Had this on my exam recently.

upvoted 4 times

🗨️ **SIAMIANJI** 1 year, 1 month ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗨️ **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: D**

The "options" attribute in Active Directory site links controls how quickly changes to Active Directory are replicated between sites. By modifying the options attribute for each site link, you can minimize the convergence time for changes to Active Directory.

Specifically, you should enable the "Change Notification" option, which allows domain controllers to immediately notify each other of directory changes, significantly reducing replication latency. This option is particularly effective in multi-site environments where timely replication is essential.

Therefore, option D is the most appropriate choice for minimizing the convergence time for changes to Active Directory.

upvoted 3 times

🗨️ **SIAMIANJI** 1 year, 1 month ago

I was wrong. A is correct. To minimize the convergence you need to modify the replication schedule.

upvoted 1 times

🗨️ **MR\_Eliot** 1 year, 9 months ago

**Selected Answer: A**

"A" seems the most logical way to archive this. Microsoft looks for standard supported answers. Updating the "repInterval" attribute is too much work and doesn't even show correctly in GUI when using something less than 15 minutes, therefore "A" is correct.

upvoted 2 times

🗨️ **syu31svc** 2 years, 3 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/archive/blogs/canberrapfe/active-directory-replication-change-notification-you>

Answer is D

upvoted 3 times

🗨️ 👤 **haibo1738sipho** 2 years, 7 months ago

**Selected Answer: D**

You cannot lower the replication schedule further down when you configure manual site link replication. Therefore, the only option left is to change the link site option attribute to use notification

upvoted 2 times

🗨️ 👤 **Andre369** 2 years, 7 months ago

**Selected Answer: D**

D seems to be the correct answers

upvoted 2 times

🗨️ 👤 **Leocan** 2 years, 7 months ago

D is correct.

You can use either ADSIEDIT.msc or Active Directory Sites and Services console to edit the properties of the site link. For example, Sites->Inter-site Transports->IP->DEFAULTIPSITELINK->Properties->Attribute Editor->options->1 (0x1=USE\_NOTIFY)

upvoted 3 times

## DRAG DROP -

You deploy a single-domain Active Directory Domain Services (AD DS) forest named contoso.com.

You deploy five servers to the domain. You add the servers to a group named ITFarmHosts.

You plan to configure a Network Load Balancing (NLB) cluster named NLBcluster.contoso.com that will contain the five servers.

You need to ensure that the NLB service on the nodes of the cluster can use a group managed service account (gMSA) to authenticate.

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

Select and Place:

## Cmdlets

New-ADServiceAccount

Install-ADServiceAccount

Add-ADComputerServiceAccount

Set-KdsConfiguration

Add-KdsRootKey

Add-ADGroupMember

## Answer Area



Correct Answer:

## Cmdlets

Add-ADComputerServiceAccount

Set-KdsConfiguration

Add-ADGroupMember

## Answer Area

Add-KdsRootKey

New-ADServiceAccount

Install-ADServiceAccount



Reference:

<https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/create-the-key-distribution-services-kds-root-key>

<https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>

jecawi9630 Highly Voted 2 years ago

Correct.

several questions asked if different ways, come down to the same basic answer:

Add-kdsrootkey (on a domain controller; if it was never configured in the past)

Add-ADServiceAccount (on domain controller - specify a server name, with \$ at the end: servername\$ or a security group name)

Install-ADServiceAccount (on the server where gMSA account will be used, specify with the servername\$)

upvoted 9 times

Ciapek Highly Voted 2 years, 2 months ago

Answer is correct

First you must create a key (process takes circa 10 hours) and then you can create an account for gMSA. If KDS does not exist you get an error. Last command to execute is Install-ADServiceAccount

upvoted 8 times

Joedn Most Recent 7 months ago

Valid 05/28/2024

upvoted 1 times

boapaulo 1 year, 1 month ago

To ensure that the NLB service on the cluster nodes can use a Group Managed Service (gMSA) account to authenticate, you must run the following PowerShell cmdlets in sequence:

Add-KdsRootKey: This cmdlet is used to create a new root key for the Key Distribution Service. This key is required for the generation of group-managed service accounts.

New-ADServiceAccount: This cmdlet is used to create a new service account in Active Directory.

Add-ADComputerServiceAccount: This cmdlet is used to add a service account to a computer. In this case, you would add the service account you just created to the servers in the NLB cluster.

Please note that the cmdlets "Install-ADServiceAccount", "Set-KdsConfiguration" and "Add-ADGroupMember" are not required to meet the mentioned requirements.

upvoted 4 times

smol84 1 year, 9 months ago

the last step is set-adserviceaccount not install

upvoted 1 times

MR\_Eliot 1 year, 3 months ago

No, with create-adserviceaccount you can already give permissions to computers. This command is not needed anymore.

upvoted 1 times

syu31svc 1 year, 9 months ago

Before you can create a group Managed Service Account (gMSA), you need to create the first master root key for Active Directory. Then, you can create the gMSA using the New-ADServiceAccount cmdlet. Finally, you can test and cache the gMSA on each of the web servers using the Install-ADServiceAccount cmdlet.

Answer is correct

upvoted 6 times

You have an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant. You have several Windows 10 devices that are Azure AD hybrid-joined. You need to ensure that when users sign in to the devices, they can use Windows Hello for Business. Which optional feature should you select in Azure AD Connect?

- A. Device writeback
- B. Group writeback
- C. Azure AD app and attribute filtering
- D. Password writeback
- E. Directory extension attribute sync

**Correct Answer: A**

Community vote distribution

A (100%)

 **empee1977** Highly Voted 2 years, 4 months ago

**Selected Answer: A**

Device writeback is an optional feature in Azure AD Connect that allows the on-premises AD DS domain to receive information about the Azure AD joined devices, including the device registration state. By enabling this feature, you can ensure that the on-premises AD DS domain has information about the Azure AD joined devices, which is required for Windows Hello for Business to function correctly. Once this information is available in the on-premises AD DS domain, you can set the appropriate policies and configure the required infrastructure to support Windows Hello for Business.


upvoted 9 times

 **RMKA\_092** Highly Voted 2 years, 10 months ago

**Selected Answer: A**

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cert-trust-prereqs>

upvoted 5 times

 **xrisimix** 2 years, 9 months ago

Windows Hello for Business deployments need device writeback, which is an Azure Active Directory premium feature.

upvoted 4 times

 **stonwall12** Most Recent 5 months, 4 weeks ago

**Selected Answer: A**

Answer: A, Device Writeback

This feature allows Windows Hello for Business credentials to be synchronized between on-premises Active Directory and Azure AD, enabling hybrid authentication scenarios.

upvoted 1 times

 **CM\_81** 8 months, 2 weeks ago

I can safely say that device writeback is NOT required for WHfB to work with Azure AD hybrid joined machines. I'm running this in multiple client environments with only hybrid config.

upvoted 1 times

 **MR\_Eliot** 1 year, 9 months ago

**Selected Answer: A**

Correct Answer is "A".

Device registration

All devices included in the Windows Hello for Business deployment must go through device registration. Device registration enables devices to authenticate to identity providers. >> For cloud only and hybrid deployment, the identity provider is Azure Active Directory <<. For on-premises deployments, the identity provider is the on-premises server running the Windows Server 2016 Active Directory Federation Services (AD FS) role.

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-planning-guide#device-registration>



upvoted 1 times

🗄️ 👤 **JohnIII** 1 year, 11 months ago

**Selected Answer: A**

It needs to be A

upvoted 1 times

🗄️ 👤 **syu31svc** 2 years, 3 months ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

Answer is A

upvoted 1 times

🗄️ 👤 **smol84** 2 years, 3 months ago

The device writeback is correct!

upvoted 1 times

🗄️ 👤 **Duks** 2 years, 3 months ago

A - device writeback 100%

upvoted 1 times

🗄️ 👤 **Robert69** 2 years, 6 months ago

Looking at the provided link indeed: Hybrid certificate trust deployments need the device write back feature. Authentication to the Windows Server 2016 Active Directory Federation Services needs both the user and the computer to authenticate. Typically the users are synchronized, but not devices. This prevents AD FS from authenticating the computer and results in Windows Hello for Business certificate enrollment failures. For this reason, Windows Hello for Business deployments need device writeback, which is an Azure Active Directory premium feature.

upvoted 2 times

🗄️ 👤 **Vitu** 2 years, 6 months ago

Answer A:

Hybrid certificate trust deployments need the device write back feature. Authentication to the Windows Server 2016 Active Directory Federation Services needs both the user and the computer to authenticate. Typically the users are synchronized, but not devices. This prevents AD FS from authenticating the computer and results in Windows Hello for Business certificate enrollment failures. For this reason, Windows Hello for Business deployments need device writeback, which is an Azure Active Directory premium feature.

upvoted 2 times

🗄️ 👤 **Ciapek** 2 years, 9 months ago

**Selected Answer: A**

Answer is A

upvoted 2 times

🗄️ 👤 **Justin0020** 2 years, 9 months ago

**Selected Answer: A**

Answer is A, passwords does nothing have to do with Hello for Business

upvoted 3 times

🗄️ 👤 **ScarfaceRecords** 2 years, 9 months ago

**Selected Answer: A**

The hybrid-certificate trust deployment needs an Azure Active Directory premium subscription because it uses the device write-back synchronization feature.

upvoted 2 times

🗄️ 👤 **LOEG** 2 years, 10 months ago

Answer is A

upvoted 4 times

## HOTSPOT -

Your network contains an Active Directory Domain Services (AD DS) forest named contoso.com. The forest contains a child domain named east.contoso.com.

In the contoso.com domain, you create two users named Admin1 and Admin2.

You need to ensure that the users can perform the following tasks:

- ⇒ Admin1 can create and manage Active Directory sites.
- ⇒ Admin2 can deploy domain controllers to the east.contoso.com domain.

The solution must use the principle of least privilege.

To which group should you add each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Admin1: 

	▼
Contoso\Administrators	
Contoso\Domain Admins	
Contoso\Enterprise Admins	
East\Administrators	
East\Domain Admins	

Admin2: 

	▼
Contoso\Administrators	
Contoso\Domain Admins	
Contoso\Enterprise Admins	
East\Administrators	
East\Domain Admins	

## Answer Area

Correct Answer:

Admin1:  ▼

Contoso\Administrators
Contoso\Domain Admins
Contoso\Enterprise Admins
East\Administrators
East\Domain Admins

Admin2:  ▼

Contoso\Administrators
Contoso\Domain Admins
Contoso\Enterprise Admins
East\Administrators
East\Domain Admins

Reference:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/ras/multisite/configure/step-2-configure-the-multisite-infrastructure>

 **xrisimix** Highly Voted 2 years, 9 months ago

Correct

Membership in the Enterprise Admins group in the forest or the Domain Admins group in the forest root domain,  
upvoted 10 times

 **MR\_Eliot** Highly Voted 1 year, 9 months ago

Correct Answer:

Box1: Contoso\Domain Admins

-> Tested this, domain admin can manage sites & site links for the current domain & child domains.

Box2: Contoso\Enterprise Admins

-> Tested this, domain admin cannot enroll domain controllers to child domains. You will need to be an enterprise admin.

-> Also, admin 2 user is not a user in child domain, so therefore you will still need to make admin 2 a member of "Contoso\Enterprise Admins" group.  
upvoted 8 times

 **ppardav** Most Recent 1 month, 1 week ago

Admin1) User1 should be member of contoso\domain admins in order to manage sites in both domains

Admin2) Should be member of Enterprise Admins in order to deploy domain controllers in child domain.

User1 and User2 are member of contoso domain and east\domain admins is a global group so can't add members from other domains

upvoted 1 times

 **jpcapobianco** 3 months, 2 weeks ago

the question is badly formulated because it says that user1 and user2 are on contoso.com, in reality user2 should be on east.contoso.com. if both groups are on contoso.com then you would need a universal group on east.contoso.com with user2 inside to then use it for the DELEGATE CONTROL function.

upvoted 2 times

 **KXNG** 7 months, 2 weeks ago

Clarification:

Admin 1 can be part of the contoso\domain admin group as the user was created in the forest root domain and using least privilege does not need to be in the enterprise admin group.

Admin 2 as per the question was created in the forest root domain contoso.com and not in the child domain. The question also states that admin 2 must deploy domain controllers TO the child domain, meaning that admin 2 is still in contoso.com. To enable admin 2 to be able to carry out this task, admin 2 would need to be in the enterprise admin group

upvoted 3 times

🗨️ 👤 **monisshk** 11 months, 1 week ago

This question is valid

Exam date - 27-07-2024

upvoted 2 times

🗨️ 👤 **sardonique** 11 months, 2 weeks ago

east\domain admins is able to modify the settings on the east.contoso.com domain, however has no rights whatsoever on the contoso domain. When you add a domain controller on the child domain, you still need enough rights to do that on the parent domain, so I would say that the least privilege needed is contoso\domain admins for both

upvoted 5 times

🗨️ 👤 **Vallion** 1 year, 2 months ago

To create domain controllers in the east.contoso domain, an admin from the contoso domain would need to be a member of the "Administrators" domain local group in the east.contoso domain(1). This can be achieved by placing the users from the contoso domain into a global group in the contoso domain, then nesting that global group into the "Administrators" domain local group in the east.contoso domain1.

This adheres to the Principle of Least Privilege (PoLP) because it grants only the necessary permissions to create domain controllers in the east.contoso domain, without granting excessive privileges.

upvoted 2 times

🗨️ 👤 **Vallion** 1 year, 2 months ago

Here's why other closely related groups are not correct:

Domain Admins: The Domain Admins group in the contoso domain does not have default rights on domain controllers in the east.contoso domain(2). Also, adding the admin to the Domain Admins group of east.contoso would grant them more permissions than necessary, violating the PoLP.

Enterprise Admins: The Enterprise Admins group has full admin rights across all domains in the forest(3). However, this would grant the admin excessive privileges across all domains, not just east.contoso, which again violates the PoLP(2).

Therefore, membership in the "Administrators" domain local group in the east.contoso domain is the most appropriate and least privilege solution. It provides the necessary rights to create domain controllers in the east.contoso domain, without granting excessive privileges in other areas.

upvoted 1 times

🗨️ 👤 **Vallion** 1 year, 2 months ago

1: <https://serverfault.com/questions/38268/granting-domain-admins-rights-to-parent-domain-members>

2: <https://serverfault.com/questions/943769/enterprise-admins-dont-have-admin-permissions-in-child-domain>

3: <https://serverfault.com/questions/1080567/parent-domain-vs-child-domain>

Extra info

<https://www.dispersednet.com/active-directory/module4/create-child-domain.php>

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory>

upvoted 1 times

🗨️ 👤 **Vallion** 1 year, 2 months ago

Info gathered using co-pilot business, may contain some errors, check yourself like im doing now, never assume anything you read here is correct

upvoted 1 times

🗨️ 👤 **sardonique** 1 year, 2 months ago

In this scenario there is 1 single forest. Domain Admins is more than enough to create sites within the root domain. John needs to be enterprise admin to create a site in east.contoso.com which is outside the boundaries of contoso.com

upvoted 1 times

🗨️ 👤 **nonoelptirobo** 4 months, 2 weeks ago

there is a trust relationship between parent and child domains

hence east.contoso.com is within boundaries of contoso.com

the least privilege option for admin 2 is "create domains ONLY in east.contoso.com"

the east/domain admin allow to join DC in the child domain without giving admin privileges in the main contoso.com domain

upvoted 1 times

🗨️ 👤 **boapaulo** 1 year, 7 months ago

Why not, Enterprise Admins?

It's important to follow the principle of least privilege when assigning permissions. This helps to minimize the potential for damage if an account is compromised.

To ensure that users can perform the tasks mentioned, you must add each user to the following group:

Admin1: You must add Admin1 to the ContosoEnterprise Admins group. This group has permissions to create and manage Active Directory sites throughout the forest.

Admin2: You must add Admin2 to the EastDomain Admins group. This group has permissions to deploy domain controllers in the east.contoso.com domain.

Just a doubt, these questions of the test are quite confusing.

upvoted 4 times

🗨️ 👤 **boapaulo** 1 year, 7 months ago

\* I remind you that it's just a doubt, these questions of the test are quite confusing.

upvoted 1 times

🗨️ 👤 **Dools** 1 year, 7 months ago

In the context of Active Directory, Enterprise Admin privileges are generally not required to create domain controllers in a child domain. Enterprise Admins have higher-level permissions that extend across all domains in the forest, including the ability to manage trusts and make changes that affect the entire forest.

Domain Admins, on the other hand, have the necessary permissions to manage and administer objects within their specific domain, including the ability to promote domain controllers within that domain. This includes the creation of domain controllers in child domains.

While Enterprise Admins can perform tasks related to the entire forest, such as managing trusts between domains, they are not explicitly required for the creation of domain controllers in a child domain. The Domain Admin role is typically sufficient for these tasks within the scope of a specific domain.

However, it's essential to consider the principle of least privilege when assigning permissions. If a user or group only needs to perform tasks within a specific domain, granting Domain Admin privileges for that domain is more appropriate than assigning higher-level Enterprise Admin privileges that provide broader access across the entire forest.

upvoted 2 times

🗨️ 👤 **sardonique** 1 year, 2 months ago

read the question carefully, Admin1 needs to be able to add sites on all the domains. Domain Admins cannot go beyond the boundaries of the domain.

upvoted 2 times

🗨️ 👤 **deepg1981** 2 years ago

admin2 is user of root domain, however answer is wrong. how it can be added in child domain as domain admin

upvoted 1 times

🗨️ 👤 **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 2 times

🗨️ 👤 **syu31svc** 2 years, 3 months ago

Answer is correct

Enterprise admin is a higher level than Domain admin

upvoted 2 times

🗨️ 👤 **smol84** 2 years, 3 months ago

Incorrect for both demo\domain admins Domain admins have full admin controllers you can manage AD sites as well as DCs with this permission.

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an Active Directory Domain Services (AD DS) forest. The forest contains three Active Directory sites named Site1, Site2, and Site3. Each site contains two domain controllers. The sites are connected by using DEFAULTIPSITELINK.

You open a new branch office that contains only client computers.

You need to ensure that the client computers in the new office are primarily authenticated by the domain controllers in Site1.

Solution: You create an organization unit (OU) that contains the client computers in the branch office. You configure the Try Next Closest Site Group Policy Object

(GPO) setting in a GPO that is linked to the new OU.

Does this meet the goal?



A. Yes

B. No

**Correct Answer: B**

Community vote distribution

B (100%)

 **smudo1965**  2 years, 8 months ago

As stated in the link provided by Jaybro:



If you enable the Try Next Closest Site setting, DC Locator uses the following algorithm to locate a domain controller:

Try to find a domain controller in the same site.

If no domain controller is available in the same site, try to find a domain controller in the next closest site. A site is closer if it has a lower site-link cost than another site with a higher site-link cost.

If no domain controller is available in the next closest site, try to find any domain controller in the domain.

As there is no different sitelink cost this will not help - so No  
upvoted 9 times

 **neilkraftmann**  10 months, 2 weeks ago

Had this on my exam recently.


upvoted 2 times

 **syu31svc** 2 years, 3 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/enabling-clients-to-locate-the-next-closest-domain-controller>

Only one site link so answer is No  
upvoted 4 times

 **phi3nix** 2 years, 2 months ago

This is a very good link:

By default, the Try Next Closest Site setting is not enabled. When the setting is not enabled, DC Locator uses the following algorithm to locate a domain controller:

\* Try to find a domain controller in the same site.

\* If no domain controller is available in the same site, try to find any domain controller in the domain.

If you enable the Try Next Closest Site setting, DC Locator uses the following algorithm to locate a domain controller:

Try to find a domain controller in the same site.

If no domain controller is available in the same site, try to find a domain controller in the next closest site. A site is closer if it has a lower site-link cost than another site with a higher site-link cost.

If no domain controller is available in the next closest site, try to find any domain controller in the domain.

To GPO works you still need to create links... Answer is NO.

upvoted 3 times

  **lukiduc9625** 2 years, 9 months ago

In my opinion suggested answer is correct.

1. Computers from new branch office will be located in subnet which is not configured in AD (there is no information about configuring new subnet in AD) so they can not recognize to which site they belong thus they can not recognize which site is closest.
2. Enabling Try Next Closest Site Group Policy Object cause that if DC Locator running on certain client does not find domain controller (DC) in same site he try to find DC in closest site - which site is closer than others? Site to which site-link has lower cost. In our case all sites are connected by ONE site-link named DEFAULTIPSITELINK thus there is no way to choose which one is closest and in my opinion DC Locator will use evenly DCs from Site1, Site2 and Site3

upvoted 3 times

  **xrisimix** 2 years, 9 months ago

A is correct answer

If you have a domain controller that runs Windows Server 2008 or newer, you can make it possible for client computers that run Windows Vista or newer or Windows Server 2008 or newer to locate domain controllers more efficiently by enabling the Try Next Closest Site Group Policy setting. This setting improves the Domain Controller Locator (DC Locator) by helping to streamline network traffic, especially in large enterprises that have many branch offices and sites.

upvoted 3 times

  **Rel2002** 2 years, 9 months ago

Its a tricky question. The question is repeated in q18 of this topid where it says that the gpo has connected to site 1. So thats definetaly a No.

But I am affraid this one is wrong too.. because it says that all sites uses the DefaultIPSitelink.. so there are no different sitelink costs so this gpo setting still will take a random DC. So I am doubting.. any guru out there ☺

upvoted 2 times

  **rimvydukas** 2 years, 8 months ago

Rel2002, you are right. Correct answer is B. There is only one site link. And for the GPO setting to work correctly we need several site links. Algoryth is the following:

If you enable the Try Next Closest Site setting, DC Locator uses the following algorithm to locate a domain controller:

Try to find a domain controller in the same site.

If no domain controller is available in the same site, try to find a domain controller in the next closest site. A site is closer if it has a lower site-link cost than another site with a higher site-link cost.

If no domain controller is available in the next closest site, try to find any domain controller in the domain.

upvoted 1 times

  **Jaybro** 2 years, 10 months ago

Looks ok. See <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/enabling-clients-to-locate-the-next-closest-domain-controller>

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an Active Directory Domain Services (AD DS) forest. The forest contains three Active Directory sites named Site1, Site2, and Site3. Each site contains two domain controllers. The sites are connected by using DEFAULTIPSITELINK.

You open a new branch office that contains only client computers.

You need to ensure that the client computers in the new office are primarily authenticated by the domain controllers in Site1.

Solution: You create a new site named Site4 and associate Site4 to DEFAULTSITELINK.

Does this meet the goal?



A. Yes

B. No

**Correct Answer: B**

Community vote distribution

B (100%)

  **Techbiz** 11 months, 2 weeks ago

Yeah I support your proposals

upvoted 1 times



  **syu31svc** 1 year, 3 months ago

**Selected Answer: B**

Still the same site link so it wouldn't make any difference

Answer is No

upvoted 2 times

  **Leocan** 1 year, 7 months ago

**Selected Answer: B**

Unless a new site link between site4 and site 1 is created at a lower cost.

upvoted 4 times



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an Active Directory Domain Services (AD DS) forest. The forest contains three Active Directory sites named Site1, Site2, and Site3. Each site contains two domain controllers. The sites are connected by using DEFAULTIPSITELINK.

You open a new branch office that contains only client computers.

You need to ensure that the client computers in the new office are primarily authenticated by the domain controllers in Site1.

Solution: You configure the Try Next Closest Site Group Policy Object (GPO) setting in a GPO that is linked to Site1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

Community vote distribution

B (82%)

A (18%)

 **empee1977** Highly Voted 11 months, 1 week ago

No,

Configuring the Try Next Closest Site Group Policy Object (GPO) setting in a GPO that is linked to Site1 will not ensure that the client computers in the new office are primarily authenticated by the domain controllers in Site1.

The Try Next Closest Site GPO setting controls how a client computer attempts to locate a domain controller if it is unable to locate one in its own site. It causes the client to try to find a domain controller in the next closest site, rather than trying to authenticate with a domain controller in a remote site.

To achieve the goal of ensuring that the client computers in the new office are primarily authenticated by the domain controllers in Site1, you would need to configure the site link and site link costs between Site1 and the new office site so that the new office site has a higher cost to communicate with other sites than Site1. This way, the clients will prefer to authenticate with the domain controllers in Site1.

upvoted 12 times

 **syu31svc** Most Recent 9 months, 1 week ago

**Selected Answer: B**

Still on the same site link so answer is No

upvoted 2 times

 **LemonBana** 10 months, 2 weeks ago

**Selected Answer: B**

See the correct explanation in Q #26.

upvoted 3 times

 **[Removed]** 11 months ago

it does meet the goal the answer is A.

upvoted 2 times

 **SwissGuy** 12 months ago

See the correct explanation in Q #26.

upvoted 1 times

 **SwissGuy** 12 months ago

I don't think this meets the goal. The new branch office almost certainly has a different subnet to any of those defined in Sites 1, 2 or 3. There's no mention of adding that new subnet to Site 1 nor any other site. The GPO is linked to Site 1, so only affects clients in Site 1.

"You open a new branch office that contains only client computers.

You need to ensure that the client computers in the new office are primarily authenticated by the domain controllers in Site1".

Solution: You configure the Try Next Closest Site Group Policy Object (GPO) setting in a GPO that is linked to Site1.

The documentation linked by joehoesofat gives the example of adding the GPO setting to the Default Domain Policy (bad practice imho) or

creating/linking a new GPO at domain level. If offered, this option would be the answer.

So, No, B in my opinion. Doesn't meet the goal. But the question is badly written.

upvoted 2 times


  **Lu5ck** 1 year ago

**Selected Answer: B**

The sites are all using the same site link which means they are of the same cost. There is no way to differentiate which site is nearer or further when the cost are the same.

The only way for these computers to see site1 as their primary DC is for these computers to be placed in the same site as site1. This is done so via subnet.


upvoted 4 times

  **Burnie** 1 year, 1 month ago

**Selected Answer: A**

This does meet the goal <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/enabling-clients-to-locate-the-next-closest-domain-controller> - keeps the request in the same site1

upvoted 2 times

  **Benjam** 1 year, 1 month ago

Looks Like A is the correct answer

upvoted 1 times

  **joehoesofat** 1 year, 2 months ago

This does meet the goal <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/enabling-clients-to-locate-the-next-closest-domain-controller> - keeps the request in the same site1

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com.

You need to identify which server is the PDC emulator for the domain.

Solution: From Active Directory Sites and Services, you right-click Default-First-Site-Name in the console tree, and then select Properties.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

Community vote distribution

B (100%)

  **Arpan\_kumar\_roy**  3 years, 1 month ago

Correct.

1. Go to Active directory users and computers.
2. Right click on the Domain.
3. Select Operation masters.
4. select PDC tab.

upvoted 16 times

  **e489b39** 1 month ago

read Active Directory Sites and Services

upvoted 1 times

  **Andre369** 2 years, 8 months ago

Is the answer A -yes or B -no

upvoted 1 times

  **phi3nix** 2 years, 1 month ago

The answer is A.

upvoted 1 times

  **VinoTee**  3 years, 2 months ago

Correct.

Here are the steps below:

1. Right-click on the domain
2. Click Operations Masters
3. Click the PDC tab to view the server holding the PDC master role

upvoted 7 times

  **HeavyNuts** 2 years, 7 months ago

This would work in ADUC but not in site and Services.

upvoted 3 times

  **SDK76**  2 months, 2 weeks ago

**Selected Answer: B**

ps:

Get-ADDomain | Select-Object InfrastructureMaster, PDCEmulator, RIDMaster | Format-List

Get-ADForest | Select-Object DomainNamingMaster, SchemaMaster | Format-List

upvoted 1 times

  **Krayzr** 11 months, 1 week ago

**Selected Answer: B**

Topic 5 Question 24

Same question

upvoted 1 times

🗨️ 👤 **NazerRazer** 1 year, 8 months ago

The solution provided does not meet the goal.

Here's how to do it using Active Directory Users and Computers:

1. Open "Active Directory Users and Computers."
2. In the left pane, expand the domain tree
3. Right-click on the domain and select "Operations Masters."
4. In the "Operations Master" dialog, go to the "PDC" tab. This tab will display the current PDC emulator for the domain.

upvoted 3 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

**Selected Answer: B**

Correct Answer: B, no explanation needed.

upvoted 4 times

🗨️ 👤 **syu31svc** 2 years, 3 months ago

**Selected Answer: B**

It's not Active Directory Domains and Trusts but Active Directory Users and Computers

Answer is No

upvoted 2 times

🗨️ 👤 **Fakecon** 2 years, 3 months ago

2 forest masters are:

Name

Schema

3 domain masters are:

RID

Infrastructure

PDC

upvoted 2 times

🗨️ 👤 **BryRob** 2 years, 6 months ago

**Selected Answer: B**

Tried this to the server so its B

upvoted 1 times

🗨️ 👤 **GuillaumeT** 2 years, 8 months ago

Checked on my personal AD, i found nothing in properties.

Correct answer is B

upvoted 2 times

🗨️ 👤 **Contactfornitish** 2 years, 10 months ago

Still valid, in exam on 23 Aug'22

upvoted 2 times

🗨️ 👤 **nefaxto** 3 years, 1 month ago

**Selected Answer: B**

B is correct

upvoted 3 times

Your network contains a single-domain Active Directory Domain Services (AD DS) forest named contoso.com. The forest contains the servers shown in the following exhibit table.

Name	Description
DC1	Domain controller
Server1	Member server

You plan to install a line-of-business (LOB) application on Server1. The application will install a custom Windows service.

A new corporate security policy states that all custom Windows services must run under the context of a group managed service account (gMSA).

You deploy a root key.

You need to create, configure, and install the gMSA that will be used by the new application.

Which two actions should you perform? Each correct answer presents part of the solution.



NOTE: Each correct selection is worth one point

- A. On Server1, run the setspn command.
- B. On DC1, run the New-ADServiceAccount cmdlet.
- C. On Server1, run the Install-ADServiceAccount cmdlet.
- D. On Server1, run the Get-ADServiceAccount cmdlet.
- E. On DC1, run the Set-ADComputer cmdlet.
- F. On DC1, run the Install-ADServiceAccount cmdlet.

**Correct Answer:** BC

Community vote distribution



BC (97%)

 **JohnO1971**  2 years, 8 months ago

**Selected Answer:** BC

BC are the correct answers

upvoted 19 times

 **lukiduc9625**  2 years, 9 months ago

There is something wrong in answer for this question. In my opinion most suitable 2 action from given possibilities are:

1. On DC1, run the New-ADServiceAccount cmdlet
2. On Server1, run the Install-ADServiceAccount cmdlet

Answer E (On DC1, run the Set-ADComputer cmdlet) does not help in configuration of gMSA at all. Maybe in original question answer E has form: "On DC1, run the Set-ADServiceAccount cmdlet" but without running Install-ADServiceAccount cmdlet gMSA will not be installed

upvoted 15 times

 **Midoria**  5 months, 2 weeks ago

**Selected Answer:** BC

B. On DC1, run the New-ADServiceAccount cmdlet:

This command is used to create a new group managed service account (gMSA) in Active Directory.

It is the first step to define the gMSA in the domain, associating it with the necessary servers or services.

C. On Server1, run the Install-ADServiceAccount cmdlet:

Once the gMSA is created, you need to install it on the server (Server1) where the application and custom service will run.

This command ensures that the gMSA is installed and ready for use by the custom Windows service.

upvoted 3 times

🗨️ 👤 **monisshk** 11 months, 1 week ago

**Selected Answer: BC**

This question is valid

Exam date - 27-07-2024

upvoted 2 times

🗨️ 👤 **SIAMIANJI** 1 year, 2 months ago

B, C

To create, configure, and install the Group Managed Service Account (gMSA) for the new application on Server1, you should perform the following actions:

B. On DC1, run the New-ADServiceAccount cmdlet.

This cmdlet creates a new gMSA account in Active Directory.

C. On Server1, run the Install-ADServiceAccount cmdlet.

This cmdlet installs the gMSA on Server1, allowing it to be used by the new application.

Therefore, the correct actions to perform are:

B. On DC1, run the New-ADServiceAccount cmdlet.

C. On Server1, run the Install-ADServiceAccount cmdlet.

These actions will create and install the gMSA on Server1, ensuring that the custom Windows service for the LOB application can run under the context of the gMSA as required by the corporate security policy.

upvoted 2 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

Correct Answers:

B & C

A. On Server1, run the setspn command.

->[incorrect] not needed

B. On DC1, run the New-ADServiceAccount cmdlet.

->[correct] This is the command which will create the service account, and allow specified domain computer, access the gMSA password.

C. On Server1, run the Install-ADServiceAccount cmdlet.

->[Correct] This is the command, used to install the gMSA on the member server, where we will use the gMSA account.

D. On Server1, run the Get-ADServiceAccount cmdlet.

->[incorrect] Returns the gMSA account, does nothing else.

E. On DC1, run the Set-ADComputer cmdlet.

->[incorrect] Not needed, command in "B" is enough. This is command is used when you need to change the configuration. In this case not required.

F. On DC1, run the Install-ADServiceAccount cmdlet.

->[incorrect] this command should be used on the domain server, where the service account is going to be used.

Explanation video:

<https://www.youtube.com/watch?v=ZS4vufyKEHo>

upvoted 5 times

🗨️ 👤 **MondherBB** 1 year, 11 months ago

Solution :

B & C:

Expl:

normally, we should do the below 3 actions:

1- New-ADServiceAccount with parameters like name, description, and so....

2- Add-ADComputerServiceAccount on DC (to add the service account to the computer Object Server1)

3- Add Powershell Module "ActiveDirectory" to Server1 (because it is not DC)

3- Install-ADServiceAccount on Server1

<https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>

upvoted 4 times

🗨️ 👤 **pewpewvx** 2 years, 2 months ago

**Selected Answer: BC**

B & C are correct. Account needs to be added, and then installed on the server that will use it.

upvoted 1 times

  **syu31svc** 2 years, 3 months ago

**Selected Answer: BC**

Options A, D & E don't make sense so that leaves B, C & E

"on server1" so B and C are the answers



upvoted 2 times

  **Duks** 2 years, 3 months ago

**Selected Answer: BC**

BC are correct

upvoted 1 times

  **LauLauLauw** 2 years, 3 months ago

**Selected Answer: BC**



Difference between gMSA and MSA is that it's targeted on the group instead of the computer account.

Since we can only give two answers we need to presume that Server1 is already in a group.

B is to create the gMSA

C is to install it on Server1



upvoted 3 times

  **Telekon** 2 years, 4 months ago

**Selected Answer: BE**

Set-adserviceaccount used for gMSA, install-adserviceaccount for MSA

upvoted 1 times

  **empee1977** 2 years, 5 months ago

BC:

To create, configure, and install the gMSA that will be used by the new application, you will need to perform the following actions:

Create a new group managed service account (gMSA) by using the PowerShell cmdlet "New-ADServiceAccount -Name <gMSA\_Name> -DNSHostName <gMSA\_FQDN> -PrincipalsAllowedToRetrieveManagedPassword <Server1>"

This cmdlet creates a new gMSA with a specific name and DNS hostname, and specifies the Server1 as the computer allowed to retrieve the managed password.



Install the gMSA on the Server1 by using the PowerShell cmdlet "Install-ADServiceAccount -Identity <gMSA\_Name>"

This cmdlet installs the gMSA on the Server1, allowing the custom Windows service to use the gMSA to authenticate.

These two actions will create and configure the gMSA that will be used by the new application, and install it on the Server1 so that the custom Windows service can use it for authentication.

It's important to note that the gMSA should be installed before installing the LOB application.

upvoted 4 times

  **Robert69** 2 years, 6 months ago


We need to: create, configure, and install the gMSA that will be used by the new application.

The Set-ADComputer cmdlet modifies the properties of an Active Directory computer object.

Install-ADServiceAccount Reference Feedback Module: ActiveDirectory Installs an Active Directory managed service account on a computer or caches a group managed service account on a computer.

So from the link provided the answer is B, C

upvoted 4 times

  **Vitu** 2 years, 6 months ago

B and E is correct, please see: <https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>

From link Microsoft:

New-ADServiceAccount ITFarm1 -DNSHostName ITFarm1.contoso.com -PrincipalsAllowedToRetrieveManagedPassword ITFarmHosts\$ -KerberosEncryptionType RC4, AES128, AES256 -ServicePrincipalNames http/ITFarm1.contoso.com/contoso.com, http/ITFarm1.contoso.com/contoso, http/ITFarm1/contoso.com, http/ITFarm1/contoso

Set-ADServiceAccount [-Identity] ITFarm1 -PrincipalsAllowedToRetrieveManagedPassword Host1\$,Host2\$,Host3\$



upvoted 2 times

  **jecawi9630** 2 years, 6 months ago

**Selected Answer: BC**

B C sent to be the correct options here

upvoted 3 times

  **sloky** 2 years, 7 months ago

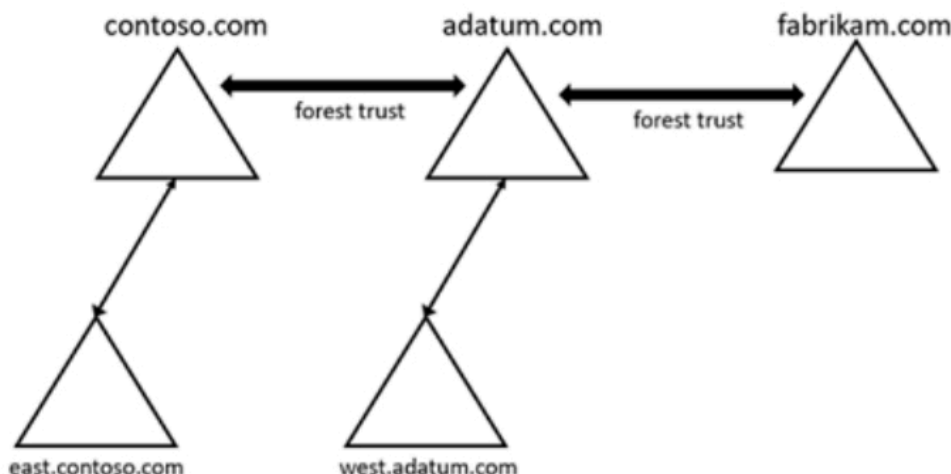
B and C

upvoted 2 times



## HOTSPOT -

Your network contains three Active Directory Domain Services (AD DS) forests as shown in the following exhibit.



The network contains the users shown in the following table.

Name	Domain
User1	east.contoso.com
User2	fabrikam.com

The network contains the security groups shown in the following table.

Name	Type	Domain
Group1	Domain local	west.adatum.com
Group2	Universal	contoso.com
Group3	Universal	east.contoso.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

You can add User1 to Group1.

Yes

☐

No

☐

You can add User2 to Group3.

☐
☐

You can grant Group2 permissions to the resources in the fabrikam.com domain.

☐
☐

Correct Answer:

#### Answer Area

##### Statements

You can add User1 to Group1.

Yes

☒

No

☐

You can add User2 to Group3.

☐
☒

You can grant Group2 permissions to the resources in the fabrikam.com domain.

☒
☐

Box 1: Yes -




User1 is in east.contoso.com. Group1 is Domain Local group in west.adutm.com.

Accounts from any domain or any trusted domain Global groups from any domain or any trusted domain can be members of Domain Local groups.

Accounts, Global groups, and Universal groups from other forests and from external domains can also be members of Domain Local groups.

Box 2: No -  
User2 is in the fabrikam.com domain.  
Group3 is a Universal group in east.contoso.com.  
Only accounts from any domain in the same forest can be added as members.

Box 3: Yes -  
Group2 is a Universal group in contoso.com.  
Group2 can grant permissions On any domain in the same forest or trusting forests.  
Active Directory Domain Services add to Domain Local group.  
Reference:  
<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups>

  **Lu5ck**  2 years ago

This is about trust.  
Contoso <-> Adatum <-> Fabrikam

User1 is from Contoso  
Group1 is from Adatum  
Both forests trusted each other, so Yes.

User2 is from Fabrikam  
Group2 is from Contoso  
Both forests don't trust each other, so No.  
Transitive trust is only applicable to domain under the said forest.

Group2 is from Contoso  
Fabrikam is another forest  
Both forests don't trust each other, so No.  
Transitive trust is only applicable to domain under the said forest.

Yes  
No  
No  
upvoted 30 times

  **RickySmith** 12 months ago

Yes  
Accounts from any domain or any trusted domain  
[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255\(v=ws.11\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255(v=ws.11)?redirectedfrom=MSDN)

No  
Accounts from any domain in the same forest.  
[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255\(v=ws.11\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255(v=ws.11)?redirectedfrom=MSDN)

N  
Forest trusts can only be created between two forests and can't be implicitly extended to a third forest.  
<https://learn.microsoft.com/en-us/entra/identity/domain-services/concepts-forest-trust#forest-trusts>  
upvoted 3 times

  **DesolateMarauder** 2 years ago

All Forests trust each other, look at the links I provided below. I'm testing here in a few hours...  
upvoted 3 times

  **Lu5ck** 2 years ago

No. Transitive trust is only applicable to domains under the said forest. What this means is that Contoso will trust Adatum and all the domains part of Adatum. However, Contoso will not trust Fabrikam because Fabrikam is not part of Adatum. Trusts between forests are required to be

made explicitly.

upvoted 11 times

  **DesolateMarauder** Highly Voted 2 years ago

Yes - Domain Local

Possible Members: Accounts from any domain or any trusted domain

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255\(v=ws.11\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255(v=ws.11)?redirectedfrom=MSDN)

No - Universal

Possible Members: Accounts from any domain in the same forest.


[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255\(v=ws.11\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255(v=ws.11)?redirectedfrom=MSDN)

Yes - Universal

Permissions: On any domain in the same forest or trusting forests

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255\(v=ws.11\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579255(v=ws.11)?redirectedfrom=MSDN)

upvoted 10 times

  **Opoveda** Most Recent 3 months, 1 week ago

I think is Y N N

upvoted 1 times

  **MR\_Eliot** 1 year, 3 months ago

Correct Answer:

YES:

-> User 1 can be added, because it is a domain local. In a domain local you can add users from current forest and other forests (I have tested this).


NO:

-> User 1 can not be a group member of "group3", because Group3 is a Universal group. In a Universal group you can only add Root en child domain users (I have tested this).

YES:

-> "Group3" is a universal group, which can be used to assign permissions in another forest. Only domain local groups cannot be assigned (I have tested this).

upvoted 1 times

  **MR\_Eliot** 1 year, 3 months ago

After further investigation, correct answer is: YES, NO, NO

upvoted 2 times

  **Returnerwesley** 1 year, 6 months ago

Yes, no, yes should be correct

upvoted 1 times

  **Gore** 1 year, 8 months ago


Yes

No

No

<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust>

upvoted 4 times

  **syu31svc** 1 year, 9 months ago

<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust#forest-trusts>



Forest trusts can only be created between two forests and can't be implicitly extended to a third forest

Yes

No

No

upvoted 5 times

  **BryRob** 1 year, 11 months ago

For me this is  
Yes (had forest trust)  
No (had forest trust)  
No (no forest trust between contoso.com and fabrikam.com)  
upvoted 3 times

🗨️ 👤 **BryRob** 1 year, 11 months ago  
Correction  
Yes (had forest trust)  
No ((no forest trust between contoso.com and fabrikam.com)  
No (no forest trust between contoso.com and fabrikam.com)  
upvoted 2 times

🗨️ 👤 **muzet112** 2 years ago  
All domain trusts in an AD DS forest are two-way, transitive trusts. When a new child domain is created, a two-way, transitive trust is automatically created between the new child domain and the parent domain  
upvoted 2 times

🗨️ 👤 **Kurko** 2 years, 1 month ago  
Yes, No, No  
Forest trusts can only be created between two forests and can't be implicitly extended to a third forest.  
<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust#forest-trusts>  
upvoted 4 times

🗨️ 👤 **kijken** 2 years, 2 months ago  
I would say yes,yes,yes  
I think if that is not the case it has to be yes,no, no  
b and c are going though 2 trusts. So it works for both or it does not work for both cases  
upvoted 1 times

🗨️ 👤 **kijken** 2 years, 2 months ago  
After more investigation I know the answer is yes no no:  
Explicit trusts are also used to enable authentication across forests. When a forest trust is created, a transitive trust is created between the forest root domains in both forests. This allows all the members in the forest to exchange authentication information with the other forest. The forest trust is also called an explicit trust between the two forests. If an additional forest trust is created between one of the original forests and a third forest, an implicit trust with the other original forest is not established to the third forest. In order for the third forest to have a trust relationship with the other forest, an explicit forest trust must be created between the two  
<https://www.sciencedirect.com/topics/computer-science/transitive-trust#:~:text=A%20forest%20trust%20is%20also,use%20resources%20in%20the%20other.>  
upvoted 6 times

🗨️ 👤 **GeertVanAssen** 2 years, 2 months ago  
edit: the explanation of the second question can you assign user two to group3? actually moves on the same presumption. You cannot assign the user to this group because they aren't in the same forest, implying that there is no trust between the contoso and fabrikam root domain forests  
upvoted 1 times

🗨️ 👤 **GeertVanAssen** 2 years, 2 months ago  
I dont think the last answer is correct. First off the question doesn't make explicit whether these are transitive or non-transitive trusts and one way or two way. Whatever may be the case, transitivity on a forest level does not span multiple forest like it does for multidomain trees. So if A establishes a forest trust with B, and B does the same with C, there should not be any trust or relationship between Forest A and C. Unfortunately my source is behind a paywall: <https://www.skillpipe.com/#/reader/urn:uuid:dfd3a70a-25b7-5262-b225-a862fec9817c@2022-01-18T21:50:42Z/content>  
upvoted 1 times

🗨️ 👤 **edykss** 2 years, 3 months ago  
Seems correct.  
upvoted 2 times

Your network contains an Active Directory Domain Services (AD DS) forest named contoso.com. The forest root domain contains a server named server1.contoso.com.

A two-way forest trust exists between the contoso.com forest and an AD DS forest named fabrikam.com. The fabrikam.com forest contains 10 child domains.

You need to ensure that only the members of a group named fabrikam\Group1 can authenticate to server1.contoso.com.

What should you do first?

- A. Add fabrikam\Group1 to the local Users group on server1.contoso.com.
- B. Enable SID filtering for the trust.
- C. Enable Selective authentication for the trust.
- D. Change the trust to a one-way external trust.

**Correct Answer: C**

Community vote distribution

C (100%)

  **empee1977**  2 years, 4 months ago

**Selected Answer: C**

Selective authentication is a feature that allows administrators to control which users from a trusted domain can access resources in a trusting domain. To meet your requirement of allowing only members of fabrikam\Group1 to authenticate to server1.contoso.com, you would need to enable selective authentication for the trust between contoso.com and fabrikam.com and then configure it to allow authentication for only members of fabrikam\Group1. This way, only members of fabrikam\Group1 would be able to access server1.contoso.com, while other users from the fabrikam.com forest would be denied access.

upvoted 8 times


  **monishhk**  11 months, 1 week ago

**Selected Answer: C**

This question is valid

Exam date - 27-07-2024

upvoted 2 times

  **MR\_Eliot** 1 year, 9 months ago

**Selected Answer: C**

C for sure. no explanation needed.

upvoted 3 times

  **Returnerwesley** 2 years ago

the answer should be A

cause we only need to give Group1 the permission

upvoted 2 times

  **JoeBob8912** 10 months ago

With a 2 way forest trust, all users in any of the domains and child domains of each forest can already authenticate with each other by default. So, we don't need to give anyone any more permissions, we just need to strip away permission from anyone that is not Group 1. To do that we have to enable selective authentication.

upvoted 1 times

  **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 1 times

  **syu31svc** 2 years, 3 months ago

**Selected Answer: C**



[https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/authn/trusts/netid-trust-](https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/authn/trusts/netid-trust-implications/#:~:text=About%20Selective%20Authentication&text=Administrators%20must%20explicitly%20grant%20the,those%20users%20to%20login%20to)

[implications/#:~:text=About%20Selective%20Authentication&text=Administrators%20must%20explicitly%20grant%20the,those%20users%20to%20login%20to](https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/authn/trusts/netid-trust-implications/#:~:text=About%20Selective%20Authentication&text=Administrators%20must%20explicitly%20grant%20the,those%20users%20to%20login%20to)

By choosing 'selective authentication', users from the trusted domain are not members of the dynamic 'Authenticated Users' group. Administrators must explicitly grant the 'allowed to authenticate' permission on the AD computer object to the users/groups in the trusted domain for each computer object (in the trusting domain) you want to allow those users to login to.

Answer is C

upvoted 4 times

  **raulgar** 2 years, 4 months ago

I think answer A is more accurate



upvoted 3 times

  **Jawad1462** 2 years, 8 months ago

**Selected Answer: C**

Is the correct answer

upvoted 4 times

  **vaaws** 2 years, 9 months ago

C

Selective authentication restricts access over an external or forest trust to only those users in a trusted domain or forest who have been explicitly given authentication permissions to computer objects (resource computers) residing in the trusting domain or forest. This authentication setting must be manually enabled.



Note: When a two way Forest Trust is created between Forest A and Forest B, all domains in Forest A will trust all domains in Forest B and vice versa.

upvoted 4 times

  **ScarfaceRecords** 2 years, 9 months ago

the answer should be A

upvoted 4 times

  **edykss** 2 years, 9 months ago

Why A?

C - Selective authentication in a forest trust enables you to limit which users and groups from the trusted domain are able to authenticate.

upvoted 3 times

  **SFM1993** 2 years, 3 months ago

I'd say A by the fact that we're only told that group1 needs to be able to authenticate to server1, but not told that all other authentications from the trusted forest should be disallowed

upvoted 4 times

  **RungBaaz** 2 years, 9 months ago

Should Be A.

upvoted 4 times

Your network contains an Active Directory forest. The forest contains two domains named contoso.com and east.contoso.com and the servers shown in the following table.

Name	Domain	Configuration
DC1	contoso.com	Domain controller
Server1	contoso.com	Member server
DC2	east.contoso.com	Domain controller
Server2	east.contoso.com	Member server

Contoso.com contains a user named User1.

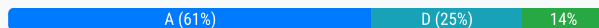
You add User1 to the built-in Backup Operators group in contoso.com.

Which servers can User1 back up?

- A. DC1 only
- B. Server1 only
- C. DC1 and DC2 only
- D. DC1 and Server1 only
- E. DC1, DC2, Server1, and Server2

**Correct Answer: A**

Community vote distribution



**certmonk** Highly Voted 2 years, 1 month ago

Correct answer: D

Members of the Backup Operators group can back up and restore all files on A computer, regardless of the permissions that protect those files.

This doesn't mean that the member of Backup operators group can backup any computer and not just a Domain controller.

They do have the permissions needed to replace files (including operating system files) on domain controllers. Because members of this group can replace files on domain controllers, they're considered service administrators.

upvoted 23 times

**Ksk08** 8 months, 2 weeks ago

yes it is D

upvoted 1 times

**mrmichael1389** 1 year, 11 months ago

It is definitely either D or E. Backup Operators can perform backup/restore operations for domain controllers and member servers. I'm just not sure if they can do this for only members of the root domain, or if those permissions would apply to child domains as well. I believe it would be that domain only.

upvoted 1 times

**MondherBB** 1 year, 11 months ago

i agree with you. But for the child domain, as you can test it, it contains his built-in Backup Operator Group, so the user in the root domain cannot have access to this child domain if he is not member of the child domain built-in security group

upvoted 1 times

**MondherBB** 1 year, 11 months ago

the correct answer should be D

DC1 and SRV1

upvoted 3 times

🗄️ 👤 **matthewk92** Highly Voted 2 years, 5 months ago

**Selected Answer: A**

Correct

"Members of the Backup Operators group can back up and restore all files on a computer, regardless of the permissions that protect those files. Backup Operators also can log on to and shut down the computer. This group can't be renamed, deleted, or removed.

By default, this built-in group has no members, and it can perform backup and restore operations on domain controllers."

upvoted 13 times

🗄️ 👤 **SDK76** Most Recent 2 months, 2 weeks ago

**Selected Answer: D**

The Backup Operators group is DOMAIN specific - thus there permissions do not extend to other domains, even in the same forest, I think the answer D.

upvoted 1 times

🗄️ 👤 **Opoveda** 3 months, 2 weeks ago

**Selected Answer: C**

The correct answer is option C: DC1 and DC2 only.

This is because User1, by being added to the Backup Operators group in the contoso.com domain, would have permissions to perform backups on the domain controllers (DC1 and DC2) within the Active Directory forest, as both are configured as domain controllers in their respective domains.

upvoted 1 times

🗄️ 👤 **Itkiller** 4 months, 3 weeks ago

**Selected Answer: A**

Tested this, as you can see in the link, a member of the group can logon to the server, i am not able to log on to my member server! But can log in to the DC.

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#backup-operators>

upvoted 2 times

🗄️ 👤 **himoumess** 6 months, 2 weeks ago

**Selected Answer: A**

1-The Backup Operators group at the domain level applies only to domain controllers within that specific domain.

2-Backup Operators cannot cross into child domains or other trusted domains unless explicitly added to the respective Backup Operators groups.

3-To back up member servers or workstations, a user must be added to the local Backup Operators group on each machine.

upvoted 1 times

🗄️ 👤 **Krayzr** 7 months, 3 weeks ago

**Selected Answer: D**

ddddddd

upvoted 1 times

🗄️ 👤 **starseed** 9 months, 2 weeks ago

Correct answer is D. 100 % No Doubt

upvoted 4 times

🗄️ 👤 **JP02021** 10 months ago

**Selected Answer: D**

Backup Operators can perform backup/restore operations for domain controllers and member servers.

upvoted 2 times

🗄️ 👤 **004b54b** 11 months, 2 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#backup-operators>

"By default, this built-in group has no members, and it can perform backup and restore operations on domain controllers."

Answer is A.

upvoted 3 times

🗄️ 👤 **SIAMIANJI** 1 year, 1 month ago



**Selected Answer: C**

Backup Operators can backup DCs and Member Servers  
upvoted 2 times

🗨️ **mohamed1999** 1 year, 1 month ago

**Selected Answer: C**

The Correct answer is C:

As a member of the Backup Operators group, you can back up and restore files and directories on all domain controllers within the domain, including child domain controllers.  
but not member servers.

I was also confused.

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>  
upvoted 1 times

🗨️ **mohamed1999** 1 year, 1 month ago

**Selected Answer: A**

The Correct answer is A:

Backup Operators group, you can only back up and restore files and directories on domain controllers within the domain. this doesn't include member server.

I was also confused.

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>  
upvoted 2 times

🗨️ **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: D**

members of the "Backup Operators" group in a domain can back up data on member servers within that domain. The "Backup Operators" group is a built-in group in Windows that has certain privileges related to backing up and restoring files and directories on computers running Windows operating systems.  
upvoted 3 times

🗨️ **jajajaf342** 1 year, 5 months ago

**Selected Answer: A**

It is clearly A. "Backup Operators" is a built-in group - this will present as a local group on member servers, and child domains will have their own "Backup Operators" group. See: <https://serverfault.com/questions/1061814/how-to-make-domain-user-for-backup-be-part-of-backup-operators-group-on-one-clie>  
upvoted 2 times

🗨️ **Bolo92** 1 year, 7 months ago

valid 27.11.23  
upvoted 2 times

🗨️ **apc1323** 1 year, 7 months ago

**Selected Answer: D**

Certmonk is correct, answer is D. Backup Operators can back up any server, including DCs.  
upvoted 4 times

## HOTSPOT

-

Your network contains an Azure Active Directory Domain Services (Azure AD DS) domain named contoso.com.

You need to configure a password policy for the local user accounts on the Azure virtual machines joined to contoso.com.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Sign in by using a user account that is a member of the:

AAD DC Administrators group  
Administrators group  
Domain Admins group

Use a Group Policy Object (GPO) linked to the:

AADDC Computers organizational unit (OU)  
AADDC Users organizational unit (OU)  
Computers container

**Answer Area**

Correct Answer:

Sign in by using a user account that is a member of the:

AAD DC Administrators group  
Administrators group  
Domain Admins group

Use a Group Policy Object (GPO) linked to the:

AADDC Computers organizational unit (OU)  
AADDC Users organizational unit (OU)  
Computers container


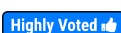
 **Goofer**  2 years, 4 months ago

A GPO linked to the AADDC Users OU has no effect on the local user accounts.

You need to link the GPO to the AADDC Computers OU.

1. AAD DC Administrators group
2. AADDC Computers organizational unit (OU)

upvoted 27 times

 **SuradjBajaj**  2 years, 4 months ago



Correct,

We need to create a Group Policy Object (GPO) in the Azure Active Directory Domain Services (Azure AD DS) domain, configure the GPO's password policy, and link the GPO to the organizational unit (OU) that contains the domain's computer accounts.

To administer group policy in a managed domain, you must be signed in to a user account that's a member of the AAD DC Administrators group.

There are two built-in Group Policy Objects (GPOs) in a managed domain - one for the AADDC Computers OU, and one for the AADDC Users OU. You can customize these GPOs to configure group policy as needed within your managed domain. By default, the AADDC Computers OU contains all the computer accounts of the member computers.

upvoted 5 times

 **stonwall12**  5 months, 3 weeks ago

Answer:



1. AAD DC Administrators group
2. AADDC Computers Group (OU)

1. In Azure AD DS, this group has the necessary permissions to manage Azure AD DS configurations including password policies.

2. In Azure AD DS, domain-joined computers are automatically placed in the AADDC Computers OU, not the default Computers container. Group Policy Objects should be linked to this OU to affect all domain-joined Azure VMs.

Reference: <https://learn.microsoft.com/en-us/azure/active-directory-domain-services/password-policy>

upvoted 1 times

  **Bob0331** 9 months, 3 weeks ago

I would think it is the computer GPO as it says local user accounts, not user accounts in aaddc. Only the computer GPO can change the settings for local user accounts

upvoted 2 times

  **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 1 times

  **MR\_Eliot** 1 year, 9 months ago

Correct answers:

1. AAD DC Administrators group

-> You need this permission to be able to login on the Azure AD domain controller

2. AADDC Computers organizational unit (OU)

-> Password policy, is a computer policy, not a user policy. so this one is right answer.

upvoted 4 times

  **syu31svc** 2 years, 3 months ago

<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy>

Answer is correct

upvoted 2 times

  **tomasek88** 1 year, 11 months ago

wrong -> correct is AADDC Computers organizational unit (OU)

upvoted 2 times

  **STFN2019** 2 years, 5 months ago

Correct

upvoted 1 times

## SIMULATION

-

You need to create a user named Admin1 in contoso.com. Admin1 must be able to back up and restore files on SRV1. The solution must use principle of the least privilege.

To complete this task, sign in the required computer or computers.

## Correct Answer:

Step 1: Sign in to the Azure portal in the User Administrator role for the organization.

Add a new user

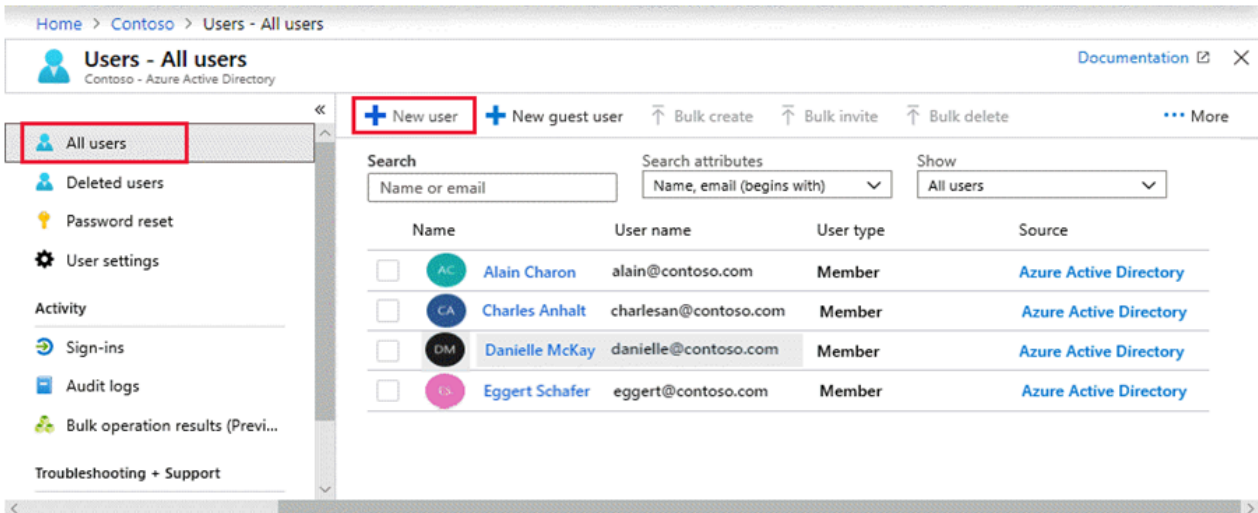
You can create a new user using the Azure Active Directory portal.

To add a new user, follow these steps:

Step 1. Sign in to the Azure portal in the User Administrator role for the organization.

Step 2: Search for and select Azure Active Directory from any page.

Step 3: Select Users, and then select New user.



Step 4: On the User page, enter information for this user:

Name: Admin1

User name: Admin1

Groups: Optional

Groups. Optional: Backup Operator

Step 5: Copy the autogenerated password provided in the Password box. You'll need to give this password to the user to sign in for the first time.

Step 6: Select Create.

The user is created and added to your Azure AD organization.

### Note:

Azure Backup provides three built-in roles to control backup management operations.

**Backup Operator** - This role has permissions to everything a contributor does except removing backup and managing backup policies. This role is equivalent to contributor except it can't perform destructive operations such as stop backup with delete data or remove registration of on-premises resources.

### Incorrect:

**Backup Contributor** - This role has all permissions to create and manage backup except deleting Recovery Services vault and giving access to others. Imagine this role as admin of backup management who can do every backup management operation.

**Backup Reader** - This role has permissions to view all backup management operations. Imagine this role to be a monitoring person.

Reference: <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>  
<https://learn.microsoft.com/en-us/azure/backup/backup-rbac-rs-vault>

**Gofer** Highly Voted 2 years, 5 months ago

1. Create domain User Admin1 in contoso.com
  2. Add Admin1 to the Backup Operators group on SRV1
- upvoted 11 times

**MR\_Eliot** 1 year, 9 months ago

I also agree with this one, however I'm not sure about the question. if it's Azure Active Directory services, then maybe it's a little different, but the current answer doesn't seem right.

upvoted 3 times

🗨️ 👤 **Anju18** Most Recent 10 months ago

Today I cleared the exam. Thank you so much exam topics and I didn't get any lab questions. 5 questions are new. New yes, No questions.  
upvoted 2 times

🗨️ 👤 **smorar** 1 year, 1 month ago

There are laboratories in the real exam?  
upvoted 2 times

🗨️ 👤 **Krayzr** 1 year ago

Should be right :?  
upvoted 1 times

🗨️ 👤 **smorar** 1 year, 1 month ago

Are there labs in the actual exam?  
upvoted 1 times

🗨️ 👤 **rknichols01** 1 year, 6 months ago

answer from C0-Pilot

Create a new user account named Admin1 in Active Directory Users and Computers 1.

On the SRV1 server, create a new local group named Backup Operators 1.

Add the Admin1 user account to the Backup Operators group on the SRV1 server 1.

Grant the Backup files and directories and Restore files and directories user rights to the Backup Operators group on the SRV1 server 1.

upvoted 2 times

🗨️ 👤 **Edileimig** 2 years, 4 months ago

There is this kind of question? I mean, simulation? I didn't see on the student guide.

It said only cases studies.

upvoted 3 times

## SIMULATION

You need to ensure that the minimum password length for members of the BranchAdmins group is 12 characters. The solution must affect only the BranchAdmins group.

To complete this task, sign in the required computer or computers.

**Correct Answer:**

Create a new fine-grained password policy.

In the following procedure you will create a new fine-grained password policy using the UI in ADAC.

To create a new fine-grained password policy.

Step 1: Right click the Windows PowerShell icon, click Run as Administrator and type dsac.exe to open ADAC.

Step 2: Click Manage, click Add Navigation Nodes and select the appropriate target domain in the Add Navigation Nodes dialog box and then click OK.

Step 3: Click Manage, click Add Navigation Nodes and select the appropriate target domain in the Add Navigation Nodes dialog box and then click OK.

Step 4: In the Tasks pane, click New, and then click Password Settings.

Fill in or edit fields inside the property page to create a new Password Settings object. The Name and Precedence fields are required.

In our case:

Minimum password length: 12

The screenshot shows the 'Create Password Settings: TestPswd' dialog box. The 'Name' field is 'TestPswd' and the 'Precedence' field is '1'. The 'Password age options' section includes checkboxes for 'Enforce minimum password age' (checked), 'Enforce maximum password age' (checked), and 'Enforce account lockout policy' (unchecked). The 'Minimum password length (characters)' is set to 7, and the 'Number of passwords remembered' is 24. The 'Directly Applies To' section is empty, and the 'Add...' button is visible.

Step 5: Under Directly Applies To, click Add, type BranchAdmin, and then click OK.

Reference: [https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-#bkmk2\\_test\\_fgpp1](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-#bkmk2_test_fgpp1)

3. In the ADAC navigation pane, open the System container and then click Password Settings Container.

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-#to-create-a-new-fine-grained-password-policy>

upvoted 17 times

🗨️ 👤 **Krayzr** 10 months, 3 weeks ago

Thanks for the links Az800 & Maup33

upvoted 1 times

🗨️ 👤 **Maup33** 2 years ago

correct, <https://activedirectorypro.com/create-fine-grained-password-policies/>

upvoted 4 times

🗨️ 👤 **neilkraftmann** Most Recent 10 months, 2 weeks ago

Had this on my exam recently.

upvoted 2 times

🗨️ 👤 **Goofer** 2 years, 5 months ago

1. Create group Policy /Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy/Minimum password length (Enable + 12)
2. Add the group BranchAdmins in the Security Filtering
3. Link the GPO to the OU in which the group BranchAdmins is located

upvoted 4 times

🗨️ 👤 **VeIN** 2 years, 3 months ago

Sorry but this will not work.

This setting that you're referring works ALWAYS from root domain object (its in reality root domain object parameter, it's a failswitch if someone would try to remove DDP GPO Link) and you can't override those setting elsewhere.

The given answer is correct. You need to user fine grained password and target the mentioned group.

upvoted 1 times

🗨️ 👤 **pewpewvx** 2 years, 2 months ago

This is incorrect. The only plausible option is FGPP policy to control it. By default a PDC emulator honors those settings ONLY in a domain. All password changed are made by the PDCE and for this reason your suggestion wont work. If you run a gpresult or a gpedit you will see that the password settings will not apply and have a red cross on it, this means the settings didn't take effect since only the PDCE will receive the password settings for a domain joined machine.

upvoted 2 times



## SIMULATION

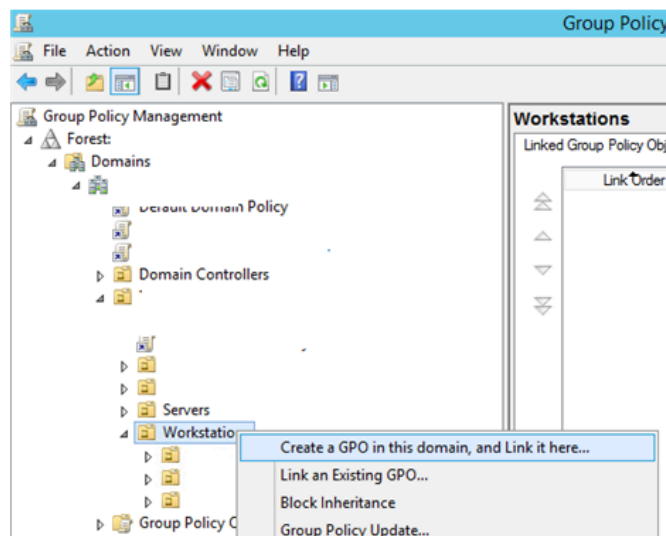
You need to configure a Group Policy preference to ensure that users in the organizational unit (OU) named Server Admins have a shortcut to a folder named \\srv1.contoso.com\data on their desktop when they sign in to the computers in the domain.

To complete this task, sign in the required computer or computers.

Create Desktop Shortcuts on Domain Computers via GPO.

Step 1: Open the Group Policy Management Console (gpmc.msc).

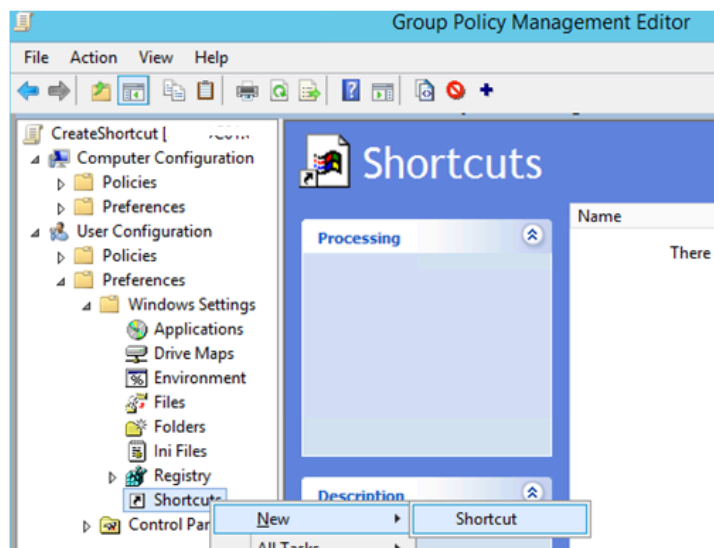
Step 2: Right-click an AD container (Organizational Unit) you want to apply a shortcut creation policy. In this case right-click on the OU Server Admins.



Step 3: Select Create a GPO in this domain, and Link it here..

Correct Answer:

Step 4: Go to the Group Policy Preferences section: User Configuration -> Preferences -> Windows Settings -> Shortcuts. Click it and select New -> Shortcut;



Step 5: Create a new shortcut item with the following settings:

Name: Something

Target Type: File System Object (you can select a URL or a Shell object here)

Location: Desktop

Target Path: \\srv1.contoso.com\data

Reference: <http://woshub.com/create-desktop-shortcuts-group-policy/>

  **Goofer** Highly Voted  2 years, 5 months ago

<https://activedirectorypro.com/group-policy-desktop-shortcuts/>  
upvoted 5 times

  **STFN2019** Highly Voted  2 years, 5 months ago

Apply to specific OU where server admins are located or use item level targetting instead  
upvoted 5 times

  **neilkraftmann** Most Recent  10 months, 2 weeks ago

Had this on my exam recently.  
upvoted 1 times

## SIMULATION

-

You plan to promote a domain controller named DC3 in a site in Seattle.

You need to ensure that DC3 only replicates with DC1 and DC2 between 8 PM and 6 AM.

To complete this task, sign in the required computer or computers.

Step 1: Create a site link between Seattle and the site in which DC1 and DC2 are located (if the site link does not already exist. If the site link already exists, then skip Step 1).

Step 2: To open Active Directory Sites and Services, click Start, click Administrative Tools, and then click Active Directory Sites and Services.  
Open Active Directory Sites and Services.

Step 3: In the console tree, click the intersite transport folder that contains the site link for which you are configuring intersite replication availability.

Step 4: In the details pane, right-click the site link whose schedule you want to configure, and then click Properties.

Step 5: Click Change Schedule.

Step 6: Select the block of time during which you want replication to be either available or not available, and then click Replication Not Available or Replication Available, respectively.  
Change the schedule to: from 8 PM to 6 AM.

**Correct Answer:** Note: Site link

Site links are Active Directory objects that represent logical paths that the KCC uses to establish a connection for Active Directory replication. A site link object represents a set of sites that can communicate at uniform cost through a specified intersite transport.

All sites contained within the site link are considered to be connected by means of the same network type. Sites must be manually linked to other sites by using site links so that domain controllers in one site can replicate directory changes from domain controllers in another site. Because site links do not correspond to the actual path taken by network packets on the physical network during replication, you do not need to create redundant site links to improve Active Directory replication efficiency.

When two sites are connected by a site link, the replication system automatically creates connections between specific domain controllers in each site that are called bridgehead servers.



Reference: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770712\(v=ws.10\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770712(v=ws.10))  
<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/replication/active-directory-replication-concepts>

 **Goofer** Highly Voted 11 months ago

1. Open - Active Directory Sites and services
  2. Goto - DC3 (DC3 only replicates with DC1 and DC2)
  3. Klik - NTDS Settings
  4. Edit Link - Tab General - Change Schedule (between 8PM and 6AM)
- Edit only the links to DC1 and DC2  
upvoted 6 times

 **STFN2019** Most Recent 11 months ago

- 1) Open Active Directory Sites and Services
  - 2) Switch to Inter-Site Transports -> IP and ensure the correct site links exist i.e. DC3 to DC1 and DC3 to DC2, or create a new site link/s if needed.
  - 3) To change schedule i.e. 8PM and 6AM click on the site link and change schedule
- upvoted 3 times

  **Itkiller** 5 months, 1 week ago

Not 100% sure if the question means ALL replication, if so,

Don't forget, Edit DC1 and DC2, they will pull from DC3.

Editing DC3 only edits the source (from servers).

Changing these settings will rename the link to a random number instead of 'Automatically Generated'

upvoted 1 times

## SIMULATION

-

You need to ensure that DC2 is the schema master for contoso.com.

To complete this task, sign in the required computer or computers.

**Seize operations master roles**

You cannot use AD DS snap-ins to seize operations master roles. Instead, you must use either the `ntdsutil.exe` command-line tool or Windows PowerShell to seize roles.

To seize or transfer the FSMO roles by using the `Ntdsutil` utility, follow these steps:

**Step 1:** Sign in to a member computer, in our case DC2, that has the AD RSAT tools installed, or a DC that is located in the forest where FSMO roles are being transferred.

**Step 2:** Select Start > Run, type `ntdsutil` in the Open box, and then select OK.

**Step 3:** Type `roles`, and then press Enter.

**Note:**

To see a list of available commands at any one of the prompts in the `Ntdsutil` utility, type `?`, and then press Enter.

**Correct Answer:**

**Step 4:** Type `connections`, and then press Enter.

**Step 5:** Type `connect to server <servername>`, and then press Enter.

**Step 6:** At the server connections prompt, type `q`, and then press Enter.

**Step 7:** To seize the role: Type `seize <role>`, and then press Enter.

In our case we type: `size schema master`.

**Step 8:** At the `fsmo maintenance` prompt, type `q`, and then press Enter to gain access to the `ntdsutil` prompt. Type `q`, and then press Enter to quit the `Ntdsutil` utility.

**Reference:** <https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds>

 **BJack**  2 years, 4 months ago

This answer describes seizing the Schema role. The role can be transferred by registering `schmmgmt.dll` (`regsvr32 schmmgmt.dll`) and using the Active Directory Schema console.


upvoted 11 times

 **Goofer**  2 years, 5 months ago

PowerShell:

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -OperationMasterRole PDCEmulator
```


upvoted 8 times

 **Goofer** 2 years, 4 months ago

PowerShell:

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -OperationMasterRole SchemaMaster
```

upvoted 10 times

 **nonoelptirobo** 4 months, 2 weeks ago

first check with the command

```
get-adforest |fl SchemaMaster
```

if not

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -OperationMasterRole SchemaMaster
```

will ask you if you want to move the role

upvoted 1 times

 **SantaClaws** 1 year, 7 months ago

This seems like the correct approach, but you need to add the -Force flag to seize the roll.

upvoted 2 times

  **sardonique** Most Recent 11 months, 1 week ago

here the logical steps:

- 1) Query Role Holder: Netdom query fsmo
- 2) if DC2 is the schema master holder, you're done. If another server is the schema role holder, you need to move the role.
- 3) try to gracefully move the role (there are more than 1 way to do that); if a graceful move of the role is not possible because role holder DC is not consistent, then you need to go to the following steps:
- 4) backup the role holder DC, turn it off, and detach the network card
- 5) login into DC2 and seize the role (seizing is a forceful action)
- 6) remove the DC from AD Users and Computers and perform a metadata clean up
- 7) never bring back to life the old role holder
- 8) query all the DCs to ensure they all are aware of the new role holder

upvoted 2 times

  **smorar** 1 year, 1 month ago



Are there labs in the actual exam?

upvoted 6 times

  **skycrap** 2 years ago

Use AD Schema snap-in: <https://activedirectorypro.com/transfer-fsmo-roles/#:~:text=To%20transfer%20the%20schema%20master%20role%20follow%20these%20steps.>

upvoted 1 times

  **sa66ath** 2 years, 3 months ago

To ensure that DC2 is the schema master for contoso.com using ntdsutil, you can perform the following steps:

Log on to DC2 or any other domain controller that has the Active Directory Domain Services (AD DS) role installed.

Open a Command Prompt window with administrative privileges.

Type "ntdsutil" and press Enter to open the ntdsutil tool.

Type "roles" and press Enter to switch to the "fsmo maintenance" prompt.

Type "connections" and press Enter to switch to the "server connections" prompt.

Type "connect to server DC2" (replace DC2 with the name of the DC you want to make the schema master) and press Enter to connect to the DC2 server.

Type "q" and press Enter to return to the "fsmo maintenance" prompt.

Type "seize schema master" and press Enter to make DC2 the schema master.

Type "q" and press Enter to exit ntdsutil.

upvoted 4 times

  **pewpewvx** 2 years, 2 months ago

Transferring and seizing are slightly different. Seizing should be done if a transfer is not possible. A transfer is where both DCs understand a change will take place, and a seize is where the one who is holding the role is offline or unavailable "usually".

I think the Powershell method of Move-AD\*Role would be more appropriate for that reason.

upvoted 7 times

  **Goofer** 2 years, 5 months ago

1. Open - Active Directory Users and Computers (on DC2!)
2. Right Klik - contoso.com (domain)
3. Klik - Operations masters
4. Klik - Tab PDC
5. Klik - Change



upvoted 3 times

  **STFN2019** 2 years, 5 months ago

Yes for PDC, Infra and RID it would work but not for schema - you have to use ntdsutil so:

- 1) Login to DC2 -> Start -> Run and type ntdsutil
- 2) Type 'roles' and then 'connections'
- 3) Type: connect to server DC1 (schema master) and then type: 'q'
- 4) Type: 'seize schema master'
- 5) Type 'q' twice to exit

upvoted 8 times

  **Goofer** 2 years, 4 months ago

Yes, I need to read better

upvoted 2 times

Your network contains an Active Directory Domain Services (AD DS) forest. The forest contains three domains. Each domain contains 10 domain controllers.

You plan to store a DNS zone in a custom Active Directory partition.

You need to create the Active Directory partition for the zone. The partition must replicate to only four of the domain controllers.

What should you use?

- A. Windows Admin Center
- B. DNS Manager
- C. Active Directory Sites and Services
- D. ntdsutil.exe

**Correct Answer: D**

Community vote distribution

D (92%)

8%

  **Krayzr** 1 year ago

**Selected Answer: D**

D it is

upvoted 1 times

  **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: D**

ntdsutil

domain management

connections

connect to server <server\_name>

quit

create nc <partition\_name> applicationDirectoryPartition



quit

upvoted 1 times

  **windowsmodulesinstallerworker** 1 year, 10 months ago

you need to create the partition first and set up replication. that is done with ntdsutil, only after that is done you can store the zone in the partition with dns manager. so answer is D

upvoted 2 times


  **Eloir** 1 year, 10 months ago

Answer is B

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/create-apply-custom-application-directory-partition>

You can create a custom Active Directory partition by using the DnsCmd command.

upvoted 2 times

  **nonoelptirobo** 4 months, 2 weeks ago

dnscmd is not part of the DNS manager (Dnsmgmt.msc)


in the DNS manager, you can create a single partition that will replicate to ALL dns servers that are domain controllers can't select just the four

upvoted 1 times

  **amartinsalves** 1 year, 11 months ago

Alternatives B and D are correct. By these two methods, we can create application partition.

upvoted 2 times

  **Techbiz** 1 year, 11 months ago

The netutils.exe is the correct answer



upvoted 2 times

  **syu31svc** 2 years, 3 months ago

**Selected Answer: D**

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc730970\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc730970(v=ws.11))

This is a subcommand of Ntdsutil and Dsmgmt

Answer is D



upvoted 3 times

  **tfulanchan** 2 years, 4 months ago

**Selected Answer: D**

This questions appeared four times, of which ntdsutil.exe and DNS Manager both appeared two times. ntdsutil.exe is the correct answer for the other question. The suggested answers are contradicting.



upvoted 2 times

  **raulgar** 2 years, 4 months ago

**Selected Answer: B**

I think B is ok, with Dns manager you can specify whats dcs you want to replicate the zone

upvoted 1 times

  **Telekon** 2 years, 4 months ago

**Selected Answer: D**

<https://techdirectarchive.com/2022/01/26/how-to-create-and-delete-a-custom-ad-ds-partition-with-the-ntdsutil-exe-tool-on-windows-server/>

upvoted 4 times

DRAG DROP

-

Your network contains a single domain Active Directory Domain Services (AD DS) forest named contoso.com. The forest contains a single Active Directory site.

You plan to deploy a read only domain controller (RODC) to a new datacenter on a server named Server1. A user named User1 is a member of the local Administrators group on Server1.

You need to recommend a deployment plan that meets the following requirements:

- Ensures that a user named User1 can perform the RODC installation on Server1
- Ensures that Server1 is in a new site named RemoteSite1
- Uses the principle of least privilege

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

### Actions

Instruct User1 to run the Active Directory Domain Services installation Wizard on Server1.

Create a site and a subnet.

Create a site link.

Pre-create an RODC account.

Add User1 to the Contoso\Administrators group.

### Answer Area



### Answer Area

Pre-create an RODC account.

Create a site and a subnet.

Instruct User1 to run the Active Directory Domain Services installation Wizard on Server1.

Correct Answer:

**LauLauLauw** 2 years, 3 months ago

Answer should be:



- Create a site and a subnet
- Pre-create RODC account
- Instruct User 1

The site needs to be there when the RODC account gets created because it needs to be placed into the new site.  
upvoted 33 times

**Tiago\_MP** 1 year, 10 months ago

The Pre-creation of RODC account is already part of the wizard actions. The 2nd step should be adding Domain admin permissions to User 1.

upvoted 2 times

 **MR\_Eliot**  1 year, 9 months ago

Correct Answer:

1. Create Site & Subnet
2. Add User1 to "contoso\administrators"
3. Instruct User1 to Run Active Directory Domain Services Installation Wizard on Server1.

- Pre-create RODC account:

-> this is not a valid answer, since user 1 also needs to be a domain admin.

upvoted 5 times

 **KXNG**  7 months, 2 weeks ago

Clarification:

1. Create a site and subnet
- Server1 is in a new datacenter, it will need to be in a new site, RemoteSite1. You need to create said site
2. Pre-create a RODC account
- Pre-creating the RODC account in AD allows you to choose User1 as the delegated installer, this means they can complete the entire installation without needing elevated domain level privilege.
3. Instruct User1 to run ADDS installation wizard on Server1
- After pre-creating it and delegating User1 as the installer, you can continue in the wizard.

All of this adheres to principle of least privilege.

upvoted 1 times


 **smorar** 1 year ago

You cannot use a non-administrative account to create a RODC account in the domain, but you can, however, delegate the second part of the RODC installation.

Then, the principle of least privileges:

- 1- Create a site and a subnet.
- 2- Pre-create an RODC account.
- 3- Instruct User1 to run the Active Directory Domain Services installation Wizard on Server1.

upvoted 3 times

 **Tiago\_MP** 1 year, 10 months ago

Its all documented here:

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/rodc/install-a-windows-server-2012-active-directory-read-only-domain-controller--rodc---level-200->


First, you will have to create the site and subnet previously (dah)

Then, see the before mentioned link, "Your current credentials are used by default. If they don't include membership in the Domain Admins group, select Alternate Credentials, "

So User1 needs to be in Domain Admins group.

Lastly, "Instruct User 1..." as the wizard already contains the step to "Pre-create RODC account".

upvoted 4 times

 **deganis** 1 year, 11 months ago

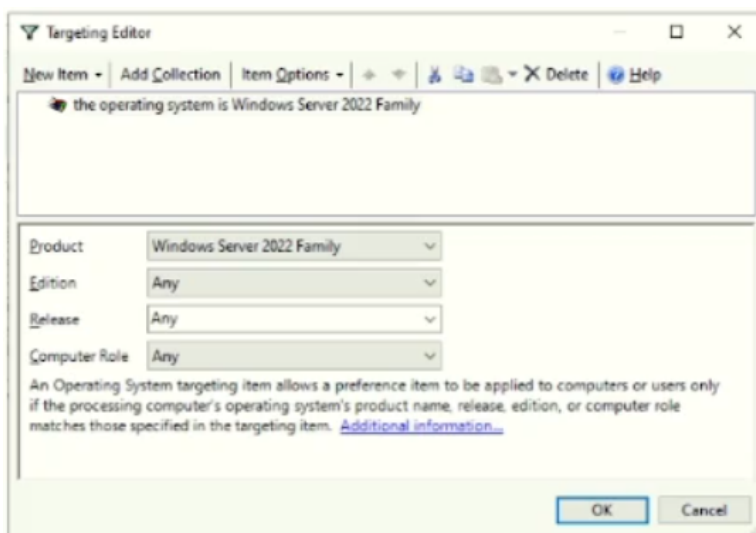
- 1 ) create site and subnet
- 2) pre-create an RODC account
- 3) instruct user1 to run the active directory domain services installation wizard on server 1

upvoted 3 times

Your network contains an Active Directory domain named contoso.com. The domain contains the computers shown in the following table.

Name	Operating system
Computer1	Windows 11
Server1	Windows Server 2016
Server2	Windows Server 2019
Server3	Windows Server 2022

On Server3, you create a Group Policy Object (GPO) named GP01 and link GP01 to contoso.com. GP01 includes a shortcut preference named Shortcut1 that has item-level targeting configured as shown in the following exhibit.



To which computer will Shortcut1 be applied?

- A. Server3 only
- B. Computer1 and Server3 only
- C. Server2 and Server3 only
- D. Server1, Server2, and Server3 only

**Correct Answer: A**

Community vote distribution

A (83%)

D (17%)

**syu31svc** Highly Voted 2 years, 3 months ago

**Selected Answer: A**

Can only be A

upvoted 7 times

**Azzainthemist** Most Recent 7 months, 2 weeks ago

**Selected Answer: D**

Windows Server 2022 family includes Windows Server 2016, 2019 & 2022 - if you do this for yourself in the domain you will see that the previous one above 2022 is 2012R2, this is because since then the family has just grown to include the new OS rather than creating a new family

upvoted 2 times

**KXNG** 7 months, 2 weeks ago

That's incorrect.

Windows Server 2022 family consists of:

Windows Server 2022 Essentials

Windows Server 2022 Standard

Windows Server 2022 Datacenter & Datacenter Azure Edition

Each version, 2016, 2019 is sold separate with distinct licenses and features. Family refers to specific versions or a generation that only included the releases within that generation.

You are likely seeing a domain functioning level / forest functioning level.



The answer is A

upvoted 1 times

  **Azzainthemist** 6 months, 3 weeks ago

I'm telling you that in this wizard, if you scope it Windows Server 2022 family it will apply to 2019 servers (as well as 2016) i've done this in production and had it apply to both when i didn't want it to, so sorry sir you are the one that is wrong this time.

upvoted 1 times

  **Itkiller** 4 months, 3 weeks ago

Sadly Azzy above here is right, tested this... all windows version get the shortcut!

This has to do with the version, 2016/2019/2022 all are version 10.0

Make you own WMI and add the buildnr to make this work:

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.%" AND ProductType = "3" AND BuildNumber = "20348"
```

14393 → Windows Server 2016

17763 → Windows Server 2019

20348 → Windows Server 2022

Windows 11:

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.%" AND ProductType = "1" AND BuildNumber >= "22000"
```

upvoted 2 times

  **monisshk** 11 months, 1 week ago

**Selected Answer: A**

This question is valid

Exam date - 27-07-2024

upvoted 3 times

Your network contains a multi-site Active Directory Domain Services (AD DS) forest. Each Active Directory site is connected by using manually configured site links and automatically generated connections.

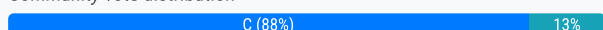
You need to minimize the latency for changes to Active Directory.

What should you do?

- A. For each site links, modify the site link costs.
- B. Create a site link bridge that contains all the site links.
- C. For each site link, modify the options attribute.
- D. For each site link, modify the replication schedule.

**Correct Answer: C**

Community vote distribution



**Duks** Highly Voted 2 years, 3 months ago

**Selected Answer: C**

In the Attribute Editor tab, double click on Options.

If the Value(s) box shows <not set>, type 1.

There is one caveat however. Change notification will fail with manual connection objects. If your connection objects are not created by the KCC the change notification setting is meaningless. If it's a manual connection object, it will NOT inherit the Options bit from the Site Link. Enjoy your 15 minute replication latency.

upvoted 7 times

**Midoria** Most Recent 5 months, 2 weeks ago

**Selected Answer: C**

The options attribute and enabling change notifications are indeed the best way to minimize latency, as it ensures near-instant replication rather than waiting for scheduled intervals.

Final Answer: C. For each site link, modify the options attribute.

upvoted 1 times

**wazza47** 6 months, 2 weeks ago

**Selected Answer: C**

To change the delay between the change to Active Directory and the first replication partner notification, open the Configuration partition in the ADSIEdit tool and go to CN=Partitions,CN=Configuration,DC=<Forest Root Domain>. In the container, right-click the crossRef object of the directory partition you want to modify the replication settings.

msDS-Replication-Notify-First-DSA-Delay - The attribute controls the delay between changes to the Directory Services (DS) and the notification of the first replica partner for a naming context (NC). The interval is 15 seconds if the attribute isn't set.

msDS-Replication-Notify-Subsequent-DSA-Delay - The attribute specifies the delay between notifications of each subsequent replica partner for an NC. The interval is three seconds if the attribute isn't set.

upvoted 1 times

**wazza47** 6 months, 2 weeks ago

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/modify-default-intra-site-dc-replication-interval>

upvoted 1 times

**KXNG** 7 months, 2 weeks ago

Read the question carefully, if you see a similar one, don't just think it's the same answer.

There is a difference between convergence and latency

This question refers to latency, which is about the delay in a replication cycle for individual changes and you minimize it by configuring the options attribute.

The convergence question which is very similar sounding is not the same thing. Convergence time is about how long it takes for all the DC's to be updated and you can minimize that by adjusting the replication schedule.

upvoted 4 times

🗨️ 👤 **Renann** 9 months ago

The correct answer to this question is D. For each site link, modify the replication schedule.

In a multi-site Active Directory forest, replication between sites is controlled by site links, and these links have a replication schedule that determines how often changes are replicated between domain controllers located in different sites.

upvoted 1 times

🗨️ 👤 **mohamed1999** 1 year, 1 month ago

**Selected Answer: C**

change notification may be enabled between site links that can span geographic locations. This will make Active Directory replication instantaneous between as if the replication partners were in the same site.

upvoted 1 times

🗨️ 👤 **mohamed1999** 1 year, 1 month ago

<https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/configuring-change-notification-on-a-manually-created/ba-p/400188#:~:text=Although%20this%20is%20well%20documented%20on%20TechNet%20and,Value%20%28s%29%20box%20shows%20%3Cnot%20set%3>

upvoted 2 times

🗨️ 👤 **SIAMIANJI** 1 year, 1 month ago

**Selected Answer: C**

To minimize the latency you need to modify attributes.

upvoted 2 times

🗨️ 👤 **fbx01** 1 year, 4 months ago

**Selected Answer: D**

D. For each site link, modify the replication schedule.

upvoted 2 times

🗨️ 👤 **jajajaf342** 1 year, 5 months ago

This exact same question is in the MeasureUp practice test test, and the answer they're looking for is D.

Not saying it's even technically the "most" correct, but on paper, the answer they're expecting is "D" for this question.

upvoted 2 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

**Selected Answer: C**

C is the correct answer. Setting the option attribute will notify the domain controllers in domain to sync with every change.

upvoted 2 times

🗨️ 👤 **MichalGr** 1 year, 2 months ago

here you claim something different

<https://www.examttopics.com/discussions/microsoft/view/78342-exam-az-800-topic-1-question-12-discussion/>

upvoted 1 times

🗨️ 👤 **KXNG** 7 months, 2 weeks ago

He's right..

There is a difference between convergence and latency.

Replication schedule for convergence

Options attribute for latency

upvoted 1 times

🗨️ 👤 **Techbiz** 1 year, 11 months ago

Sorry, I will contradict my solution below, The answer is C.

upvoted 3 times

🗨️ 👤 **Techbiz** 1 year, 11 months ago

I think the answer is D, you can adjust the replication schedule to manage latency, but C will only enforce replication.

upvoted 2 times

## DRAG DROP

-

Your network contains two Active Directory Domain Services (AD DS) forests named contoso.com and fabrikam.com. Contoso.com contains three child domains named amer.contoso.com, apac.contoso.com, and emea.contoso.com. Fabrikam.com contains a child domain named apac.fabrikam.com. A bidirectional forest trust exists between contoso.com and fabrikam.com.

You need to provide users in the contoso.com forest with access to the resources in the fabrikam.com forest. The solution must meet the following requirements:

- Users in contoso.com must only be added directly to groups in the contoso.com forest.
- Permissions to access the resources in fabrikam.com must only be granted directly to groups in the fabrikam.com forest.
- The number of groups must be minimized.

Which type of groups should you use to organize the users and to assign permissions? To answer, drag the appropriate group types to the correct requirements. Each group 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.

**Answer Area****Group types**

Domain global

Domain local

Universal

Organize users:

Assign permissions:

**Answer Area****Correct Answer:**

Organize users:

Domain global

Assign permissions:

Domain local

 **Aliabdo** Highly Voted 1 year, 7 months ago

Organize users : Universal groups

Permission : Domain Local

upvoted 12 times

 **skycrap** Highly Voted 2 years ago


Coorect: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#group-scope>

upvoted 5 times

 **mrmichael1389** 1 year, 11 months ago

Organize users would be Universal groups. There are child domains that would need to have users added to the groups. It speaks about users/groups in the forest (not just the domain).

upvoted 7 times

 **tomasek88** 1 year, 11 months ago

BUT users are NOT members of Universal. Users are members of Global and Globals are members Universal.

A -> G -> U -> DL -> Permissions

upvoted 6 times



 **Ksk08** Most Recent 8 months, 1 week ago





domain global  
domain local  
upvoted 1 times

  **monisshk** 11 months, 1 week ago

This question is valid  
Exam date - 27-07-2024  
upvoted 3 times

  **fbx01** 1 year, 4 months ago

domain local  
universal Local  
upvoted 1 times

  **Bolo92** 1 year, 7 months ago

valid 27.11.23  
upvoted 1 times

  **MR\_Eliot** 1 year, 9 months ago

Answer seems correct, do your own research, but in my mind:

Users go to global groups, because, they say ONLY CONTOSO.com MEMBERS. Universal group will allow CHILDDOMAIN MEMEBERS as well.

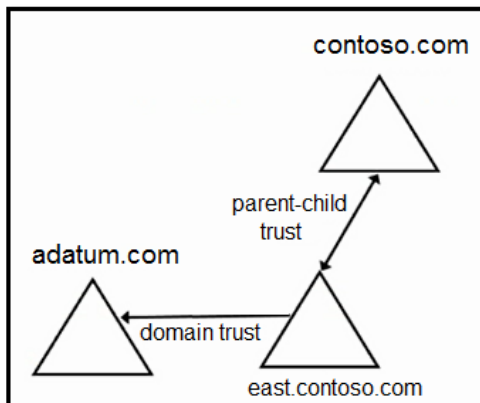
For assigning the permissions, it should be DOMAIN LOCAL. Because of A>G>U>DL=>Permissions. AND also DOMAIN LOCAL groups, can contain groups/users of other forests.

upvoted 4 times

## HOTSPOT

-

Your network contains two Active Directory forests and a domain trust as shown in the following exhibit.



The domain trust has the following configurations:

- Name: adatum.com
- Type: External
- Direction: One-way, outgoing
- Outgoing trust authentication level: Domain-wide authentication

The forests contain the users shown in the following table.

Name	Domain
User1	adatum.com
User2	contoso.com
User3	east.contoso.com

The forests contain the network shares shown in the following table.

Name	In domain
Share1	adatum.com
Share2	contoso.com
Share3	east.contoso.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.

### Answer Area

Statements	Yes	No
User1 can be assigned permissions for Share3. <input type="radio"/>	<input type="radio"/>	<input type="radio"/>
User2 can be assigned permissions for Share1. <input type="radio"/>	<input type="radio"/>	<input type="radio"/>
User3 can be assigned permissions for Share1. <input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Answer Area

	Statements	Yes	No
Correct Answer:	User1 can be assigned permissions for Share3.	<input checked="" type="radio"/>	<input type="radio"/>
	User2 can be assigned permissions for Share1.	<input type="radio"/>	<input checked="" type="radio"/>
	User3 can be assigned permissions for Share1.	<input type="radio"/>	<input checked="" type="radio"/>

  **AlexKL** Highly Voted 2 years ago

I think the answer is correct. Since Share3 trusts User1, so User1 can assign permission for Share3. As per Microsoft: "A one-way trust is a unidirectional authentication path created between two domains (trust flows in one direction, and access flows in the other). This means that in a one-way trust between a trusted domain and a trusting domain, users or computers in the trusted domain can access resources in the trusting domain. However, users in the trusting domain cannot access resources in the trusted domain. Some one-way trusts can be either nontransitive or transitive, depending on the type of trust being created."

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759554\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759554(v=ws.10)?redirectedfrom=MSDN)

upvoted 16 times

  **skycrap** 2 years ago

Spot on. I agree.

upvoted 4 times

  **skycrap** Highly Voted 2 years ago

I think that the answer should be: No - No - Yes.

user1 --> Share3: No because it is an outgoing domain trust from east.contoso.com

user2 --> Share1: No, no trust relationship between adatum and contoso domains



User3 ↗ Share1: Yes because of the outgoing trust with Adatum domain

upvoted 11 times

  **skycrap** 2 years ago

Change: YES - NO - NO as AlexKL explained.

upvoted 9 times

  **Shnash** 1 year, 11 months ago


Good Boy....

upvoted 5 times

  **DanielRO** 1 year, 11 months ago

You are right. The picture is wrong. The connection is One-way, outgoing. Outgoing not Incoming.

upvoted 2 times

  **HardeWerker433** Most Recent 3 months ago

For all those wondering about where @alexKL are coming from. The picture is 'wrong' and you should look at the text.

upvoted 1 times

  **Ksk08** 7 months, 2 weeks ago

1. Can User1 (from adatum.com) use Share3 (in east.contoso.com)?

YES ✓

Because east.contoso.com has specifically allowed adatum.com users to access its resources

2. Can User2 (from contoso.com) use Share1 (in adatum.com)?

NO ✓

There's no path or permission for contoso.com users to access adatum.com

3. Can User3 (from east.contoso.com) use Share1 (in adatum.com)?

NO ✓

The trust is one-way only, allowing adatum.com users to access east.contoso.com, but not the other way around

upvoted 2 times

  **Ksk08** 8 months, 1 week ago

Answer: No No YES

upvoted 1 times

🗨️ 👤 **sardonique** 11 months, 2 weeks ago

Direction of access is the opposite of direction of trust. so if east.contoso.com one way trusts Adatum.com, that means that adatum users can access east.contoso.com resources, however not the other way around since it is a 1 way trust. There is an implicit trust between all domains within the same forests, so east.contoso and contoso trust each other, thus giving users of both domains the technical ability to access their respective resources.

upvoted 2 times

🗨️ 👤 **zimek1908** 1 year ago

description and picture doesnt match this is why people are arguing.

upvoted 1 times

🗨️ 👤 **DE5** 1 year, 1 month ago

To make this a little bit more clear. First the Alex has absolutely right, the error on the diagram is represent who trust who, not who connect to, show the east.contoso.com trust the adatum.com and that means the users from adatum.com can have access at resources o the east.

upvoted 3 times

🗨️ 👤 **MichalGr** 1 year, 2 months ago

Add on the exhibit u1/s1 @adatum.com - u2/s2 @contoso.com - u3/s3 @east.contoso.com and keep in mind that users in the trusted domain can access resources in the trusting domain, but not the other way around.

upvoted 1 times

🗨️ 👤 **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 1 times

🗨️ 👤 **MAKH83** 1 year, 7 months ago

If we take this as a trust relation between 2 neighbours, then:

An outgoing trust means that you give your key to your neighbor, so they can enter your home and use your resources. You are the trusting domain, and your neighbor is the trusted domain. You trust them to access your home, but you cannot access theirs. Taking this example, Adatum.com is the trusting domain and east.contoso.com is the trusted domain. As east.contoso.com is trusted, it can access resources in adatum.com but not the other way around.

upvoted 2 times

🗨️ 👤 **MAKH83** 1 year, 7 months ago

Had another look at this and actually i agree its No-No-Yes.

upvoted 1 times

🗨️ 👤 **MAKH83** 1 year, 7 months ago

So Answer should be No, No, Yes

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

Correct Answers:

1. [YES]

-> There is an Outgoing trust, So we trust Adatum. Since this is forest trust, child domain, also can assign permissions to Adatum users.

2. [NO]

-> Type trust is outpoint to Adatum. Only Adatum users can sign-in to Contoso forest.

3. [NO]

-> Type trust is outpoint to Adatum. Only Adatum users can sign-in to Contoso forest.

upvoted 7 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

SHARE3: EAST.CONTOSO

-> USER1: Adatum domain (OUTGOING TRUST) => GRANTED so TRUE

SHARE1: ADATUM.com

-> USER2: Contoso domain (NO TRUST) => ACCESS NOT GRANTED so FALSE

-> USER3: EAST.Contoso domain (OUTGOING TRUST) => NOT GRANTED so FALSE

upvoted 3 times

🗨️ 👤 **Tiago\_MP** 1 year, 10 months ago

Yes

No

No

That is based on the description, not in the pic, see:

<https://www.tech-faq.com/understanding-trust-relationships.html>

upvoted 2 times

## HOTSPOT

-

Your network contains an Active Directory Domain Services (AD DS) forest named contoso.com. The forest contains a child named east.contoso.com and the servers shown in the following table.

Name	Domain	Description
DC1	contoso.com	Has the schema master, infrastructure master, and domain naming master roles
DC2	east.contoso.com	Has the PDC emulator and RID master roles and is a global catalog server
Server1	contoso.com	Has the File Server, DFS Namespaces, and DFS Replication server roles

You need to create a folder for the Central Store to manage Group Policy template files for the entire forest.

What should you name the folder, and on which server should you create the folder? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Name:  ▼

- CentralDefinitions
- PolicyDefinitions
- TemplateDefinitions

Server:  ▼

- DC1 only
- DC2 only
- Server1 only
- DC1 and DC2 only
- DC1, DC2, and Server1

## Answer Area

Correct Answer:

Name:  ▼

- CentralDefinitions
- PolicyDefinitions**
- TemplateDefinitions

Server:  ▼

- DC1 only
- DC2 only**
- Server1 only
- DC1 and DC2 only
- DC1, DC2, and Server1

 **skycrap** Highly Voted 2 years ago

Shouldn't be: "Policydefinitions" and DC1 and DC2 (each domain has his own set of gp)  
upvoted 16 times

 **skycrap** 2 years ago

A Central Store is a per-domain concept. As the central store exists in the SYSVOL, and SYSVOL is only replicated among Domain Controllers within the domain, and it does not replicate to Domain Controllers in the other domains within same forest, it can be safely concluded that the Central Store is only available for each domain.  
upvoted 6 times

 **cao75rgl** 2 years ago

Correcto, cada dominio tiene su propio conjunto de GPO. Pero segun a pregunta esta pidiendo una carpeta donde guardar los template, por lo que el nombre deberia ser "TemplateDefinition", y en DC1 y DC2

upvoted 1 times

 **MR\_Eliot**  1 year, 9 months ago

I have tested this in my lab. Each domain needs it's own central policy store.

so:

1. PolicyDefinitions
2. DC1 & DC2

upvoted 13 times

 **KXNG**  7 months, 2 weeks ago

Identify the forest root domain - DC1 (Contains schema master & domain naming master roles)

Create Central Store called PolicyDefinitions in the SYSVOL folder of the forest root domain (DC1)

This will automaticall replicate to all other domain controllers within the forest making templates accessible across both contoso.com and east.contoso.com

PolicyDefinitions

DC1

upvoted 2 times


 **KXNG** 7 months, 2 weeks ago

Apologies - I was wrong

The correct answers are:

- Policy Definitions  
DC1 & DC2

upvoted 1 times

 **2892e28** 7 months, 3 weeks ago

1. Policy Definitions
2. DC1

Per <https://learn.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store>:

1. To create a Central Store for .admx and .adml files, create a new folder named PolicyDefinitions
2. The files that are in the Central Store are replicated to all domain controllers in the domain

upvoted 1 times

 **Ksk08** 8 months, 1 week ago


Answer is Policydefinitions and DC1.

upvoted 1 times

 **MichalGr** 1 year, 2 months ago

I'm wondering between (2, 2) and (2, 4). While we can technically create the PolicyDefinitions folder on either domain controller, it's common practice to perform such changes on the domain controller holding the PDC Emulator role. The PDC Emulator is considered the primary domain controller for processing GPO updates and other important tasks. Therefore, making changes or updates on the domain controller with the PDC Emulator role could be seen as a best practice. But... in our case, we should maintain a separate PolicyDefinitions folder in the SYSVOL directory for each domain controller if they are in different domains within the forest. This approach ensures that each domain can manage its GPOs independently while allowing for the possibility of having domain-specific administrative templates. So rather (2, 4), what do you think?

upvoted 2 times

 **afриди43** 1 year, 9 months ago

To create a folder for the Central Store to manage Group Policy template files for the entire forest, you should use the following options:

Name: 2. PolicyDefinitions

Server: 1. DC1 Only

You should name the folder "PolicyDefinitions" and create it on DC1, as DC1 in the contoso.com domain holds the schema master role, which is required to update the schema for Group Policy Central Store.

upvoted 1 times

🗨️ 👤 **Tiago\_MP** 1 year, 10 months ago

PolicyDefinitions, DC1 and DC2.

See <https://learn.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store>

upvoted 4 times

🗨️ 👤 **DonChevoDeLaPaca** 1 year, 11 months ago

Correct answer should be:

PolicyDefinitions

DC1 and DC2

\*

Policy definitions are domain-specific and are not shared between domains. Therefore Contoso and East Contoso would need to have their own set of Policies.

<https://learn.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store>

upvoted 6 times

🗨️ 👤 **ahenriquez02** 2 years ago

<https://learn.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store#the-central-store>

upvoted 1 times

🗨️ 👤 **wouter0121** 1 year, 11 months ago

Can you elaborate? The question is a bit unclear. We have 2 domains, so they both would have their own policydefinitions. Id say the question is invalid and wouldnt know what to answer

upvoted 1 times

🗨️ 👤 **ahenriquez02** 2 years ago

To take advantage of the benefits of .admx files, you must create a Central Store in the sysvol folder on a Windows domain controller. The Central Store is a file location that is checked by the Group Policy tools by default. The Group Policy tools use all .admx files that are in the Central Store. The files that are in the Central Store are replicated to all domain controllers in the domain.

We suggest keeping a repository of any ADMX/L files that you have for applications that you may want to use. For example, operating system extensions like Microsoft Desktop optimization Pack (MDOP), Microsoft Office, and also third-party applications that offer Group Policy support.

To create a Central Store for .admx and .adml files, create a new folder named PolicyDefinitions in the following location (for example) on the domain controller:

\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions

upvoted 2 times

🗨️ 👤 **NadirAwan** 1 year, 10 months ago

That means Option A "DC1" is the right answer ?

upvoted 1 times



## HOTSPOT

-

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains the domain controllers shown in the following table.

Name	Description
DC1	Has the schema master, infrastructure master, and domain naming master roles
DC2	Has the PDC emulator and RID master roles and is a global catalog server
DC3	None

You need to configure DC3 to be the authoritative time server for the domain.

Which operations master role should you transfer to DC3, and which console should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Role:  ▼

- Domain naming master
- Infrastructure master
- PDC emulator
- RID master
- Schema master

Console:  ▼

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers


**Answer Area****Correct Answer:**

Role:  ▼

- Domain naming master
- Infrastructure master
- PDC emulator**
- RID master
- Schema master

Console:  ▼

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers**

 **monishk** Highly Voted 11 months, 1 week ago

Answer is correct.

This question is valid

Exam date - 27-07-2024

upvoted 6 times

 **Ksk08** Most Recent 8 months ago

Role: PDC Emulator

Console: Active Directory Users and Computers

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

Answer is correct.

upvoted 3 times

🗨️ 👤 **Shnash** 1 year, 11 months ago

You can transfer FSMO roles by using the Ntdsutil.exe command-line utility or by using an MMC snap-in tool. Depending on the FSMO role that you want to transfer, you can use one of the following three MMC snap-in tools:

Active Directory Schema snap-in

Active Directory Domains and Trusts snap-in

Active Directory Users and Computers snap-in

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/view-transfer-fsmo-roles>

upvoted 2 times

🗨️ 👤 **Shnash** 1 year, 11 months ago

1- In the console tree, right-click Active Directory Users and Computers, point to All Tasks, and then click Operations Master.

2- Click the appropriate tab for the role that you want to transfer (RID, PDC, or Infrastructure), and then click Change.

3- Click OK to confirm that you want to transfer the role, and then click Close.

upvoted 1 times

🗨️ 👤 **skycrap** 2 years ago

Correct

upvoted 4 times

DRAG DROP

Your network contains an Active Directory domain named contoso.com. The domain contains group managed service accounts (gMSAs). You have a server named Server1 that runs Windows Server and is in a workgroup. Server1 hosts Windows containers.

You need to ensure that the Windows containers can authenticate to 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.

### Actions

On Server1, install and run ccg.exe.

On Server1, run New-CredentialSpec.

In contoso.com, generate a Key Distribution Service (KDS) root key.

In contoso.com, create a gMSA and a standard user account.

From a domain-joined computer, create a credential spec file and copy the file to Server1.

### Answer Area



### Answer Area

Correct Answer:

- 1 In contoso.com, generate a Key Distribution Service (KDS) root key.
- 2 On Server1, run New-CredentialSpec.
- 3 On Server1, install and run ccg.exe.

**skycrap** Highly Voted 2 years ago

I think:

Create a gMSA and a standard user account

From a domain-joined computer, cerate a credential spec file and copy the file to Server1

On Server1, install and run ccg.exe

<https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/manage-serviceaccounts#use-case-for-creating-gmsa-account-for-non-domain-joined-container-hosts>

upvoted 29 times

**Tiago\_MP** 1 year, 10 months ago

You nailed it! Nothing to add!

upvoted 4 times

**MR\_Eliot** 1 year, 9 months ago

I agree

upvoted 1 times

**Dools** 1 year, 7 months ago

Your comment is correct

From the MS doco.

The credential spec file is created using the CredentialSpec PowerShell module on a domain-joined machine.

upvoted 3 times

🗨️ 👤 **rknichols01** Highly Voted 1 year, 6 months ago

the kds key is already created, because there are already gMSA accounts.

- 1) create a new gMSA account
- 2) from a domain joined computer create a credential spec file and copy to server 1. this can only be created from a domain joined computer.
- 3) run ccg.exe using the credentials file.

upvoted 5 times

🗨️ 👤 **albert\_oc** Most Recent 10 months ago

As per Copilot:

To ensure that the Windows containers on Server1 can authenticate to contoso.com, follow these steps in sequence:

1. In contoso.com, generate a Key Distribution Service (KDS) root key: This is necessary to create group Managed Service Accounts (gMSAs).
2. In contoso.com, create a gMSA and a standard user account: This will provide the necessary accounts for authentication.
3. From a domain-joined computer, create a credential spec file and copy the file to Server1: This file will be used by the containers to authenticate using the gMSA12.

<https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/gmsa-run-container>

<https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/manage-serviceaccounts>

upvoted 3 times

🗨️ 👤 **Srle** 4 months, 2 weeks ago

You are correct, since "New-CredentialSpec" and "ccg.exe" commands CAN'T be run on non-domain joined server, so only 3 options are left to choose in sequence

upvoted 1 times

🗨️ 👤 **Tayhull2023** 2 months, 2 weeks ago

ccg.exe can be run on a non-domain computer.

"gMSA for containers with a non-domain joined host provides the flexibility of creating containers with gMSA without joining the host node to the domain. Starting with Windows Server 2019, ccg.exe is supported, which enables a plug-in mechanism to retrieve gMSA credentials from Active Directory" -

<https://learn.microsoft.com/en-us/azure/aks/aksarc/prepare-windows-nodes-gmsa>

upvoted 1 times

🗨️ 👤 **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 4 times

🗨️ 👤 **Jothar** 1 year, 7 months ago

Server 1 is NOT on the domain so it can't run new-credentialspec.

<https://www.fearofoblivion.com/running-a-windows-container-under-gmsa>

So that can be rules out.

upvoted 1 times

🗨️ 👤 **NazerRazer** 1 year, 8 months ago

To enable Windows containers hosted on Server1 to authenticate to contoso.com using group Managed Service Accounts (gMSAs), you should perform the following actions in sequence:

In contoso.com, generate a key distribution service (KDS) root key: This step is crucial for creating and managing gMSAs.

In contoso.com, create a gMSA and a standard user account: This is necessary to associate the gMSA with a service and grant it appropriate permissions.

On Server1, run new-credential spec: This step allows you to create a credential specification file for the gMSA, which you'll use to configure container authentication.

upvoted 1 times

🗨️ 👤 **Burkidur** 1 year, 6 months ago

It says that the domain ALREADY contains gMSAs. That means KDC was already created.

upvoted 3 times

🗨️ 👤 **NazerRazer** 1 year, 8 months ago

The other answers are incorrect for the following reasons:

On Server1, install and run ccg.exe: This action is not needed to set up gMSA-based authentication for Windows containers. The "ccg.exe" tool (Container Credential Guard) is related to credential protection and is not directly involved in the process of configuring gMSAs.

From a domain-joined computer, create a credential spec file and copy the file to Server1: While creating a credential spec file is part of the process, it should be performed on Server1, not on a domain-joined computer. The correct sequence of actions involves creating the credential spec file on Server1 after the necessary gMSA and KDS root key have been set up in the domain . Copying the file to Server1 is typically part of the final steps in configuring the container for gMSA-based authentication.

upvoted 3 times

Your on-premises network contains an Active Directory domain named contoso.com. You have an Azure AD tenant.

You plan to sync contoso.com with the Azure AD tenant by using Azure AD Connect cloud sync.

You need to create an account that will be used by Azure AD Connect cloud sync.

Which type of account should you create?

- A. system-assigned managed identity
- B. group managed service account (gMSA)
- C. user
- D. InetOrgPerson

**Correct Answer: B**

*Community vote distribution*

B (50%)

C (50%)

🗳️ 👤 **ScKn** 1 month, 3 weeks ago

**Selected Answer: C**

gMSAs are supported in Azure AD Connect (the full agent) but not in Azure AD Connect Cloud Sync  
upvoted 2 times

🗳️ 👤 **Krayzr** 10 months, 1 week ago

**Selected Answer: B**

B.) gMSa

<https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/how-to-prerequisites>  
upvoted 2 times

🗳️ 👤 **JackBauer** 1 year, 8 months ago

Managed Service Account is recommended. the local user account is for 2017-2021 / Legacy.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-adsync-service-account>  
upvoted 2 times

🗳️ 👤 **examesmsft** 1 year, 12 months ago

Looks like correct, follow the step by step: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-install>  
upvoted 3 times

🗳️ 👤 **sacz** 2 years ago

Seems correct ans is C  
upvoted 3 times

🗳️ 👤 **Maup33** 1 year, 12 months ago

B. You need the following to use Azure AD Connect cloud sync:

Domain Administrator or Enterprise Administrator credentials to create the Azure AD Connect Cloud Sync gMSA (group Managed Service Account) to run the agent service.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-prerequisites?tabs=public-cloud>  
upvoted 4 times

🗳️ 👤 **franyotron** 2 years ago

Correct. <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-prerequisites?tabs=public-cloud>  
upvoted 4 times

🗳️ 👤 **skycrap** 2 years ago

Not sure: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/reference-connect-accounts-permissions>

upvoted 1 times

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains the domain controllers shown in the following table.

Name	Description
DC1	PDC emulator, RID master, and global catalog server
DC2	Infrastructure master and domain naming master
DC3	Schema master
RODC1	Read-only domain controller (RODC)

You need to ensure that if an attacker compromises the computer account of RODC1, the attacker cannot view the Employee-Number AD DS attribute.



Which partition should you modify?

- A. configuration
- B. global catalog
- C. domain
- D. schema

**Correct Answer: D**

Community vote distribution

D (100%)

  **miguelangel2801** 5 months, 2 weeks ago

**Selected Answer: D**

Answer is D

The RODC filtered attribute set is a dynamic set of attributes that is not replicated to any RODCs in the forest. You can configure the RODC filtered attribute set on a schema master that runs Windows Server 2008. When the attributes are prevented from replicating to RODCs, that data cannot be exposed unnecessarily if an RODC is stolen or compromised.

<https://learn.microsoft.com/en-us/windows/win32/ad/rodc-and-active-directory-schema#marking-attributes-as-confidential>

upvoted 1 times

  **Ksk08** 8 months ago

Schema is correct

upvoted 1 times

  **Ni\_yot** 8 months, 2 weeks ago

The employee number attribute is typically associated with the **\*\*User\*\*** objects in Active Directory. In the context of FSMO (Flexible Single Master Operation) roles, this attribute is not specifically tied to a single FSMO role. However, the **\*\*Schema Master\*\*** role is responsible for managing the schema of Active Directory, which includes the definition of attributes like employee number.

So, if you're looking to modify or understand the employee number attribute, you would be interacting with the Schema Master role.

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Answer is C

upvoted 1 times

  **starseed** 9 months, 2 weeks ago

Answer is C. Domain because actual data is stored in domain partition not in schema. schema just defines the structure how the data is stored in Database

upvoted 3 times

  **boapaulo** 1 year, 6 months ago



To ensure that if an attacker compromises RODC1's computer account, he cannot view the AD DS Employee-Number attribute, you must modify the partition in the "C.domain" partition.

The domain split is where Active Directory domain-specific data is stored. By modifying the permissions in these sections, you can restrict access to certain attributes, such as Employee Number, to ensure data security.

Therefore, the correct answer is "C. domain".

upvoted 4 times

🗨️ 👤 **bda92b3** 1 year, 5 months ago

Correct

upvoted 1 times

🗨️ 👤 **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 3 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

**Selected Answer: D**

D is the answer.

upvoted 2 times

🗨️ 👤 **RickySmith** 1 year, 6 months ago

To mark an attribute confidential, you have to remove the Read permission for the attribute for the Authenticated Users group. Marking the attribute as confidential provides an additional safeguard against an RODC that is compromised by removing the permissions that are necessary to read the credential-like data

<https://learn.microsoft.com/en-us/windows/win32/ad/rodc-and-active-directory-schema#marking-attributes-as-confidential>

upvoted 3 times

🗨️ 👤 **c7d45f4** 1 year, 9 months ago

**Selected Answer: D**

According to this link [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-adls/0afba1a7-ff6b-4878-97d0-f099de319dfb](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adls/0afba1a7-ff6b-4878-97d0-f099de319dfb) the modifications need to be done at schema partition. If you scroll up on the left navigation menu and click on 2 Attributes it tells The following sections specify the attributes in the Active Directory Lightweight Directory Services schema.

upvoted 3 times

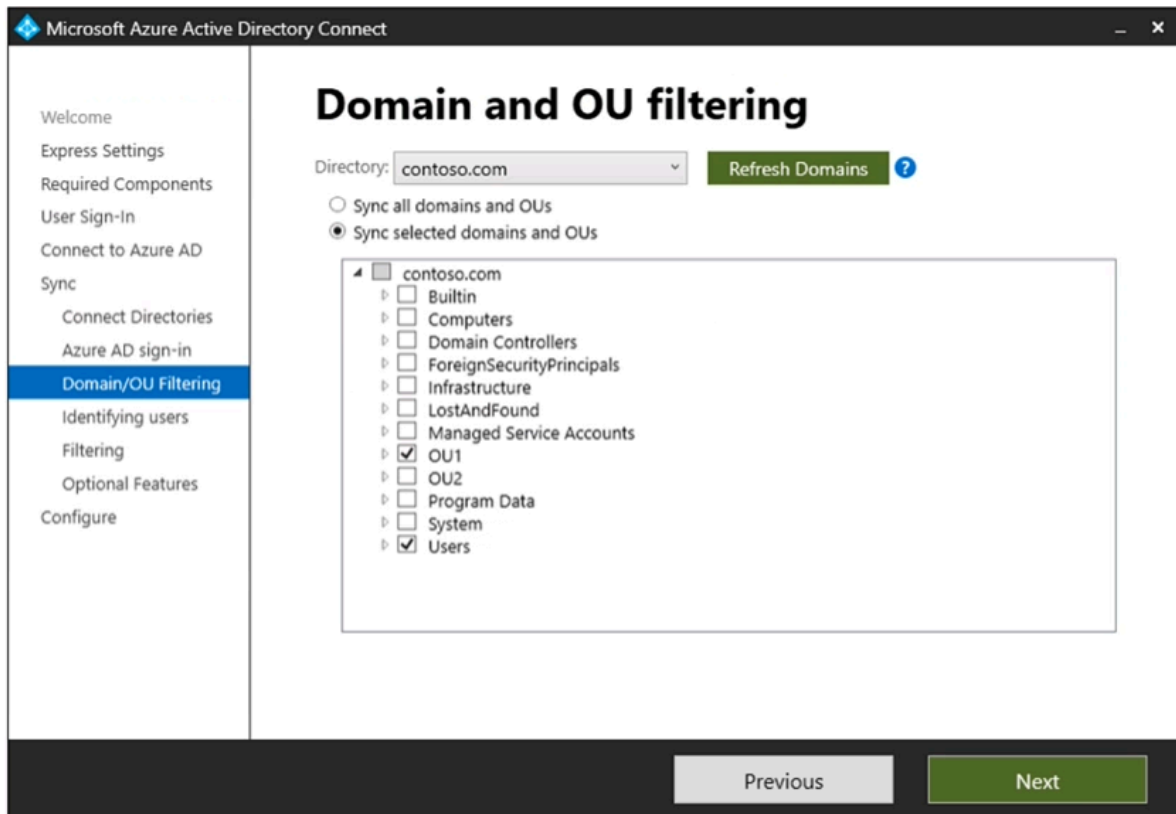
## HOTSPOT

-

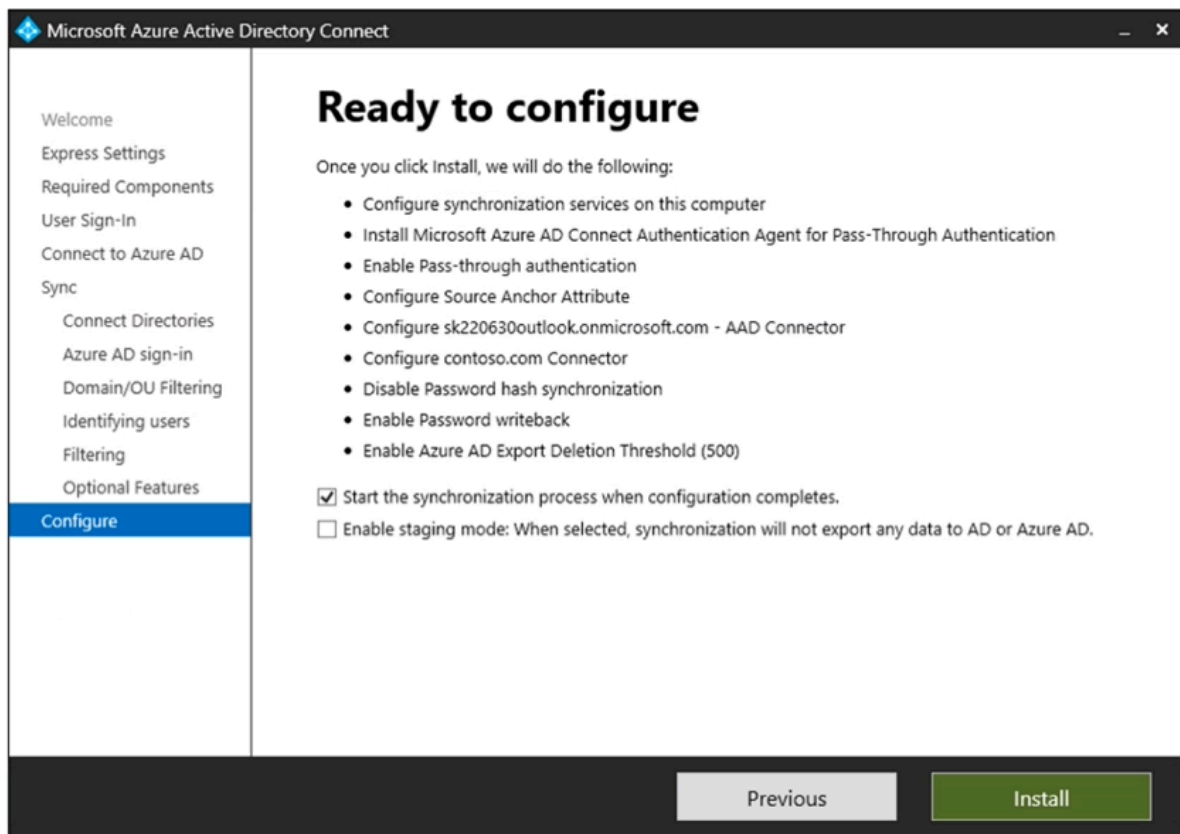
Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com that syncs with an Azure AD tenant. The tenant contains a group named Group1 and the users shown in the following table.

Name	In organizational unit (OU)
User1	OU1
User2	OU2

Domain/OU filtering in Azure AD Connect is configured as shown in the Filtering exhibit. (Click the Filtering tab.)



You review the Azure AD Connect configurations as shown in the Configure exhibit. (Click the Configure tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

#### Answer Area

##### Statements

User1 can use self-service password reset (SSPR) to reset his password.

Yes

☐

No

☐

If User1 connects to Microsoft Exchange Online, an on-premises domain controller provides authentication.

☐
☐

You can add User2 to Group1 as a member.

☐
☐

#### Correct Answer:

##### Answer Area

##### Statements

User1 can use self-service password reset (SSPR) to reset his password.

☒

No

☐

If User1 connects to Microsoft Exchange Online, an on-premises domain controller provides authentication.

☒

No

☐

You can add User2 to Group1 as a member.

☒

No

☐

**MR\_Eliot** Highly Voted 1 year, 9 months ago

1. [YES]

-> Password Write back is enabled.

2. [YES]

-> Pass-Through authentication is in use, therefore AD is the Identity Provider.

3. [NO]

-> "User2" is under "OU2" which is not syned to the Azure Tenant.

upvoted 26 times

**formacionproxia** 4 months, 3 weeks ago


The statement indicates that users User1 and User2 already exist in the tenant.

upvoted 1 times

**PXAbstraction** 1 year, 8 months ago

Correct. The amount of wrong answers provided on this test is pretty ridiculous.

upvoted 9 times

 **NazerRazer**  1 year, 8 months ago

1. User1 can use self-service password reset (SSPR) to reset his password.

-> [YES]. User1 can use self-service password reset (SSPR) because they are in the synchronized organizational unit (OU1), and "Enable Password writeback" is configured.

2. If User1 connects to Microsoft Exchange Online, an on-premises domain controller provides authentication.

-> [Yes]. When User1 connects to Microsoft Exchange Online or any other Azure AD-integrated service, their authentication request is passed directly to an on-premises AD domain controller for validation because Pass-through Authentication (PTA) is used.

3. You can add User2 to Group1 as a member.


-> [No]. User2 is in OU2, which is not selected for synchronization according to the provided configuration details. Since User2's OU is not included in the synchronization scope, you cannot directly add User2 to Group1 from the on-premises AD.

upvoted 5 times

 **Opoveda**  3 months, 1 week ago

I think is Y Y N

upvoted 1 times

 **nap61** 11 months, 3 weeks ago

"The tenant contains a group named Group1 and the users shown in the following table."

User 2 is already member of Group1 as stated...


upvoted 1 times

 **nonoelptirobo** 4 months, 1 week ago

it's not stated that the users are in te group1, if they where already in the group, they wouldn't as to add user2 to the group there must be a missing coma :

"the "The tenant contains a group named Group1; and the users shown in the following table

upvoted 1 times

 **Joedn** 1 year, 1 month ago

Valid 05/28/2024

upvoted 2 times

 **MaryMargh** 9 months, 3 weeks ago

Is there a simulation in exam?

upvoted 1 times

 **SIAMIANJI** 1 year, 2 months ago

Question3: No.

If the organizational unit (OU2) to which User2 belongs is not selected for synchronization in Azure AD Connect, then User2 will not be synchronized to Azure Active Directory (Azure AD). As a result, User2 will not be visible in Azure AD, and you won't be able to directly add User2 to Group1 in Azure AD.


upvoted 1 times

 **Payday123** 1 year, 7 months ago

"The TENANT contains a group named Group1 and the users shown in the following table."

So the Group1 is AAD only and therefore User2 cannot be added as it doesn't exist in the tenant  
YYN

upvoted 2 times

 **Jothar** 1 year, 7 months ago


Question #3 NEVER said that you were adding user2 to group1 on the aad. Sounds like you are doing this from AD and of course it will work. So yes for #3 as well.

upvoted 2 times

 **SIAMIANJI** 1 year, 2 months ago

Incorrect! It says: "The tenant contains a group named Group1". Group1 is not in AD it's in Azure Tenant.

upvoted 1 times

  **SantaClaws** 1 year, 7 months ago

I disagree. Read the first line:

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com that syncs with an Azure AD tenant. The tenant contains a group named Group1 and the users shown in the following table.

It is explicitly stated that Group1 exists in the Tenant. You are TECHNICALLY correct that Group1 might ALSO exist in AD, but in the SPIRIT of the question, we should assume not. Otherwise they ought to have told us that explicitly.

Therefore the answer ought to be NO, because OU2 is not synced in AAD and Group1 is an AAD group.

upvoted 4 times

HOTSPOT

-

Your on-premises network contains an Active Directory Domain Services (AD DS) domain.

You plan to sync the domain with an Azure AD tenant by using Azure AD Connect cloud sync.

You need to meet the following requirements:

- Install the software required to sync the domain and Azure AD.
- Enable password hash synchronization.

What should you install, and what should you use to enable password hash synchronization? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Install:

- Active Directory Administrative Center
- Azure AD Connect
- The AD FS Management console
- The Azure AD Connect provisioning agent

Use:

- Active Directory Administrative Center
- Azure AD Connect
- The AD FS Management console
- The Azure portal



### Answer Area

Correct Answer: Install:

- Active Directory Administrative Center
- Azure AD Connect**
- The AD FS Management console
- The Azure AD Connect provisioning agent

Use:

- Active Directory Administrative Center
- Azure AD Connect
- The AD FS Management console
- The Azure portal**

 **bdbea79**  1 year, 5 months ago

Payday123 is right, "Azure AD Connect cloud sync" and "Azure AD Connect" are two different tools. I could not find a Microsoft Article about it but this made it clear: <https://www.linkedin.com/pulse/how-azure-ad-connect-cloud-sync-different-from-guide-sharif/>

Install Provisioning agent

Use Azure Portal

upvoted 12 times

🗄️ 👤 **nonoelptirobo** 4 months, 1 week ago

<https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/how-to-install>

here is the articles, you install the provisioning agent then :

Sign in to the Microsoft Entra admin center as at least a Hybrid Identity Administrator.

On the left, select Protection, select Password reset, then choose On-premises integration.

Check the option for Enable password write back for synced users .

upvoted 1 times

🗄️ 👤 **Payday123** Highly Voted 1 year, 8 months ago

"Azure AD Connect cloud sync" and "Azure AD Connect" are two different tools!

upvoted 7 times

🗄️ 👤 **formacaotismic** Most Recent 7 months, 2 weeks ago

Podemos usar o Azure AD Connect para habilitar a sincronização de hash de senha. O Azure AD Connect é uma solução completa que inclui a funcionalidade de sincronização de hash de senha, além de outras opções avançadas de sincronização e autenticação.

Portanto, podemos responder:

Instalar: Azure AD Connect

Utilizar: Azure AD Connect

upvoted 2 times

🗄️ 👤 **Ksk08** 8 months, 1 week ago

Install: The Azure AD Connect provisioning agent

Use: The Azure portal

upvoted 1 times

🗄️ 👤 **starseed** 9 months, 2 weeks ago

Correct answer is The Azure AD Connect Provisioning Agent and The Azure portal because here key thing is Azure AD connect cloud sync. It is different tool which is more cloud native than Azure AD connect.

upvoted 5 times

🗄️ 👤 **monishk** 11 months, 1 week ago

This question is valid

Exam date - 27-07-2024

upvoted 3 times

🗄️ 👤 **rasmart** 1 year, 1 month ago

To Install: AZ AD Connect

Use : AZ AD Connect

upvoted 5 times

🗄️ 👤 **SIAMIANJI** 1 year, 2 months ago

To achieve your requirements, follow these steps:

Install Azure AD Connect:

Azure AD Connect is the software you need to install to sync your on-premises Active Directory domain with Azure AD. It facilitates the synchronization of user accounts, passwords, and other attributes between your local AD and the cloud-based Azure AD.

Enable Password Hash Synchronization (PHS):

Once Azure AD Connect is installed, configure it to enable PHS. Password hash synchronization ensures that user passwords are synchronized from your on-premises AD to Azure AD.

Here's how to enable PHS using Azure AD Connect:

Open "Azure AD Connect."

Choose "Customize synchronization options."

Sign in to Azure AD (requires an account with global administrator privileges).

Ensure that the connection to the on-premises Active Directory is successfully established.

Click "Next."

Select "Password Hash Synchronization."

upvoted 3 times

🗄️ 👤 **IcE** 1 year, 2 months ago

1. Install the 'Microsoft Entra provisioning agent'

2. You can use the 'Azure AD Connect' tool to manage and monitor this synchronization

upvoted 5 times

🗨️ 👤 **h123456789a** 1 year, 2 months ago

Should be both azure AD connect

upvoted 2 times

🗨️ 👤 **boapaulo** 1 year, 6 months ago

To meet the specified requirements, you must install Azure AD Connect and use Azure AD Connect to enable password hash synchronization. Let's look at the correct options:

Install:

Azure AD Connect

Use:

Azure AD Connect

Therefore, the correct selections are:

Install: Azure AD Connect

Use: Azure AD Connect

upvoted 2 times

🗨️ 👤 **PXAbstraction** 1 year, 7 months ago

Upon further review, selecting both answers as "Azure AD Connect" and "Azure AD Connect Provisioning Agent" and "Azure Portal" could be valid. Azure AD Connect Cloud Sync is a different product, but the way it's written in the question doesn't imply you're using that one (note that cloud sync isn't capitalized). To me, that reads like you are using AD Connect to cloud sync the accounts, which means "Azure AD Connect" is the right answer for both. That's how I would answer and if I was told I was wrong, I'd contest it under the guise of the question being poorly written.

upvoted 2 times

🗨️ 👤 **NazerRazer** 1 year, 8 months ago

Here's the explanation:

Azure AD Connect and the Azure Portal.

Azure AD Connect is the primary tool you need to install to set up synchronization between your on-premises AD DS domain and Azure AD. It allows you to configure various synchronization options, including password hash synchronization.

The Azure portal is where you can manage your Azure AD settings and configuration, including enabling and configuring password hash synchronization. This is where you'll perform the necessary steps to enable this feature in your Azure AD tenant.

The other options listed, such as Active Directory Administrative Center and the AD FS Management console, are not directly related to setting up Azure AD synchronization with password hash synchronization in this context, so you do not need to install them or use them for this specific requirement.

upvoted 1 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

Both should be Azure AD Connect.

upvoted 5 times

🗨️ 👤 **MR\_Eliot** 1 year, 9 months ago

I was wrong, correct answer below:

KEY:

Azure AD Connect cloud sync

First Box:

The Azure AD Connect Provisioning Agent

Second Box:

The Azure Portal

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-configure>



upvoted 10 times

  **sam801** 1 year, 9 months ago

Azure AD Connect and Azure AD Connect.

When you install Azure AD Connect by using the Express Settings option, password hash synchronization is automatically enabled.

upvoted 5 times

  **PXAbstraction** 1 year, 7 months ago


This is correct. I've done it many times myself. You don't have to explicitly enable password hash sync in the portal.

upvoted 1 times

  **c7d45f4** 1 year, 9 months ago

the answer is AD Connect and AD connect <https://learn.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-password-hash-sync>

upvoted 2 times

  **Mikepsperu** 1 year, 9 months ago

It seems that they are asking to use "cloud sync," the answer should be:

1: The Azure AD Connect provisioning agent: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-install>

2: The Azure Portal: [https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-](https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-configure#:~:text=On%20the%20configuration%20screen%2C%20select%20your%20domain%20and%20whether%20to%20enable%20password%20hash%2)

[configure#:~:text=On%20the%20configuration%20screen%2C%20select%20your%20domain%20and%20whether%20to%20enable%20password%20hash%2](https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-configure#:~:text=On%20the%20configuration%20screen%2C%20select%20your%20domain%20and%20whether%20to%20enable%20password%20hash%2)

upvoted 17 times

  **MR\_Eliot** 1 year, 9 months ago

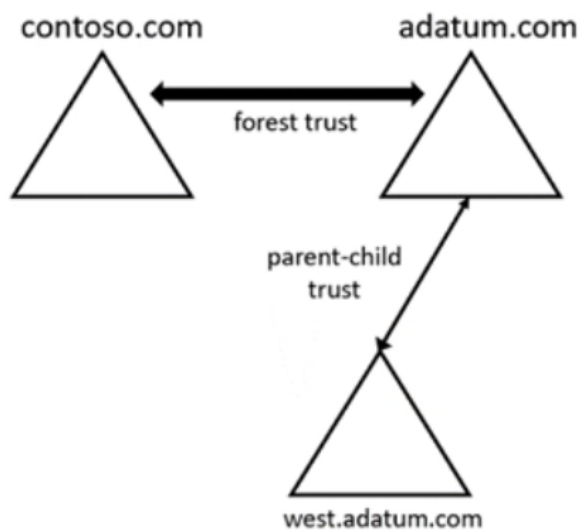
Agreed

upvoted 1 times

## HOTSPOT

-

Your network contains two Active Directory Domain Services (AD DS) forests as shown in the following exhibit.



The forests contain the domain controllers shown in the following table.

Name	Domain	Global catalog	Schema master
DC1	adatum.com	Yes	Yes
DC2	adatum.com	No	No
DC3	west.adatum.com	Yes	No
DC4	contoso.com	Yes	Yes

You perform the following actions on DC1:

- Create a user named User1.
- Extend the schema with a new attribute named Attribute1.

To which domain controllers are User1 and Attribute1 replicated? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

User1:

<input type="checkbox"/>	DC2 only
<input type="checkbox"/>	DC3 only
<input type="checkbox"/>	DC2 and DC3 only
<input type="checkbox"/>	DC3 and DC4 only
<input type="checkbox"/>	DC2, DC3, and DC4

Attribute1:

<input type="checkbox"/>	DC2 only
<input type="checkbox"/>	DC4 only
<input type="checkbox"/>	DC2 and DC3 only
<input type="checkbox"/>	DC2, DC3, and DC4

**Answer Area**


Correct Answer:

User1:

<input type="checkbox"/>	DC2 only
<input type="checkbox"/>	DC3 only
<input type="checkbox"/>	DC2 and DC3 only
<input checked="" type="checkbox"/>	DC3 and DC4 only
<input type="checkbox"/>	DC2, DC3, and DC4

Attribute1:

<input type="checkbox"/>	DC2 only
<input checked="" type="checkbox"/>	DC4 only
<input type="checkbox"/>	DC2 and DC3 only
<input type="checkbox"/>	DC2, DC3, and DC4

 **Mikepsperu** Highly Voted 1 year, 9 months ago

User1:

This is a domain-level object.

Since DC1 and DC2 are in the same domain (adatum.com), User1 will be replicated to DC2.

DC3 is in a different domain (west.adatum.com), but it is in the same forest. Since it's a Global Catalog (GC) server, it will receive a partial replica of the adatum.com domain, including the newly created User1.

DC4 is in a completely different forest (contoso.com) and there is no direct trust relationship between contoso.com and west.adatum.com, so User1 will not be replicated to DC4.

Attribute1:

This is a schema-level object. The schema is a forest-wide object.

The schema master for the adatum.com forest is DC1, so any changes to the schema (such as adding a new attribute) are initially made on DC1.

These changes are then replicated to all other domain controllers in the adatum.com forest, which includes DC2 and DC3.

However, DC4 is in a different forest, so it will not receive the schema changes made in the adatum.com forest.

In summary, User1 and Attribute1 will be replicated to DC2 and DC3

upvoted 28 times

 **sardonique** 11 months ago

"DC4 is in a completely different forest (contoso.com) and there is no direct trust relationship between contoso.com and west.adatum.com, so User1 will not be replicated to DC4." this is true, it will not be replicated however the reason you mentioned is wrong. A forest is a logical boundary,

replication process does not cross the forest boundaries by design. the Trust has barely anything to do with replication, the Trust is meant to grant access to foreign security principals

upvoted 2 times

  **Itkiller** Most Recent 5 months ago

User1 is Created on DC1, therefore available on DC2, child domains (DC3) have their own PDC role AND objects! (DC2 ONLY)

Attribute1: Adding attributes in the schema are available on all (child) domain controllers, as it is a forest role. Doesn't matter what server has the role, you can edit the schema on any domain controller within a forest. (DC2, DC3 ONLY)

A forest trust has nothing to do with schema and AD objects in another forest, you can give other forest users and domain object access to resources.

upvoted 2 times

  **formacaotismic** 7 months, 2 weeks ago

DC2 Only

Quando se cria um novo user em parent domain, esse user não é automaticamente replicado para um child domain. Cada domínio no Active Directory mantém seu próprio conjunto de objetos de users e outros objetos de diretório. A replicação ocorre apenas dentro do mesmo domínio.

Se precisar que o user esteja disponível em ambos os domínios, você precisará criar o user separadamente em cada domínio.

DC2 and DC3 Only

Quando você estende o esquema com um novo atributo, como o Attribute1, em uma floresta do AD, essa alteração é replicada para todos os controladores de domínio dentro dessa mesma floresta. No entanto, essa replicação não se estende automaticamente para outras florestas, mesmo que haja uma relação de confiança (forest trust) entre elas.

Portanto, se você precisar que o Attribute1 esteja disponível em outra floresta, será necessário estender o esquema também nessa floresta separadamente.

upvoted 2 times

  **Ksk08** 8 months ago



User1: DC2 and DC3 only

Reason: User1 replicates within adatum.com (DC2) and to GC servers in the same forest (DC3)

Attribute1: DC2 and DC3 only

Reason: Schema changes replicate to all DCs within the same forest only

upvoted 2 times

  **starseed** 9 months, 2 weeks ago

answer is dc2 for user1 and for attribute dc2 and dc3

upvoted 4 times

  **004b54b** 10 months, 2 weeks ago

<https://serverfault.com/questions/280570/will-the-global-catalogs-in-two-forests-with-transitive-trust-replicate-data>

Global Catalogs are not synced between forests (even with a trust relationship)

upvoted 1 times

  **rasmart** 1 year, 1 month ago

Based on Active Directory structure:

DC1 is part of the adatum.com domain and holds the Schema Master role.

DC2 and DC3 are also part of the adatum.com domain.

DC4 is part of the contoso.com domain and therefore in a different forest.

Answers

User1: Since User1 was created in the adatum.com domain, User1 will be replicated to all domain controllers within the same domain. Therefore, DC2 and DC3 will have User1's information.

Attribute1: Since Attribute1 is a schema extension and schema is replicated across the entire forest, all domain controllers in the adatum.com forest (which includes DC1, DC2, and DC3) will get the schema update. DC4 will not get this update as it is in a different forest.

User1: DC2, DC3

Attribute1: DC2, DC3

upvoted 4 times

🗨️ 👤 **SIAMIANJI** 1 year, 2 months ago

Based on the information provided, let's analyze the actions performed on DC1:

User Creation:

You created a user named User1 on DC1.

Schema Extension:

You extended the schema with a new attribute named Attribute1 on DC1.

Now let's determine the replication behavior for User1 and Attribute1:

User1 Replication:

Since User1 was created on DC1, it will be replicated to other domain controllers within the same domain (adatum.com).

Therefore, User1 will be replicated to DC2 (contoso.com) and DC3 (contoso.com).

Attribute1 Replication:

When you extend the schema with a new attribute, the schema update is replicated to all domain controllers in the forest.

Therefore, Attribute1 will be replicated to all domain controllers in both forests: adatum.com and contoso.com (including DC1, DC2, DC3, and DC4).

In summary:

User1 will be replicated within the adatum.com domain.

Attribute1 will be replicated across all domain controllers in both forests.

upvoted 2 times

🗨️ 👤 **Vallion** 1 year, 2 months ago

This question begs questions

upvoted 1 times

🗨️ 👤 **dfguss** 1 year, 2 months ago

User1:

DC2 and DC3: User1 is created within the adatum.com domain. Object replication is standard within a domain, ensuring that DC2 and DC3 receive an update.

DC4: Because DC4 is in a separate forest (contoso.com) and it is not specified that there is a direct trust relationship between contoso.com and west.adatum.com, User1 would not replicate to DC4.

Attribute1:

DC2 and DC3: Schema changes are applied at the forest level. As DC2 and DC3 have the function of Global Catalog (GC), they receive replication from Attribute1.

DC4: Although DC4 is also a GC, it resides in a separate forest (contoso.com). Schema changes do not automatically propagate between multiple forests.

upvoted 1 times

🗨️ 👤 **JhonyTrujillo** 1 year, 4 months ago

User1 = DC2 Only

Attribute1 = DC2 and DC3 Only

upvoted 4 times

🗨️ 👤 **janshal** 1 year, 5 months ago

Box1:

To whom who think that the user is sync to the subdomain, please explain in what OU or container in the sub domain the user will be sync to, and maybe you will understand that the user will be sync only to it local domOn...

upvoted 2 times

🗨️ 👤 **NotThatGuy242** 1 year, 5 months ago

User1 will replicate to DC3 because, even though it's a DC in the child domain, it's a global catalog. "The global catalog of a forest includes a partial replica of every object in the forest."

Source: <https://learn.microsoft.com/en-us/windows/win32/ad/attributes-included-in-the-global-catalog>

upvoted 1 times

🗨️ 👤 **RichardChris** 1 year, 7 months ago

Why are people giving different answers?? It's very confusing which one to chose in this case

upvoted 3 times

  **e489b39** 4 weeks, 1 day ago

User1 - D2

Atribute1 - D2, D3

upvoted 1 times

  **SantaClaws** 1 year, 7 months ago

User1 is replicated to:

\* DC2 in the adatum.com domain: User objects are part of the domain partition, which is replicated to all domain controllers in the same domain.

\* DC3 in the west.adatum.com domain: Because there's a parent-child trust between west.adatum.com and adatum.com, user objects are replicated between the two domains.

Attribute1 is replicated to:

\* DC2 in the adatum.com domain: Schema updates are part of the schema partition, which is replicated to all domain controllers in the same forest.

\* DC3 in the west.adatum.com domain: Because west.adatum.com is a child domain of adatum.com, it's part of the same forest, and schema updates are replicated to all domain controllers in the forest.

\* DC4 in the contoso.com forest: Because there's a forest trust between contoso.com and adatum.com, schema updates are replicated between the two forests.

upvoted 2 times

  **SantaClaws** 1 year, 7 months ago

I take this back. DC4 will not have the attribute replicated because schema updates are not replicated across forest trusts. Answer is DC2 and DC3 for both.

upvoted 1 times

  **JhonyTrujillo** 1 year, 8 months ago

User1 - D2

Atribute1 - D2, D3, D4

upvoted 2 times

  **MR\_Eliot** 1 year, 9 months ago

Contoso:

- DC-4:

> Nothing replicated, another forest.

Adatum:

- DC1 (ADATUM):

> Create User1, Schema Extended with a new attribute

- DC2 (ADATUM):

> User + Attribute is replicated

- DC3 (WEST.ADATAUM):

> User + Attribute is replicated


Schema master FSMO role

The schema master FSMO role holder is the DC responsible for performing updates to the directory schema, that is, the schema naming context or LDAP://cn=schema,cn=configuration,dc=<domain>. This DC is the only one that can process updates to the directory schema. Once the Schema update is complete, it's replicated from the schema master to all other DCs in the directory. There's only one schema master per forest.

<https://www.windows-active-directory.com/global-catalog-server.html>

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-roles>

upvoted 2 times

  **MR\_Eliot** 1 year, 9 months ago

For both boxes, answer should be DC2 & DC3

upvoted 5 times

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains the resources shown in the following table.

Name	Description
CLIENT1	Client computer that runs Windows
DC1	Domain controller
Server1	File server
Server2	File server

You plan to replicate a volume from Server1 to Server2 by using Storage Replica.

You need to configure Storage Replica.

Where should you install Windows Admin Center?

- A. Server1
- B. CLIENT1
- C. DC1
- D. Server2

**Correct Answer: B**

Community vote distribution

B (93%)

7%

 **RickySmith** Highly Voted 1 year, 9 months ago

**Selected Answer: B**


B CLient 1

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/installation-options>

We don't recommend using Windows Admin Center for local management of the same server on which it's installed. - Not A,D.

Installing Windows Admin Center on a Domain controller is not supported - Not C

upvoted 9 times

 **Ksk08** Most Recent 8 months ago

B client 1

upvoted 1 times

 **004b54b** 10 months, 2 weeks ago

**Selected Answer: B**


<https://learn.microsoft.com/en-us/windows-server/storage/storage-replica/server-to-server-storage-replication?source=recommendations#windows-admin-center-requirements>

To use Storage Replica and Windows Admin Center together, you need the following:

[...]

1 PC Win 10 for WAC

upvoted 1 times

 **Joedn** 1 year, 1 month ago

Valid 05/28/2024

upvoted 2 times

 **mohamed1999** 1 year, 1 month ago

**Selected Answer: B**

Right now you can't use Windows Admin Center on a server to manage Storage Replica.

<https://learn.microsoft.com/en-us/windows-server/storage/storage-replica/server-to-server-storage-replication>

upvoted 2 times

 **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: B**

To configure Storage Replica for replicating a volume from Server1 to Server2, you should install Windows Admin Center on a management workstation or server. Since Server1 and Server2 are involved in the replication process, it's preferable to install Windows Admin Center on a separate machine to centrally manage both servers.

Given the options provided, the best choice would be:

B. CLIENT1

Installing Windows Admin Center on CLIENT1 allows you to manage both Server1 and Server2 from a single management workstation. This ensures that you have a centralized management interface for configuring and monitoring Storage Replica replication between the two servers.



upvoted 2 times

  **MichalGr** 1 year, 2 months ago

<https://learn.microsoft.com/en-us/windows-server/storage/storage-replica/server-to-server-storage-replication>

check the video, project Honolulu



upvoted 1 times

  **fbx01** 1 year, 4 months ago

**Selected Answer: A**

Server1

upvoted 1 times

  **fbx01** 1 year, 4 months ago

Server1

upvoted 1 times

  **boapaulo** 1 year, 6 months ago

To configure Storage Replication between Server1 and Server2, where you need to replicate a volume, it is recommended to install Windows Admin Center on Server1 or a remote administration computer. This way, you can manage Storage Replica configuration efficiently.

(A). Server1

upvoted 1 times

  **Mikepsperu** 1 year, 9 months ago

We can install it everywhere but installing it on the Client will no impact on the server performances.

So the answer is CLIENT1

upvoted 2 times



You have an on-premises Active Directory Domain Services (AD DS) domain named contoso.com that syncs with Azure AD by using Azure AD Connect.

You enable password protection for contoso.com.

You need to prevent users from including the word contoso as part of their password.

What should you use?

- A. the Azure Active Directory admin center
- B. Active Directory Users and Computers
- C. Synchronization Service Manager
- D. Windows Admin Center

**Correct Answer: A**

Community vote distribution

A (93%)

7%

🗳️ **mhmyz** 10 months, 2 weeks ago

**Selected Answer: A**

On-premises Microsoft Entra Password Protection

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-deploy>

upvoted 2 times

🗳️ **rasmart** 1 year, 1 month ago

**Selected Answer: A**

Option A is where we define the banned password lists that the Azure AD Password Protection service uses. we can specify "contoso" as a banned word here, and it will be enforced both in Azure AD and our on-premises Active Directory, provided we have the Azure AD Password Protection service set up correctly.

upvoted 2 times

🗳️ **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: A**

The correct answer is:

A. the Azure Active Directory admin center

You can configure the custom banned password list, which includes preventing the use of the word "contoso" as part of passwords, through the Azure Active Directory admin center. This allows you to enforce password policies centrally for both on-premises AD DS domain and Azure AD users.

upvoted 2 times

🗳️ **MichalGr** 1 year, 2 months ago

M\$ Entra admin center -> M\$ Entra Password Protection

so A.

upvoted 1 times

🗳️ **fbx01** 1 year, 4 months ago

**Selected Answer: D**

D. Windows Admin Center

upvoted 1 times

🗳️ **boapaulo** 1 year, 6 months ago

To enforce a password policy that prevents users from including specific words, such as "contoso", you must use Group Policy in Active Directory. The appropriate tool for this would be "Active Directory Users and Computers"

(B). Active Directory Users and Computers

upvoted 3 times

🗨️ 👤 **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 1 times

🗨️ 👤 **Payday123** 1 year, 7 months ago

**Selected Answer: A**

Incorrect. Should be A

upvoted 1 times

🗨️ 👤 **NazerRazer** 1 year, 8 months ago

**Selected Answer: A**

To prevent users from including the word "contoso" as part of their password in an on-premises Active Directory (AD DS) domain that syncs with Azure AD using Azure AD Connect, you should use Azure AD Password Protection.

Therefore, the correct option is:

A. the Azure Active Directory admin center

upvoted 3 times

🗨️ 👤 **infavolante** 1 year, 8 months ago

**Selected Answer: A**

Correct answer is A and not D.

You can block what you dont want from Azure AD

upvoted 1 times

🗨️ 👤 **CheMetto** 1 year, 9 months ago

**Selected Answer: A**

The answer is A! I'm using password protection too. I can customize password locked in the azure portal, by going to password protection section

upvoted 1 times

🗨️ 👤 **windowsmodulesinstallerworker** 1 year, 9 months ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations>

upvoted 2 times

🗨️ 👤 **De09z** 1 year, 9 months ago

Can anyone please illustrate how this answer is correct?

upvoted 1 times

🗨️ 👤 **JackBauer** 1 year, 8 months ago

it's not. the answer is definitely A

upvoted 2 times

Your network contains an Active Directory Domain Services (AD DS) forest. The forest contains three domains. Each domain contains 10 domain controllers.

You plan to store a DNS zone in a custom Active Directory partition.

You need to create the Active Directory partition for the zone. The partition must replicate to only four of the domain controllers.

What should you use?

- A. Windows Admin Center
- B. Set-DnsServer
- C. New-ADObject
- D. ntdsutil.exe

**Correct Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **Krayzr** 10 months ago

**Selected Answer:** D

D. ntdsutil.exe

upvoted 1 times

🗳️ 👤 **Jothar** 1 year, 7 months ago

Same issue as Question #30. One of these commands, ntdsutil, creates the partition. the other is used for controlling dns zone replication. So both in fact, unless the question is something else entirely.

upvoted 2 times

🗳️ 👤 **NazerRazer** 1 year, 8 months ago

To create a custom Active Directory partition for a DNS zone and control the replication scope, you should use the --> ntdsutil.exe <--utility. In this case, you need to create the partition to replicate to only four out of the ten domain controllers.

So, the correct option is:

D. ntdsutil.exe

upvoted 3 times

🗳️ 👤 **JackBauer** 1 year, 8 months ago

Set-DnsServer

upvoted 1 times

🗳️ 👤 **Burkidur** 1 year, 6 months ago

No, this set the configuration of DNS \_server\_. But creating an AD partition is a very different operation that requires very different permissions.

upvoted 1 times

HOTSPOT

-

You have an Active Directory Domain Services (AD DS) domain that contains a group named Group1.

You need to create a group managed service account (gMSA) named Account1. The solution must ensure that Group1 can use Account1.

How should you complete the script? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Add-ADComputerServiceAccount Install-ADServiceAccount New-ADObject New-ADServiceAccount	"Account" -DNSHostName "website.contoso.com" -	-AuthenticationPolicy -Instance -PrincipalsAllowedToDelegateToAccount -PrincipalsAllowedToRetrieveManagedPassword	"Group"
--	--	--	---------

**Correct Answer:**

Add-ADComputerServiceAccount Install-ADServiceAccount New-ADObject New-ADServiceAccount	"Account" -DNSHostName "website.contoso.com" -	-AuthenticationPolicy -Instance -PrincipalsAllowedToDelegateToAccount -PrincipalsAllowedToRetrieveManagedPassword	"Group"
--	--	--	---------

**De09z** Highly Voted 1 year, 9 months ago

It should be New-ADServiceAccount and -PrincipalsAllowedToRetrieveManagedPassword  
upvoted 18 times

**nook6** Highly Voted 1 year, 8 months ago

Example to Create gMSA account :

New-ADServiceAccount -Name "Account1" -DNSHostName "Account1.YourDomain.com" -PrincipalsAllowedToRetrieveManagedPassword "Group1" -Path "OU=CustomOU,DC=YourDomain,DC=com"  
upvoted 7 times

**thomasemr** Most Recent 4 months, 2 weeks ago

A opção PrincipalsAllowedToDelegateToAccount é usada para especificar quais principais (usuários ou grupos) têm permissão para delegar a conta de serviço gerenciada (gMSA) a outros serviços ou contas. Isso é diferente de PrincipalsAllowedToRetrieveManagedPassword, que define quais principais podem recuperar a senha gerenciada da gMSA.

No seu caso, se o objetivo é permitir que Group1 use a gMSA Account1, a opção correta é PrincipalsAllowedToRetrieveManagedPassword, pois isso garante que os membros do grupo possam acessar a senha gerenciada necessária para autenticar e usar a conta de serviço.

Se você precisar que Group1 delegue a gMSA a outros serviços, então você usaria PrincipalsAllowedToDelegateToAccount.

upvoted 1 times

**KXNG** 7 months, 2 weeks ago

New-ADServiceAccount & -PrincipalsAllowedToRetrieveManagedPassword

It's not -PrincipalsAllowedToDelegateToAccount because this is used when setting up delegation, which is not required here. We are needing to focus on which principals can use the gMSA. Since group 1 needs to use the the gMSA, we use -PrincipalsAllowedToRetrieveManagedPassword  
upvoted 1 times

**formacaotismic** 7 months, 2 weeks ago

New-ADServiceAccount -Name "Account1" -PrincipalsAllowedToRetrieveManagedPassword "Group1" -Path "OU=CustomOU,DC=YourDomain,DC=com"  
upvoted 1 times

**AK\_1234** 1 year, 1 month ago

New-ADServiceAccount and -PrincipalsAllowedToRetrieveManagedPassword  
upvoted 2 times

**SIAMIANJI** 1 year, 2 months ago

It should be:

New-ADServiceAccount -Name "Account1" -DNSHostName "web.contoso.com" -PrincipalsAllowedToDelegateToAccount "Group1"  
upvoted 1 times



  **RickySmith** 1 year, 6 months ago

New-ADServiceAccount -PrincipalsAllowedToDelegateToAccount

<https://learn.microsoft.com/en-us/powershell/module/activedirectory/new-adserviceaccount?view=windowsserver2022-ps#principalsallowedtodelegatetoaccount>

<https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/resource-based-constrained-delegation>

upvoted 1 times

  **Leoanetor** 1 year, 7 months ago

The answer should be New-ADServiceAccount -Name "Account1" -DNSHostName "website.contoso.com" -

PrincipalsAllowedToRetrieveManagedPassword "Group1"

Ref: <https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/manage-serviceaccounts#use-case-for-creating-gmsa-account-for-non-domain-joined-container-hosts>

upvoted 2 times

  **NazerRazer** 1 year, 8 months ago

New-ADServiceAccount -Name "Account1" -DNSHostName "website.contoso.com" -PrincipalsAllowedToRetrieveManagedPassword "Group1"

This option specifies that "Group1" is allowed to retrieve the managed password for "Account1." While it doesn't explicitly mention allowing "Group1" to use "Account1" for service operations, it does grant permission for retrieving the password, which may indirectly allow for its use in certain scenarios.

upvoted 4 times

You have an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You deploy an app that adds custom attributes to the domain.

From Azure Cloud Shell, you discover that you cannot query the custom attributes of users.

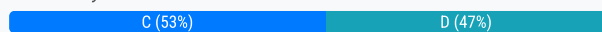
You need to ensure that the custom attributes are available in Azure AD.

Which task should you perform from Microsoft Azure Active Directory Connect first?

- A. Configure device options
- B. Manage federation
- C. Customize synchronization options
- D. Refresh directory schema

**Correct Answer:** C

Community vote distribution



**Tachinaori** Highly Voted 1 year, 8 months ago

To ensure that custom attributes from on-premises Active Directory are synchronized to Azure AD, you should perform the following task:

C. Customize synchronization options

Here's why:

Custom attributes need to be defined in the synchronization rules and schema mapping in Azure AD Connect to ensure they are synchronized from your on-premises AD to Azure AD. Customizing synchronization options allows you to define which attributes should be synchronized and how they should be mapped to corresponding attributes in Azure AD.

Option D (Refresh directory schema) typically doesn't apply in this scenario, as it's more related to updating the schema in the on-premises Active Directory, and it's not a common step to perform just to sync custom attributes to Azure AD.

Options A (Configure device options) and B (Manage federation) are unrelated to custom attribute synchronization and are not the first steps to take in this scenario.

upvoted 12 times

**nonoelptirobo** 4 months, 1 week ago

there is an option "Directory sync Extension attribute sync" in ad connect:

"this option allow you to extend the Azure AD schema based on extensions made to your organization's on prem AD instance

we had a custom attribute wich is a schema extention

upvoted 1 times

**himoumess** 6 months, 2 weeks ago

This is incorrect because you cannot customize synchronization options for an attribute that Azure AD Connect does not yet recognize. The schema must be refreshed first.

upvoted 2 times

**hrad** Most Recent 4 months, 2 weeks ago

**Selected Answer: C**

AD Connect needs to be told to sync the attribute

upvoted 1 times

**Midoria** 5 months, 2 weeks ago

**Selected Answer: D**

Refreshing directory schema in Microsoft Azure Active Directory Connect is the correct task to perform in order to ensure that custom attributes added to the on-premises AD DS domain are synchronized and available in Azure AD. This action updates the schema and allows the new attributes to be replicated to Azure AD.

upvoted 1 times

🗳️ 👤 **himoumess** 6 months, 2 weeks ago

**Selected Answer: D**

C. Customize synchronization options:

While this option allows you to customize which attributes are synced, you must refresh the schema first for the new custom attributes to appear as options, so the correct answer is D

upvoted 1 times

🗳️ 👤 **Ksk08** 8 months, 2 weeks ago

C is correct

upvoted 1 times

🗳️ 👤 **Fiscini** 8 months, 2 weeks ago

**Selected Answer: C**

There are custom attributes that needed to be added to the ADConnect sync options

upvoted 1 times

🗳️ 👤 **ademgradd** 8 months, 3 weeks ago

**Selected Answer: C**

answe is C

upvoted 2 times

🗳️ 👤 **denbever** 11 months, 2 weeks ago

**Selected Answer: C**

No attributen have yet been matches, so C.

upvoted 2 times

🗳️ 👤 **rasmart** 1 year, 1 month ago

**Selected Answer: C**

Option D might seem relevant, but it typically refers to refreshing the schema in Azure AD Connect when schema changes occur on-premises. However, it does not handle the selection of attributes to sync.

So my answer is C

upvoted 2 times

🗳️ 👤 **NotThatGuy242** 1 year, 5 months ago

**Selected Answer: D**

"Refresh directory schema: This option is used if you have changed the schema in one of your on-premises AD DS forests." Adding custom attributes is done by modifying the schema, so D makes sense.

Source: <https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-installation-wizard>

upvoted 4 times

🗳️ 👤 **Fiscini** 7 months, 3 weeks ago

It seems correct, the question specify "first" so, Update schema and later change the sync options.

upvoted 1 times

🗳️ 👤 **RickySmith** 1 year, 6 months ago

**Selected Answer: D**

[https://support.zixcorp.com/app/answers/detail/a\\_id/1411](https://support.zixcorp.com/app/answers/detail/a_id/1411)

upvoted 1 times

🗳️ 👤 **boapaulo** 1 year, 6 months ago

To ensure that custom attributes are available in Azure AD, you must first perform the "Update Directory Schema" task in Microsoft Azure Active Directory Connect.

Therefore, the correct answer is:

(D). Update Directory Schema

upvoted 3 times

You have an Active Directory Domain Services (AD DS) domain that contains the domain controllers shown in the following table.

Name	Operations master role
DC1	Schema master
DC2	Infrastructure master
DC3	Domain naming master
DC4	PDC emulator, RID master

The domain contains an app named App1 that uses a custom application partition to store configuration data.

You decommission App1.

When you attempt to remove the custom application partition, the process fails.

Which domain controller is unavailable?

- A. DC1
- B. DC2
- C. DC3
- D. DC4

**Correct Answer: C**

Community vote distribution

C (91%)

9%

 **thomasemr** 4 months, 2 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/fsmo-roles#domain-naming-master-fsmo-role>  
upvoted 1 times

 **monishk** 11 months, 1 week ago

**Selected Answer: C**

This question is valid  
Exam date - 27-07-2024  
upvoted 3 times

 **OwerGame** 11 months, 3 weeks ago

**Selected Answer: B**

If you're having trouble removing custom storage used for an app on your domain, you might want to check the server holding the Infrastructure Master FSMO role. The Infrastructure Master is responsible for updating references from objects in its domain to objects in other domains<sup>1</sup>. It's also responsible for removing an object from its domain and putting it in another domain during an object move  
upvoted 1 times

 **RickySmith** 1 year, 6 months ago

**Selected Answer: C**

C  
Domain Naming Master - Must be online when domains and application partitions in a forest are added or removed.  
<https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-placement-and-optimization-on-ad-dcs#more-information>  
upvoted 4 times

 **boapaulo** 1 year, 7 months ago



To remove a custom application partition, the domain controller that plays the role of schema master must be available. Therefore, if the removal process is failing, it is likely that DC1, which is the schema master, is unavailable. I recommend checking the status of the DC1 and making sure it is online and working properly. If DC1 is inaccessible, you need to resolve this issue before you can remove the custom application partition.  
upvoted 1 times

 **boapaulo** 1 year, 7 months ago



Why not option A?

upvoted 1 times

  **Sucxi** 1 year, 8 months ago

The domain naming master FSMO role holder is the DC responsible for making changes to the forest-wide domain name space of the directory, that is, the Partitions\Configuration naming context or LDAP://CN=Partitions, CN=Configuration, DC=<domain>. This DC is the only one that can add or remove a domain from the directory. It can also add or remove cross references to domains in external directories.

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-roles#domain%20naming>

upvoted 1 times

  **PXAbstraction** 1 year, 8 months ago

**Selected Answer: C**

C is the correct answer.

upvoted 2 times

## DRAG DROP

-

## Case Study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

## To start the case study

-

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

## Overview

-

## Company Information

-

ADatum Corporation is a manufacturing company that has a main office in Seattle and two branch offices in Los Angeles and Montreal.

## Fabrikam Partnership

-

ADatum recently partnered with 2 company named Fabrikam, Inc.

Fabrikam is a manufacturing company that has a main office in Boston and a branch office in Orlando.

Both companies intend to collaborate on several joint projects.

## Existing Environment

-

## ADatum AD DS Environment

-

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

The forest contains two domains named adatum.com and east.adatum.com and the domain controllers shown in the following table.

Name	Domain	Operations master roles
DC1	adatum.com	Schema master
DC2	adatum.com	None
DC3	east.adatum.com	PDC emulator, RID master

Fabrikam AD DS Environment

-

The on-premises network of Fabrikam contains an AD DS forest named fabrikam.com.

The forest contains two domains named fabrikam.com and south.fabrikam.com.

The fabrikam.com domain contains an organizational unit (OU) named Marketing.

Server Infrastructure

-

The adatum.com domain contains the servers shown in the following table.

Name	Role
HyperV1	Hyper-V
SSPace1	File and Storage Services

HyperV1 contains the virtual machines shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2022 Datacenter	Joined to the adatum.com domain Contains a file share named Data1 and a local user named User1
VM2	Red Hat Enterprise Linux (RHEL)	Contains a local user named User2
VM3	Windows Server 2022 Standard	Joined to the adatum.com domain Has the File and Storage Services role installed

All the virtual machines on HyperV1 have only the default management tools installed.

SSPace1 contains the Storage Spaces virtual disks shown in the following table.

Name	Number of physical disks	Redundancy
Disk1	8	Three-way mirror
Disk2	12	Parity

Azure Resources

-

ADatum has an Azure subscription that contains an Azure AD tenant. Azure AD Connect is configured to sync the adatum.com forest with Azure AD.

The subscription contains the virtual networks shown in the following table.

Name	Location	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	West US	SubnetA, SubnetB

The subscription contains the Azure Private DNS zones shown in the following table.

Name	Virtual network link
Zone1.com	VNet1
Zone2.com	VNet2
Zone3.com	None

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Security type
Server1	Windows Server 2022 Datacenter: Azure Edition	Trusted launch
Server2	Windows Server 2022 Datacenter: Azure Edition	Standard
Server3	Windows Server 2022 Datacenter	Standard
Server4	Windows Server 2019 Datacenter	Trusted launch

All the servers are in a workgroup.

The subscription contains a storage account named storage1 that has a file share named share1.

#### Requirements

-

#### Planned Changes

-

ADatum plans to implement the following changes:

- Sync Data1 to share1.
- Configure an Azure runbook named Task1.
- Enable Azure AD users to sign in to Server1.
- Create an Azure DNS Private Resolver that has the following configurations:
  - Name: Private1
  - Region: West US
  - Virtual network: VNet1
  - Inbound endpoint: SubnetB
- Enable users in the adatum.com domain to access the resources in the south.fabrikam.com domain.

#### Technical Requirements

-

ADatum identifies the following technical requirements:

- The data on SSPace1 must be available always.
- DC2 must become the schema master if DC1 fails.
- VM3 must be configured to enable per-folder quotas.
- Trusts must allow access to only the required resources.
- The users in the Marketing OU must have access to storage1.
- Azure Automanage must be used on all supported Azure virtual machines.
- A direct SSH session must be used to manage all the supported virtual machines on HyperV1.

DC1 fails.

You need to meet the technical requirements for the schema master.

You run ntdsutil.exe.

Which five commands should you run in sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order?

**Commands**

seize schema master

connect

connect to server dc2.adatum.com

roles

quit

metadata cleanup

>

<

**Answer Area**

**Answer Area**

roles

connect

connect to server dc2.adatum.com

quit

seize schema master

**Correct Answer:**

 **lucacose** Highly Voted 1 year ago

- run Ntdsutil.exe as stated in the question then:

- 1 Roles
- 2 Connections
- 3 Connect to server nameserver
- 4 quit
- 5 seize schema master

upvoted 10 times

 **Hull** Highly Voted 1 year, 2 months ago

Besides that "Connect" should be "Connections", it's correct.

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/transfer-or-seize-operation-master-roles-in-ad-ds#seize-or-transfer-operation-master-roles>

upvoted 8 times

 **ltkiller** 4 months, 3 weeks ago

Tip, in the tool you can use part of the commands, minimum 2 letters :)

try: pa ma, if it got 2 words use the 2 letters of each command.

So 'co' would bring you in connections.

upvoted 1 times

## Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

## To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

## Overview -

## Company Information -

ADatum Corporation is a manufacturing company that has a main office in Seattle and two branch offices in Los Angeles and Montreal.

## Fabrikam Partnership -

ADatum recently partnered with 2 company named Fabrikam, Inc.

Fabrikam is a manufacturing company that has a main office in Boston and a branch office in Orlando.

Both companies intend to collaborate on several joint projects.

## Existing Environment -

## ADatum AD DS Environment -

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

The forest contains two domains named adatum.com and east.adatum.com and the domain controllers shown in the following table.

Name	Domain	Operations master roles
DC1	adatum.com	Schema master
DC2	adatum.com	None
DC3	east.adatum.com	PDC emulator, RID master

## Fabrikam AD DS Environment -

The on-premises network of Fabrikam contains an AD DS forest named fabrikam.com.

The forest contains two domains named fabrikam.com and south.fabrikam.com.

The fabrikam.com domain contains an organizational unit (OU) named Marketing.

#### Server Infrastructure -

The adatum.com domain contains the servers shown in the following table.

Name	Role
HyperV1	Hyper-V
SSPace1	File and Storage Services

HyperV1 contains the virtual machines shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2022 Datacenter	Joined to the adatum.com domain Contains a file share named Data1 and a local user named User1
VM2	Red Hat Enterprise Linux (RHEL)	Contains a local user named User2
VM3	Windows Server 2022 Standard	Joined to the adatum.com domain Has the File and Storage Services role installed

All the virtual machines on HyperV1 have only the default management tools installed.

SSPace1 contains the Storage Spaces virtual disks shown in the following table.

Name	Number of physical disks	Redundancy
Disk1	8	Three-way mirror
Disk2	12	Parity

#### Azure Resources -

ADatum has an Azure subscription that contains an Azure AD tenant. Azure AD Connect is configured to sync the adatum.com forest with Azure AD.

The subscription contains the virtual networks shown in the following table.

Name	Location	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	West US	SubnetA, SubnetB

The subscription contains the Azure Private DNS zones shown in the following table.

Name	Virtual network link
Zone1.com	VNet1
Zone2.com	VNet2
Zone3.com	None

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Security type
Server1	Windows Server 2022 Datacenter: Azure Edition	Trusted launch
Server2	Windows Server 2022 Datacenter: Azure Edition	Standard
Server3	Windows Server 2022 Datacenter	Standard
Server4	Windows Server 2019 Datacenter	Trusted launch

All the servers are in a workgroup.

The subscription contains a storage account named storage1 that has a file share named share1.

Requirements -

Planned Changes -

ADatum plans to implement the following changes:

- Sync Data1 to share1.
- Configure an Azure runbook named Task1.
- Enable Azure AD users to sign in to Server1.
- Create an Azure DNS Private Resolver that has the following configurations:
  - Name: Private1
  - Region: West US
  - Virtual network: VNet1
  - Inbound endpoint: SubnetB
- Enable users in the adatum.com domain to access the resources in the south.fabrikam.com domain.

Technical Requirements -

ADatum identifies the following technical requirements:

- The data on SSPE1 must be available always.
- DC2 must become the schema master if DC1 fails.
- VM3 must be configured to enable per-folder quotas.
- Trusts must allow access to only the required resources.
- The users in the Marketing OU must have access to storage1.
- Azure Automate must be used on all supported Azure virtual machines.
- A direct SSH session must be used to manage all the supported virtual machines on HyperV1.

You need to ensure that access to storage1 for the Marketing OU users meets the technical requirements.

What should you implement?

- A. Active Directory Federation Services (AD FS)
- B. Azure AD Connect in staging mode
- C. Azure AD Connect cloud sync
- D. Azure AD Connect in active mode

**Correct Answer: C**

  **Ksk08** 8 months ago

Answer is C

Azure AD Connect cloud sync allows synchronization of on-premises Active Directory objects to Azure AD. This is essential for enabling Azure role-based access control (RBAC) for users in the Marketing OU, thereby granting them the necessary permissions to access storage1  
upvoted 1 times

  **MichalGr** 1 year, 2 months ago



While the Azure AD Connect Wizard might suffice for basic configurations, the Synchronization Rules Editor provides the necessary capabilities for more advanced scenarios involving custom attributes and filtering requirements.



upvoted 1 times

  **Leoanetor** 1 year, 7 months ago

Azure AD Connect cloud sync allows you to connect to multiple disconnected on-premises AD forests and provides multiple active agents for high availability. The tool does not connect to LDAP directories or support Pass-Through Authentication. It is not designed for large groups with up to 250,000 members.

Ref: <https://blog.quest.com/understanding-azure-ad-sync-an-overview-of-azure-ad-connect-sync-and-cloud-sync/#:~:text=Azure%20AD%20Connect%20cloud%20sync%20allows%20you%20to%20connect%20to,with%20up%20to%20250%2C000%20members.https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync>

upvoted 2 times

  **Jothar** 1 year, 7 months ago

Ok i'm confused. Why is it C and not D?

upvoted 3 times

  **Natthaphol** 1 year, 7 months ago

Because it 2 separate forests, we need Azure AD Cloud Sync to connect to multiple disconnected on-premises AD forests to Azure Tenant. Marketing OU is in fabrikam. <https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync>

upvoted 2 times

  **lucacose** 1 year, 6 months ago

Note that Azure AD Connect is different from Azure AD Connect Cloud Sync. The second one will allow you to sync object from different forest not in trust.

upvoted 2 times

Your network contains an Active Directory Domain Services (AD DS) domain.

You plan to use Active Directory Administrative Center to create a new user named User1.

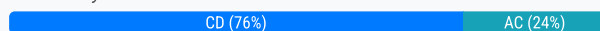
Which two attributes are required to create User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Password
- B. Profile path
- C. User SamAccountName logon
- D. Full name
- E. First name
- F. User UPN logon

**Correct Answer:** CD

Community vote distribution



**kkee321** Highly Voted 1 year, 5 months ago

**Selected Answer:** CD

When you are trying to create new account required fields are:

Full name:

and

User SamAccountName logon:

So the answer is correct C&D

upvoted 7 times

**himoumess** Most Recent 6 months, 2 weeks ago

**Selected Answer:** CD

Tried it in lab, in ADAC:

Full name: Clearly marked with an asterisk (\*), making it mandatory.

User SamAccountName (logon name): Also marked with an asterisk, making it required.

The user account is created but will remain disabled until you set the password.

upvoted 1 times

**formacaotismic** 7 months, 2 weeks ago

In ADAC console:

C,D

upvoted 2 times

**michoolly15** 8 months ago

The correct answer is Full name and User SamAccountName logon.

upvoted 1 times

**athadd** 12 months ago

It is C and D. When you open up ADAC, you choose New - User, and you have only two fields with asterisk. If password option is set "user must change password at next logon", while settings Full Name and User samaccountname, it will allow you to create a user.

upvoted 2 times

**TONPL\_Team** 1 year, 1 month ago

I have checked in ADAC, and try to create new user then it showing asterik in FullName and UserSAMAccountName so

Correct Answer is C, D

upvoted 3 times

**bpaccount** 1 year, 1 month ago

Selected Answer: AC

ChatGPT states:

To create a new user named User1 in Active Directory Administrative Center, the two required attributes are:

User logon name (also known as the User Principal Name or UPN)

Password

These are the minimum attributes needed to successfully create a new user account in Active Directory. Here's a brief explanation of each:

User logon name (UPN): This is the name that the user will use to log in to the domain. It typically has the format username@domain.com.

Password: This is the initial password for the user account. The password is necessary for the account to be able to authenticate and log in to the domain.

While other attributes like First name, Last name, Display name, and Email are often filled out and important for identification and communication purposes, they are not strictly required to create the account.

upvoted 2 times

🗳️ 👤 **AK\_1234** 1 year, 1 month ago

A and C

upvoted 1 times

🗳️ 👤 **SIAMIANJI** 1 year, 2 months ago

Selected Answer: CD

o create a new user named User1 using Active Directory Administrative Center, the following attributes are required:

C. User SamAccountName logon: This is the user's logon name in the pre-Windows 2000 format, also known as the SamAccountName or the User Logon Name.

D. Full name: This is the display name of the user, commonly referred to as the Full Name.

upvoted 2 times

🗳️ 👤 **Bluediamond** 1 year, 3 months ago

A and C

upvoted 1 times

🗳️ 👤 **Tuffgong** 1 year, 3 months ago

Correct answer is C only. When you create a user with ADAC it run command "New-ADUser" (check command history) that require Only the argument "Name" that correpnd to the SAMAccountName following these documentations : <https://learn.microsoft.com/en-us/powershell/module/activedirectory/new-aduser?view=windowsserver2022-ps> <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/advanced-ad-ds-management-using-active-directory-administrative-center--level-200->

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 3 months ago

The question literally says "which two attributes", it's definitely not C only.

Plus if you actually had opened ADAC and create a new user, you could see that the only 2 required field are C and D, as there are giant red asterisks next to those two fields.

upvoted 3 times

🗳️ 👤 **HoangNam2711** 1 year, 4 months ago

Selected Answer: CD

Absolutely C and D

upvoted 3 times

🗳️ 👤 **fbx01** 1 year, 4 months ago

Selected Answer: AC

A,C ANSWER

upvoted 2 times

🗳️ 👤 **rkNichols01** 1 year, 5 months ago



From Co-Pilot:

To create a new user named User1 using Active Directory Administrative Center, you need to provide the following two attributes:

First name: The first name of the user.



User logon name: The user logon name for the user 1.

upvoted 1 times

  **rd\_dr** 1 year, 6 months ago



password and samaccountname

upvoted 2 times

  **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 2 times

  **Jacbin** 1 year, 7 months ago

correct answer

upvoted 1 times

HOTSPOT

-

Your on-premises network contains an Active Directory Domain Services (AD DS) domain. The domain contains the servers shown in the following table.

Name	Description
DC1	Domain naming master, PDC emulator, and RID master
DC2	Schema master and infrastructure master
RODC1	Read-only domain controller (RODC)
Server1	Azure AD Connect server
Server2	Azure AD Application Proxy connector

The domain controllers do NOT have internet connectivity.

You plan to implement Azure AD Password Protection for the domain.

You need to deploy Azure AD Password Protection agents. The solution must meet the following requirements:

- All Azure AD Password Protection policies must be enforced.
- Agent updates must be applied automatically.
- Administrative effort must be minimized.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Install the Azure AD Password Protection agent on:

▼

DC1 only  
DC1 and DC2 only  
DC1, DC2, and RODC1

Install the Azure AD Password Protection Proxy on:

▼

DC1  
DC2  
RODC1  
Server1  
Server2

### Answer Area

Install the Azure AD Password Protection agent on:

DC1 only  
DC1 and DC2 only  
DC1, DC2, and RODC1

Correct Answer:

Install the Azure AD Password Protection Proxy on:

DC1  
DC2  
RODC1  
Server1  
Server2

 **RickySmith** Highly Voted 1 year, 6 months ago

Azure AD Password Protection agent - Only DC1 and DC2.

Agents need to be on full DC's as RODC's cannot process all password changes.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-deploy#read-only-domain-controller-considerations>

Azure AD Password Protection Proxy - Server1


-Needs to be on Member Server only

-Not compatible with RODC.

-Not compatible with AAD App Proxy.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-deploy#microsoft-entra-connect-agent-updater-prerequisites>

upvoted 8 times

 **Krayzr** 12 months ago

True. found on RickySmith's link

.

Warning

Microsoft Entra Password Protection proxy and Microsoft Entra application proxy install different versions of the Microsoft Entra Connect Agent Updater service, which is why the instructions refer to Application Proxy content. These different versions are incompatible when installed side by side and doing so will prevent the Agent Updater service from contacting Azure for software updates, so you should never install Microsoft Entra Password Protection Proxy and Application Proxy on the same machine.

upvoted 4 times

 **lucacose** Highly Voted 1 year, 6 months ago

Install Azure AD Password Protection -> Only DC1 and DC2

WHY? RODCs are not supported

Install Azure AD Password Protection Proxy -> Server1

WHY? You can't install AAD Password Protection PROXY (Now Microsoft Entra Password Proxy) in a server with Azure AD Application Connector proxy

Look for the prerequisite at this page:

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-deploy>

upvoted 5 times

 **Ksk08** Most Recent 8 months ago

Dc1 and dc2

Server 1

upvoted 1 times


 **Jools\_SP** 1 year, 5 months ago

Incorrect answer.

Microsoft Entra Password Protection proxy and Microsoft Entra application proxy install different versions of the Microsoft Entra Connect Agent

Updater service, which is why the instructions refer to Application Proxy content. These different versions are incompatible when installed side by side and doing so will prevent the Agent Updater service from contacting Azure for software updates, so you should never install Microsoft Entra Password Protection Proxy and Application Proxy on the same machine.

upvoted 2 times

  **Payday123** 1 year, 7 months ago

Is it a new question?

upvoted 1 times

## HOTSPOT

-

Your on-premises network contains a single-domain Active Directory Domain Services (AD DS) forest. You have an Azure AD tenant named contoso.com. The AD DS forest syncs with the Azure AD tenant by using Azure AD Connect.

You need to ensure that users in the forest that have a custom attribute of NoSync are excluded from synchronization.

How should you configure the Azure AD Connect cloudFiltered attribute, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Attribute:

	▼
False	
Null	
True	

Tool:

	▼
ADSI Edit	
Synchronization Rules Editor	
The Microsoft Azure AD Connect wizard	

**Answer Area**

Correct Answer:

Attribute:

	▼
False	
Null	
True	

Tool:

	▼
ADSI Edit	
Synchronization Rules Editor	
The Microsoft Azure AD Connect wizard	

 **boapaulo** Highly Voted 1 year, 7 months ago

To ensure that users in the forest who have a custom NoSync attribute are excluded from synchronization, you must configure the Azure AD Connect cloudFiltered attribute to True.

And the tool that you should use is the Synchronization Rules Editor.

With the Synchronization Rules Editor, you can create a custom inbound rule that sets the cloudFiltered attribute to True when the NoSync attribute is present. This will cause Azure AD Connect to exclude these users from synchronization. Keep in mind that any such change should be made with care to avoid unintended impacts on domain services and operations

upvoted 11 times

 **004b54b** Most Recent 10 months, 1 week ago

Given answer seems to be right:

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-installation-wizard#customize-synchronization-options> > doesn't mention attribute filtering (but does mention Domain, OU and Group filtering).

upvoted 1 times



🗨️ 👤 **mhmyz** 10 months, 2 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering>

Note

Microsoft Entra Cloud Sync and Microsoft Entra Connect Sync filter out any Active Directory objects where the `isCriticalSystemObject` attribute is set to `True`.

upvoted 2 times

🗨️ 👤 **bpaccount** 1 year, 1 month ago

Tested in lab setup, both Azure AD connect and Sync Rules editor seem to be a way to do this, and since it's missing the extra addition like "Least administrative effort", both answers are ok?

upvoted 3 times

🗨️ 👤 **SIAMIANJI** 1 year, 1 month ago

To exclude users with a custom attribute of `NoSync` from synchronization, you can configure the `cloudFiltered` attribute in Azure AD Connect. Here's how you can do it:

Configure the `cloudFiltered` Attribute:

The `cloudFiltered` attribute is used to exclude objects from synchronization to Azure AD. You can't directly set this attribute in Active Directory; instead, you'll create an inbound rule to set its value in the metaverse.

In Azure AD Connect, go to the Transformations section.

Click Add transformation.

Set the FlowType to Constant.

Set the Target Attribute to `cloudFiltered`.

In the Source field, enter `true`.

Which Tool to Use:

You'll use Azure AD Connect to configure the `cloudFiltered` attribute. This tool allows you to manage synchronization between your on-premises AD DS forest and Azure AD, ensuring that the specified users are excluded from synchronization

upvoted 1 times

🗨️ 👤 **lucacose** 1 year, 6 months ago

Attribute: `TRUE`

Tool: Microsoft Azure AD Connect

upvoted 1 times

🗨️ 👤 **Payday123** 1 year, 7 months ago

Seems to be correct

<https://www.youtube.com/watch?v=zYy0KAZBLQ0>

upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory Domain Services (AD DS) forest. The forest contains three Active Directory sites named Site1, Site2, and Site3. Each site contains two domain controllers. The sites are connected by using DEFAULTIPSITELINK.

You open a new branch office that contains only client computers.

You need to ensure that the client computers in the new office are primarily authenticated by the domain controllers in Site1.

Solution: You create a new site named Site4 and associate Site4 to DEFAULTIPSITELINK.

Does this meet the goal?


A. Yes

B. No

**Correct Answer:** B

Community vote distribution

B (100%)

 **RickySmith** Highly Voted 1 year, 6 months ago

**Selected Answer:** B

Same as q 17

upvoted 5 times

 **Krayzr** Most Recent 12 months ago

**Selected Answer:** B

Same as Questions 16, 17, 18, 19

upvoted 2 times

## SIMULATION

-

You need to create a group-managed service account (gMSA) named gMSA1 and make gMSA1 available on SRV1.

To complete this task, sign in to the required computer or computers.

**Correct Answer:**

To create a gMSA using the New-ADServiceAccount cmdlet.

Step 1: On the Windows Server 2012 domain controller (here SRV1), run Windows PowerShell from the Taskbar.

Step 2: At the command prompt for the Windows PowerShell, type the following commands, and then press ENTER.  
(The Active Directory module will load automatically.)

New-ADServiceAccount gMSA1

Enter the command on a single line.

Step 3: Install the gMSA on the host

The Install-ADServiceAccount cmdlet installs an existing gMSA on the server on which the cmdlet is run. Use the cmdlet with the following syntax:

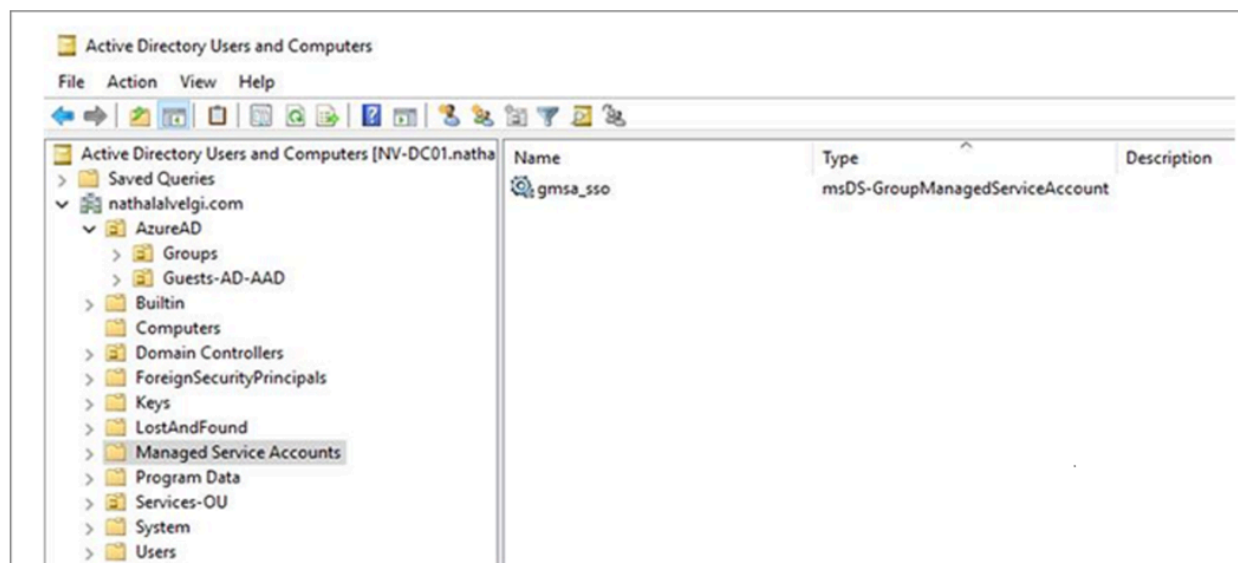
Install-ADServiceAccount `
 -Identity <ADServiceAccount>

Run the following PowerShell commands as administrator.

Install-ADServiceAccount gMSA1

Note: Managed Service Accounts container

To work effectively, gMSAs must be in the Managed Service Accounts container.



Reference:

<https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>

<https://learn.microsoft.com/en-us/entra/architecture/service-accounts-group-managed>

**Krayzr** 12 months ago

The first PS command will ask for a DNSHostName:

upvoted 2 times

**Krayzr** 6 months, 1 week ago

1. Open PowerShell as an Administrator on a domain controller.

2. Create the KDS Root Key (if not already created):

Add-KdsRootKey -EffectiveImmediately

3. Create the gMSA:

```
New-ADServiceAccount -Name gMSA1 -DNSHostName srv1.yourdomain.com -PrincipalsAllowedToRetrieveManagedPassword "Domain Computers"
```

4. Install the gMSA on SRV1:

Open PowerShell on SRV1 as an Administrator.



Install the AD module if not already installed:  
`Install-WindowsFeature RSAT-AD-PowerShell`



Install the gMSA:  
`Install-ADServiceAccount -Identity gMSA1`



5. Test the gMSA installation:

```
Test-ADServiceAccount -Identity gMSA1
```

If the test returns True, the gMSA is successfully installed and available on SRV1.  
upvoted 2 times

  **nonoelptirobo** 4 months, 1 week ago  
the dns hostname is for the GMSAname :  
`new-adserviceAccount -Name gMSA1 -DNShostname gMSA1.contoso.org -principalAllowedToRetrieveManagedPassword "group"`  
the the rest is correct  
upvoted 1 times

  **nonoelptirobo** 4 months, 1 week ago  
in this case "group" should be SRV1\$  
upvoted 1 times

  **bpaccount** 1 year, 1 month ago  
No need to check for a KDS Root key first?  
upvoted 4 times

## SIMULATION

-

You use a Group Policy preference to map \\dc1.contoso.com\install as drive H for all users. If a user already has an existing drive mapping for H, the new drive mapping must take precedence.

To complete this task, sign in to the required computer or computers.

**Correct Answer:**

## Mapping drives using Group Policy preferences

Steps involved:

1. Open Group Policy Management.
2. Right-click the domain or the required subfolder to create a new GPO, or select an already existing one. Right-click and select Edit to open the Group Policy Management Editor.
3. Go to User Configuration > Preferences > Windows Settings > Drive Maps.
4. Right-click and select New > Mapped Drive.
5. Under the General tab (see Figure below), do the following:

The screenshot shows the 'K: Properties' dialog box with the 'General' tab selected. The 'Common' sub-tab is also visible. The 'Action' dropdown is set to 'Update'. The 'Location' text box contains '\\Anjali-dc1\\c'. The 'Reconnect' checkbox is unchecked. The 'Label as' text box contains 'SharedDrive'. Under the 'Drive Letter' section, the 'Use:' radio button is selected, and the dropdown shows 'K'. The 'Connect as (optional)' section has empty text boxes for 'User name:', 'Password:', and 'Confirm password:'. Under 'Hide/Show this drive', the 'Show this drive' radio button is selected. Under 'Hide/Show all drives', the 'Show all drives' radio button is selected. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

6. Action: Select Create or Update.
7. Location: Specify the full file path, e.g. \\Anjali-dc1\\c.  
Specify: \\dc1.contoso.com\\install
8. Reconnect: Enable this to auto connect the drive.
9. Label as: Pick a suitable name for the shared drive, e.g. SharedDrive.
10. Drive Letter: Select a suitable letter for the drive, e.g. K.

Specify H

(11. Connect as: Enter a username and password if you want users to connect with certain credentials other than their own Windows login credentials.)

(12. Hide/Show this drive: Select whether you want to hide the folder or make it visible on the network.)

(13. Hide/Show all drives: Select whether, by default, all the shared drives/folders are hidden or visible.)

Reference:

<https://blogs.manageengine.com/active-directory/active-directory-academy/2019/11/18/mapping-drives-using-group-policy-preferences.html>

🗒️ 👤 **Webcatman** 7 months, 2 weeks ago

In screenshot step5 'Action' set to 'replace' --> If H drive exist map to other drive.  
upvoted 3 times

🗒️ 👤 **Fiscini** 8 months, 1 week ago

or just manage the GPO priority  
upvoted 1 times

🗒️ 👤 **Hull1** 9 months, 2 weeks ago

If you link the group policy to domain, I would also enforce the GPO to ensure it has precedence over other GPOs that might be linked to OUs and create H drives for users  
upvoted 1 times



## HOTSPOT

-

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com.

The domain contains the users shown in the following table.

Name	Located in
User1	Contoso.com
User2	Contoso.com/Users
User3	Contoso.com/OU1

The domain has the Group Policy Objects (GPOs) shown in the following table.

Name	Linked to
Default Domain Policy	Contoso.com
Default Domain Controllers Policy	Domain Controllers
GPO1	OU1

The GPOs are configured as shown in the following table.

GPO	Minimum password length
Default Domain Policy	8
Default Domain Controllers Policy	12
GPO1	10

For each of the following statements, select Yes if the statement is true, Otherwise, select No.

NOTE: Each correct selection is worth one point.

## Answer Area

## Statements

When User1 changes their password, at least eight characters must be used for the new password.

Yes

☐

No

☐

When User2 changes their password, at least 12 characters must be used for the new password.

☐☐

When User3 changes their password, at least 10 characters must be used for the new password.

☐☐

## Answer Area

## Statements

When User1 changes their password, at least eight characters must be used for the new password.

Yes

☒

No

☐

When User2 changes their password, at least 12 characters must be used for the new password.

☐

No

☒

When User3 changes their password, at least 10 characters must be used for the new password.

☒☐

Correct Answer:

6de0f77 Highly Voted 1 year, 3 months ago

No granular password policies are mentioned. So the Default Domain Policy is leading. In this case minimal password length of 8.

So:

YES

NO

NO

upvoted 12 times

🗨️ 👤 **[Removed]** 1 year, 3 months ago

You're correct.

To add to this, only 1 password policy can be in effect for a domain and can only be defined in the default domain policy, or in another GPO linked to the root domain and that would be given precedence.

The only way to have multiple is to use fine grained policies.

upvoted 2 times

🗨️ 👤 **Andmachado** 6 months, 3 weeks ago

Guys, I did the following test. I created an OU and a user. I added the user to this OU. I tested it by changing the password to 8 characters in the Default Domain Policy. Soon after, I created a GPO in the new OU, and created a GPO with only the minimum 10 characters. At first it didn't work, but I ran a gpupdate /force, and restarted the computer, and after the restart, it only worked with the 10 characters. So I believe the answer given is correct.

upvoted 2 times

🗨️ 👤 **Ksk08** Most Recent 🔍 8 months ago

YES NO NO

upvoted 2 times

🗨️ 👤 **starseed** 9 months, 2 weeks ago

answer is yes no no

upvoted 1 times

🗨️ 👤 **Krayzr** 12 months ago

YNN

should be the answer

upvoted 1 times

🗨️ 👤 **JimmyC** 1 year ago

This question tricked me since I forgot that password policy can only be applied at the root domain level, so I appreciate the other comments indicating that.

I just wanted to mention that User3 is also a red herring - password length is a Computer policy, so the fact that User3 resides in an OU where that policy is applied would make no difference unless loopback was enabled. It's a moot point, but important in its own way in case that failed to trip something in your head.

upvoted 1 times

🗨️ 👤 **JimmyC** 1 year ago

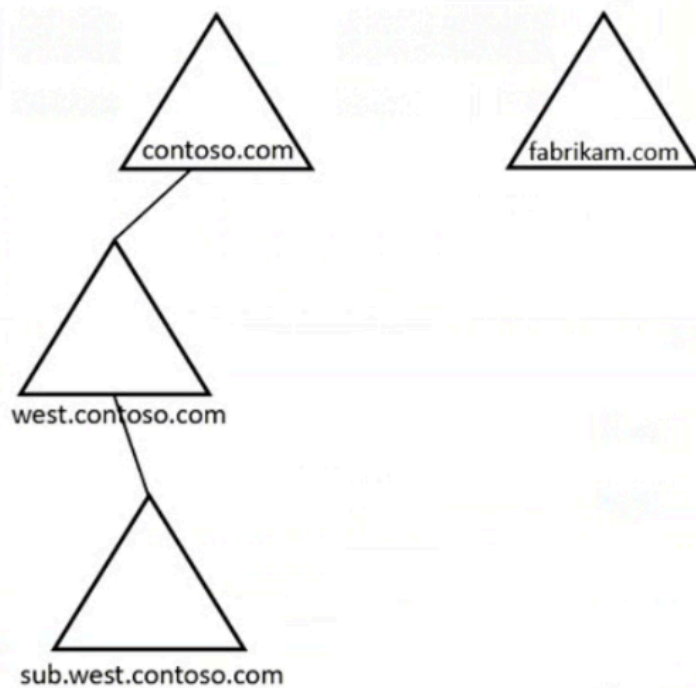
Actually I take back my mention of loopback as well - it works for user policy in a computer OU, not computer policy in a user OU. So forget I mentioned it - computer policy in a user OU would simply never be enforced (unless the user and computer both reside in that same OU).

upvoted 2 times

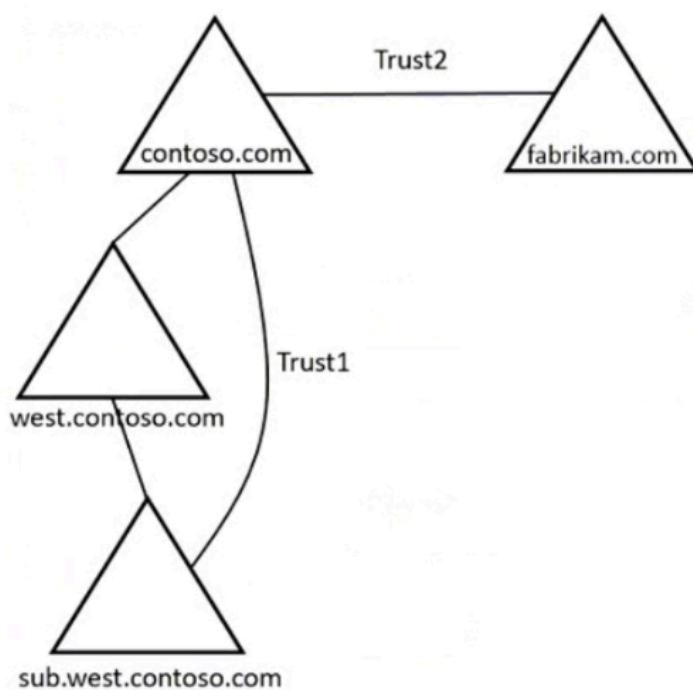
## HOTSPOT

-

Your network contains the domains shown in the following exhibit.



You need to establish trust relationships as shown in the following exhibit.



Which type of trust can you use for Trust1 and Trust2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Trust1:

- External trust only
- Forest trust only
- Shortcut trust only
- Forest trust or external trust only
- Forest trust, shortcut trust, or external trust

Trust2:

- Forest trust only
- External trust or shortcut trust only
- Forest trust or shortcut trust only
- Forest trust or external trust only
- Forest trust, shortcut trust, or external trust

### Answer Area

Correct Answer:

Trust1:

- External trust only
- Forest trust only
- Shortcut trust only**
- Forest trust or external trust only
- Forest trust, shortcut trust, or external trust

Trust2:

- Forest trust only
- External trust or shortcut trust only
- Forest trust or shortcut trust only
- Forest trust or external trust only**
- Forest trust, shortcut trust, or external trust

 **jrodthelegend** Highly Voted 7 months ago

Answer is correct

Trust 1: Shortcut Only

Trust 2: Forest Trust or External Trust

upvoted 14 times

 **RucasII** Most Recent 4 months, 2 weeks ago

Trust 1: Shortcut Only

Trust 2: Because External Trust is  
one way only, has to be Forest Trust  
upvoted 1 times

 **chiiaa** 9 months, 1 week ago

Trust 1 - forest trust or external trust

Trust 2- foresr trust only

upvoted 3 times

## HOTSPOT

-

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains the users shown in the following table.

Name	Located in
User1	Contoso\Users
User2	Contoso\OU1
User3	Contoso\OU1\OU2

The domain has the Group Policy Objects (GPOs) shown in the following table.

Name	Linked to	Enforcement
GPO1	Contoso.com	Enforce is enabled for the GPO link.
GPO2	OU1	None
GPO3	OU2	Block inheritance is enabled for OU2.

The GPOs are configured to map a drive named H as shown in the following table.

Name	Configuration
GPO1	Drive H maps to \\server1\share.
GPO2	Drive H maps to \\server2\share.
GPO3	Drive H maps to \\server3\share.

For each of the following statements, select Yes if the statement is true, Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
For User1, \\server2\share maps to drive H.	<input type="radio"/>	<input type="radio"/>
For User2 \\server1\share maps to drive H.	<input type="radio"/>	<input type="radio"/>
For User3, \\server3\share maps to drive H.	<input type="radio"/>	<input type="radio"/>

### Answer Area

	Statements	Yes	No
Correct Answer:	For User1, \\server2\share maps to drive H.	<input type="radio"/>	<input checked="" type="radio"/>
	For User2 \\server1\share maps to drive H.	<input checked="" type="radio"/>	<input type="radio"/>
	For User3, \\server3\share maps to drive H.	<input checked="" type="radio"/>	<input type="radio"/>

  **makonmakon** Highly Voted 1 year, 3 months ago

N/Y/N

Enforced. If the GPO link is enforced, it cannot be blocked at a lower-level (in the Group Policy processing hierarchy) container.

<https://learn.microsoft.com/en-us/powershell/module/grouppolicy/set-gplink?view=windowsserver2022-ps>

upvoted 17 times

  **Itkiller** 5 months ago

N/Y/N, but also, containers dont get policies, Domain\Users is a container, not an OU. You simply cant see containers in GPO management!

upvoted 1 times

  **nublit** 9 months, 2 weeks ago

When you block inheritance on an Organizational Unit (OU) in Active Directory, it prevents Group Policy Objects (GPOs) from parent OUs from being applied to that OU. However, enforced GPOs (also known as "No Override" GPOs) will still apply to the child OU, even if inheritance is blocked.

Enforced GPOs take precedence over linked GPOs on the OU where the user object resides. When a GPO is enforced (No Override), it ensures that its settings apply regardless of any other GPOs linked to the OU, even if those GPOs would normally have higher precedence.

upvoted 2 times

  **egdeeptha** Most Recent 11 months ago

User 3 is in OU2, GPO3 has \\Server3\share and GPO 3 is attached to OU2 directly, therefore \\Server3\share maps to User3


upvoted 4 times

  **zuzmo483** 4 months ago

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-processing>

Enforced is a link property, and block policy inheritance is a container property. Enforced takes precedence over block policy inheritance.

upvoted 1 times

  **Andmachado** 6 months, 2 weeks ago

I agree. I also tested it in the environment, and server3 was mapped to user3.



N, Y, Y.

upvoted 2 times

  **e489b39** 3 weeks, 6 days ago

What about the forced GPO ? have you got 2 H drive ?!

upvoted 1 times

  **thomasemr** 4 months, 1 week ago


Only if the Action is Create, if you change to Replace, the user3 map GPO1 , I agree N,Y,Y

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Agree with you. Answer is No, Yes, Yes

upvoted 2 times

  **SIAMIANJI** 1 year, 1 month ago

The correct answers:

N

Y

N

upvoted 1 times

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains a user named User1. User1 is a member of a group named Group1 and is in an organizational unit (OU) named OU1.

The domain has minimum password lengths configured as shown in the following table.

Value	Location
10	Default Domain Policy
12	Default Domain Controllers Policy
8	Group Policy linked to OU1
14	Password settings object applied to Group1
7	Password settings object applied to User1

What is the minimum password length that User1 should use when changing to a new password?

- A. 7
- B. 8
- C. 10
- D. 12
- E. 14

**Correct Answer: A**

Community vote distribution

A (86%)

14%

 **Jothar** 7 months, 2 weeks ago

A is correct. I would like to point out that, if it's not a Password Settings Object, the ONLY gpo that can create a password length policy is default domain policy. A gpo linked to an ou with a password policy will never apply.

upvoted 1 times

 **Itkiller** 5 months ago

True but the question is incomplete. 2 Password settings with the same precedence, the lowest GUID will win. Password settings can apply to Users and Groups and take Precedence over Default Domain GPO.

upvoted 1 times

 **Itkiller** 4 months, 3 weeks ago

Correction: Even if an FGPP assigned to a security group has a precedence of 1, a directly assigned FGPP still takes priority over it!

upvoted 1 times

 **monisshk** 11 months, 1 week ago

Correct answer: A

Tested in LAB.

upvoted 2 times

 **Krayzr** 12 months ago

**Selected Answer: A**

Seems to be correct

upvoted 1 times

 **bpaccount** 1 year, 1 month ago

**Selected Answer: A**

A is correct. Tested it.

upvoted 1 times

 **IcE** 1 year, 1 month ago

**Selected Answer: E**

User1 is apart of Group1. In AD, the most specific policy applies

upvoted 1 times

 **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: A**

When determining the minimum password length that User1 should use when changing to a new password, the following precedence order should be considered:

Password Settings object applied directly to the user (User1).

Password Settings object applied to the user's group (Group1).

Group Policy linked to the user's organizational unit (OU1).

Default Domain Policy.

Default Domain Controllers Policy.

Based on the precedence order and the configuration provided:

Password Settings object applied to User1: 7

Password Settings object applied to Group1: 14

Group Policy linked to OU1: 8

Default Domain Policy: 10

Default Domain Controllers Policy: 12

User1's minimum password length will be determined by the Password Settings object applied directly to the user (User1), which specifies a minimum password length of 7 characters. Therefore, User1 should use a minimum password length of 7 characters when changing to a new password.

upvoted 4 times

 **KatinTeam** 1 year, 1 month ago

I'd say this is correct.

PSO applied to User (highest precedence)

If no PSO applied to User, then PSO applied to Group

If no PSO for User and Group, then GPO linked to OU

Default Domain Policy

Default Domain Controllers Policy

Answer is A: 7

upvoted 4 times



## SIMULATION

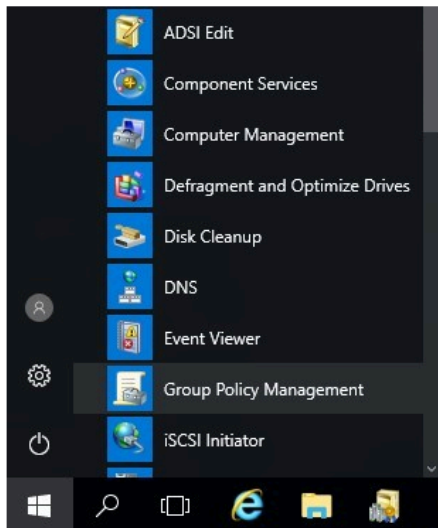
-

You need to create a Group Policy Object (GPO) named GPO1 that only applies to a group named MemberServers.

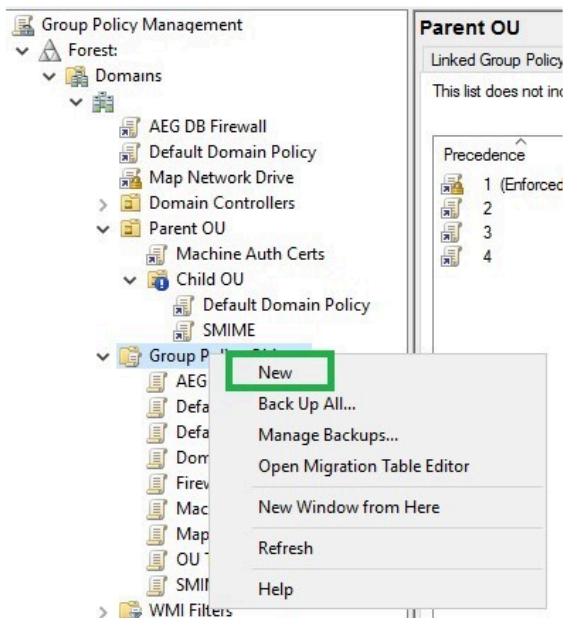
To complete this task, sign in the required computer or computers.

Correct Answer:

Step 1: Open Group Policy Management by navigating to the Start menu > Windows Administrative Tools, then select Group Policy Management.



Step 2: Right-click Group Policy Objects, then select New to create a new GPO.



Step 3: Enter a name [here GPO1] for the new GPO that you can identify what it is for easily, then click OK.

Step 4: Select the GPO from Group Policy Objects list, then in the Security Filtering section, Add and Remove users, groups, and computers that the GPO should apply to. [Here add group MemberServers]

Step 5: Close the GPO Editor when you are done.

Now, the GPO is created.

Reference:

<https://support.globalsign.com/aeg/aeg-how-create-and-link-gpo-active-directory>

 **smorar** Highly Voted 7 months, 1 week ago

Could you tell me how to answer this question? In the exam, do we have to connect to another PC to run the exercise like a laboratory?

Thanks.

upvoted 5 times

Your network contains an Active Directory Domain Services (AD DS) forest named contoso.com. The forest contains the domain controllers shown in the following table.

Name	Operations master role
DC1	Schema master
DC2	Infrastructure master
DC3	Domain naming master
DC4	PDC emulator, RID master

You have a partner organization that has an AD DS forest named fabrikam.com.

You create a trust relationship between contoso.com and fabrikam.com.

You need to configure selective authentication for the trust relationship.



Which domain controller should be granted permissions to fabrikam.com?

- A. DC1
- B. DC2
- C. DC3
- D. DC4

**Correct Answer: D**

Community vote distribution

D (100%)

  **Krayzr** 7 months, 2 weeks ago

**Selected Answer: D**

The PDC emulator is responsible for handling authentication requests and password changes, making it the appropriate domain controller for managing selective authentication settings.

[https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-adts/f96ff8ec-c660-4d6c-924f-c0dbbcac1527](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/f96ff8ec-c660-4d6c-924f-c0dbbcac1527)

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Answer : DC4

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

The PDC emulator (DC4) is the domain controller responsible for handling these trust-related tasks.

upvoted 1 times

You have a Microsoft Entra Domain Services domain named contoso.com.

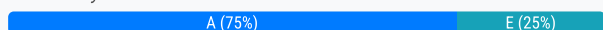
You need to provide an administrator with the ability to manage Group Policy Objects (GPOs). The solution must use the principle of least privilege.

To which group should you add the administrator?

- A. AAD DC Administrators
- B. Domain Admins
- C. Schema Admins
- D. Enterprise Admins
- E. Group Policy Creator Owners

**Correct Answer: A**

*Community vote distribution*



🗳️ 👤 **AnonChen** 4 weeks, 1 day ago

**Selected Answer: A**

Co-Pilot:

AAD DC Administrators

This group is specific to Microsoft Entra Domain Services.

Members of this group have administrative privileges in the managed domain, including the ability to:

Create and manage GPOs

Administer domain-joined machines

Manage users and groups within the domain

This group is the least privileged group that still allows full GPO management in Entra Domain Services.

E. Group Policy Creator Owners

Allows users to create new GPOs, but not manage existing ones.

Also, in Entra Domain Services, this group is not typically used or exposed.

upvoted 1 times

🗳️ 👤 **SunRise** 6 months ago

**Selected Answer: A**

Please do your research by if my analysis is right:

The question is talking about Entra DS, not on-prim, so if I am not mistake there no group as GP Creator Owner there, the the Answer should be A

upvoted 2 times

🗳️ 👤 **Krayzr** 6 months, 2 weeks ago

**Selected Answer: A**

AAD AD Admins

upvoted 3 times

🗳️ 👤 **VirtuaTech** 6 months, 3 weeks ago

**Selected Answer: E**

Group Policy Creator Owners = Just the right access to just manage GPOs

upvoted 2 times

🗳️ 👤 **Ksk08** 8 months, 2 weeks ago



Answer is E

upvoted 2 times

🗳️ 👤 **Abdullah993** 8 months, 1 week ago

Answer is A

upvoted 5 times

  **Ksk08** 7 months, 1 week ago

Imagine a building with many rooms:

Domain Admins = Access to everything (too much)



Enterprise Admins = Access to multiple buildings (way too much)

Schema Admins = Access to building blueprints (wrong type of access)

AAD DC Administrators = Access to different areas (not specific enough)

Group Policy Creator Owners = Just the right access to just manage GPOs

upvoted 1 times

  **FERNFHIT** 6 months, 3 weeks ago

Wrong. The Group Policy Creator Owners group lets its members create new GPOs. However, those members can only edit or delete GPOs that they have created. The Group Policy Creator Owners group also has no permission to link GPOs to a container such as a domain or OU.... therefor members of that group cannot sufficiently manage group policies.

upvoted 3 times

## HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. Contoso.com contains an organizational unit (OU) named OU1.

You have an Azure subscription that is linked to a Microsoft Entra tenant named fabrikam.com.

You need to sync contoso.com with fabrikam.com. The solution must meet the following requirements:

- Support Windows Hello for Business by using a hybrid certificate deployment.
- Ensure that the passwords in contoso.com do NOT sync to fabrikam.com.

Which Microsoft Entra Connect feature should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Support Windows Hello for Business by using a hybrid certificate deployment:

Device writeback  
Pass-through authentication  
Password hash synchronization  
Password writeback

Ensure that the passwords in contoso.com do NOT sync with fabrikam.com:

Device writeback  
Pass-through authentication  
Password hash synchronization  
Password writeback

## Answer Area

Support Windows Hello for Business by using a hybrid certificate deployment:

Device writeback  
Pass-through authentication  
Password hash synchronization  
Password writeback

## Correct Answer:

Ensure that the passwords in contoso.com do NOT sync with fabrikam.com:

Device writeback  
Pass-through authentication  
Password hash synchronization  
Password writeback

 **Krayzr** 7 months, 2 weeks ago

Support Windows Hello for Business by using a hybrid certificate deployment:

Device writeback. This feature is necessary for hybrid certificate trust deployments as it allows devices to be registered in Microsoft Entra ID.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization>

Ensure that the passwords in contoso.com do NOT sync with fabrikam.com:

Pass-through authentication. This feature allows users to authenticate using their on-premises passwords without syncing the password hashes to Microsoft Entra ID.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta>

upvoted 3 times

 **Ksk08** 8 months, 2 weeks ago

Answer is correct

upvoted 3 times

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains two servers named Server1 and Server2 and the users shown in the following table.

Name	Member of
User1	Contoso\Administrators
User2	Contoso\Remote Management Users
User3	Server2\Administrators
User4	Server2\Remote Management Users

Which users can establish a PowerShell remoting session from Server1 to Server2?

- A. User1 and User3 only
- B. User2 and User4 only
- C. User3 and User4 only
- D. User1, User3, and User4 only
- E. User1, User2, User3, and User4

**Correct Answer: C**

Community vote distribution



**AnonChen** 4 weeks, 1 day ago

**Selected Answer: C**

ChatGPT:

User3 Server2\Administrators ✓ Yes (Local admin on Server2)

User4 Server2\Remote Management Users ✓ Yes (Member of allowed remote group on Server2)

✓ Correct Answer:

C. User3 and User4 only

These two users have appropriate local rights on Server2, which is required for PowerShell remoting from Server1 to Server2.

upvoted 1 times

**ppardav** 1 month, 3 weeks ago

**Selected Answer: C**

domain\administrators and domain\remote management users are not added by default to computers

upvoted 2 times

**SDK76** 2 months, 1 week ago

**Selected Answer: E**

By default, PowerShell Remoting only allows connections from members of the Administrators group. However, members of the Remote Management Users group also have access to PowerShell Remoting starting from PowerShell 4.0. This group is created by default and allows users to connect remotely without requiring full administrator privileges.

upvoted 1 times

**Westied78** 2 months, 1 week ago

**Selected Answer: C**

User 1 and 2 are domain users, Server 2 is not domain-joined, they therefore have no permissions. It has to be C users 3 and 4 only.

upvoted 1 times

**ScKn** 1 month, 3 weeks ago

Server2 is in the domain as well

upvoted 1 times

**zuzmo483** 4 months ago

**Selected Answer: A**



<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#remote-management-users>

Use the Remote Management Users group to allow users to manage servers through the Server Manager console. Use the WinRMRemoteWMIUsers\ group to allow users to remotely run Windows PowerShell commands.

upvoted 2 times

🗨️ 👤 **RayFXWang** 4 months ago

**Selected Answer: C**

User1 and User1 have permission on domain controller only, no permission on server1 and server2.

upvoted 2 times

🗨️ 👤 **Tvoja\_mt** 1 month, 3 weeks ago

This is the correct answer

upvoted 1 times

🗨️ 👤 **brunosilvam** 4 months, 2 weeks ago

**Selected Answer: A**

To create remote sessions and run remote commands, by default, the current user must be a member of the Administrators group on the remote computer or provide the credentials of an administrator. Otherwise, the command fails.

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_requirements?view=powershell-7.5](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements?view=powershell-7.5)

upvoted 1 times

🗨️ 👤 **Itkiller** 5 months ago

**Selected Answer: A**

User1 and User3 only, default ONLY administrators.

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_requirements?view=powershell-7.5#user-permissions](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements?view=powershell-7.5#user-permissions)

upvoted 1 times

🗨️ 👤 **Itkiller** 5 months ago

in both powershell 7 and 5

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_requirements?view=powershell-5.1#user-permissions](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements?view=powershell-5.1#user-permissions)

upvoted 1 times

🗨️ 👤 **Itkiller** 4 months, 3 weeks ago

So default U1 and U3, but since U2/U4 are member of Remote Management Users, Everyone! (E), cant change my mistake tho :P

upvoted 1 times

🗨️ 👤 **FERNFHIT** 6 months, 3 weeks ago

**Selected Answer: D**

User1: Benutzer, die in einer Domänen-Administratoren-Gruppe sind, verfügen in der Regel über lokale Administratorrechte auf allen Domänenservern (sofern dies nicht explizit entzogen wurde). Somit kann User1 sich per PowerShell Remoting mit Server2 verbinden.

User3: Als lokaler Administrator auf Server2 hat User3 standardmäßig Zugriff auf PowerShell-Remoting-Sessions zu Server2.

User4: Mitglieder dieser lokalen Gruppe dürfen standardmäßig auf Server2 per PowerShell remoten. Da User4 in dieser Gruppe ist, erhält er ebenfalls Zugriff.

User2: Die reine Mitgliedschaft in einer Domänen-Remote-Management-Gruppe bedeutet nicht automatisch lokale Rechte auf Server2. Da User2 nicht in der lokalen "Remote Management Users"-Gruppe von Server2 ist, erhält er keinen Zugriff.

upvoted 1 times

🗨️ 👤 **formacaotismic** 7 months, 1 week ago

**Selected Answer: E**

User1 (contoso/administrators): Pode estabelecer uma sessão remota, pois é membro do grupo Administrators no domínio contoso.

User2 (contoso/Remote Management Users): Pode estabelecer uma sessão remota, pois é membro do grupo Remote Management Users no domínio contoso.

User3 (Server2/administrators): Pode estabelecer uma sessão remota, pois é membro do grupo Administrators no Server2.

User4 (Server2/Remote Management Users): Pode estabelecer uma sessão remota, pois é membro do grupo Remote Management Users no Server2.

upvoted 2 times

🗨️ 👤 **formacaotismic** 7 months, 2 weeks ago

E

User1 (contoso/administrators): Pode estabelecer uma sessão remota, pois é membro do grupo Administrators no domínio contoso.

User2 (contoso/Remote Management Users): Pode estabelecer uma sessão remota, pois é membro do grupo Remote Management Users no domínio contoso.



User3 (Server2/administrators): Pode estabelecer uma sessão remota, pois é membro do grupo Administrators no Server2.

User4 (Server2/Remote Management Users): Pode estabelecer uma sessão remota, pois é membro do grupo Remote Management Users no Server2.  
upvoted 1 times


  **Krayzr** 7 months, 2 weeks ago

**Selected Answer: E**

By default, members of the Administrators group and the Remote Management Users group can initiate PowerShell remoting sessions  
upvoted 1 times

  **Jothar** 7 months, 2 weeks ago

Change that. A because contoso admins would have the same rights. so both admins could remote in.  
upvoted 1 times

  **Jothar** 7 months, 2 weeks ago

C. From google ai: User Permissions:

By default, only members of the Administrators group on the remote computer have permission to use PowerShell remoting. However, you can configure it to allow non-administrative users by granting them Execute permissions to the appropriate session configurations.  
upvoted 1 times

  **Ksk08** 7 months, 2 weeks ago

D is correct  
upvoted 1 times

  **0b2ca83** 8 months ago

D right?  
upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Answer is A. user 1 and 3 since they have the administrator right  
upvoted 1 times

## HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. Contoso.com contains an organizational unit (OU) named OU1.

You have an Azure subscription named Sub1 that is linked to a Microsoft Entra tenant named fabrikam.com. Fabrikam.com syncs with contoso.com.

In Sub1, you create a Microsoft Entra Domain Services domain configured as shown in the following table.

Property	Value
DNS domain name	domain1.onmicrosoft.com
Location	East US
IP addresses	East US/10.0.2.5 10.0.2.4
Secure LDAP	Disabled
Secure LDAP external IP addresses	East US/52.188.201.46
Synchronization	All
Admin group	AAD DC Administrators

In domain1.onmicrosoft.com, you create two OUs named OU1 and OU2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area****Statements****Yes****No**

If you add a user named User1 to OU1 in contoso.com, User1 will sync with the AADDC Users OU in domain1.onmicrosoft.com.

☐☐

If you add a user named User2 to OU2 in domain1.onmicrosoft.com, User2 will sync with fabrikam.com.

☐☐

If you add a user named User3 to fabrikam.com, User3 will sync with the Users container in domain1.onmicrosoft.com.

☐☐**Correct Answer:****Answer Area****Statements****Yes****No**

If you add a user named User1 to OU1 in contoso.com, User1 will sync with the AADDC Users OU in domain1.onmicrosoft.com.

☐☒

If you add a user named User2 to OU2 in domain1.onmicrosoft.com, User2 will sync with fabrikam.com.

☐☒

If you add a user named User3 to fabrikam.com, User3 will sync with the Users container in domain1.onmicrosoft.com.

☒☐

  **b3cbdd9** Highly Voted 8 months ago

stop trolling @Ksk08

upvoted 8 times

  **Krayzr** Highly Voted 7 months, 2 weeks ago

Y N Y

Yes.

Users in the on-premises AD DS domain (contoso.com) that are synchronized to Microsoft Entra ID (fabrikam.com) will be synchronized to the AADDC Users OU in the managed domain (domain1.onmicrosoft.com)

No.

Synchronization in Microsoft Entra Domain Services is one-way from Microsoft Entra ID to the managed domain. Users created in the managed domain (domain1.onmicrosoft.com) do not sync back to Microsoft Entra ID (fabrikam.com).

Yes.

Users created in Microsoft Entra ID (fabrikam.com) will be synchronized to the managed domain (domain1.onmicrosoft.com) and placed in the AADDC Users OU1.



<https://learn.microsoft.com/en-us/entra/identity/domain-services/synchronization>

upvoted 5 times

  **Ksk08** Most Recent 8 months, 1 week ago

Confirm answer is yes no yes

upvoted 1 times

  **Ksk08** 7 months, 2 weeks ago

it is correct yes no yes

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Sorry answer should be Yes No No bcause sync should only happend one way direction

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Answer is Yes no Yes

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Sorry is No Yes Yes

upvoted 1 times

## HOTSPOT

-

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com.

You have a Microsoft Entra tenant.

You need to implement Microsoft Entra Connect Sync. The solution must meet the following requirements:

- Prevent the password hashes of contoso.com from being synced to the Microsoft Entra tenant.
- Minimize user effort when authenticating to Microsoft Entra registered apps.
- Minimize the number of on-premises infrastructure components.

What should you include in the solution for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Prevent contoso.com password hashes from being synced to the tenant:

Federation with Active Directory Federation Services (AD FS)

Pass-through authentication

Password hash synchronization

Single sign-on (SSO)

Minimize user effort when authenticating to Microsoft Entra registered apps:

Federation with Active Directory Federation Services (AD FS)

Pass-through authentication

Password hash synchronization

Single sign-on (SSO)

**Correct Answer:****Answer Area**

Prevent contoso.com password hashes from being synced to the tenant:

Federation with Active Directory Federation Services (AD FS)

Pass-through authentication

Password hash synchronization

Single sign-on (SSO)

Minimize user effort when authenticating to Microsoft Entra registered apps:

Federation with Active Directory Federation Services (AD FS)

Pass-through authentication

Password hash synchronization

Single sign-on (SSO)

  **Krayzr** 7 months, 2 weeks ago

**\*\*Prevent the password hashes of contoso.com from being synced to the Microsoft Entra tenant:**

Pass-through authentication. This method allows users to authenticate using their on-premises passwords without syncing the password hashes to Microsoft Entra ID1.

**\*\*Minimize user effort when authenticating to Microsoft Entra registered apps:**

Single sign-on (SSO). This feature allows users to sign in once and gain access to all their applications without needing to re-enter their credentials2.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta>

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn>

upvoted 4 times

  **Ksk08** 8 months, 2 weeks ago

Answer is Correct

upvoted 1 times

**HOTSPOT -**

You have 10 on-premises servers that run Windows Server.

You plan to use Azure Network Adapter to connect the servers to the resources in Azure.

Which prerequisites do you require on-premises and in Azure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

To configure the on-premises servers, use:

Azure CLI
Routing and Remote Access
Server Manager
Windows Admin Center

To connect the Azure resources and Azure Network Server Manager Adapter, use:

Azure Bastion
Azure Firewall
An Azure virtual network gateway
A private endpoint
A public Azure Load Balancer

Correct Answer:

**Answer Area**

To configure the on-premises servers, use:


Azure CLI
Routing and Remote Access
Server Manager
Windows Admin Center

To connect the Azure resources and Azure Network Server Manager Adapter, use:

Azure Bastion
Azure Firewall
An Azure virtual network gateway
A private endpoint
A public Azure Load Balancer

Reference:

<https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter>

 **syu31svc** Highly Voted 1 year, 9 months ago

From the provided link

A Windows Admin Center connection to Azure

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

Answer is correct

upvoted 6 times

🗒️ 👤 **AvoKikinha** Highly Voted 🏆 2 years, 7 months ago

Requirements

Using Azure Network Adapter to connect to a virtual network requires the following:

An Azure account with at least one active subscription.

An existing virtual network.

Internet access for the target servers that you want to connect to the Azure virtual network.

A Windows Admin Center connection to Azure. To learn more, see [Configuring Azure integration](#).

The latest version of Windows Admin Center. To learn more, see [Windows Admin Center](#).

upvoted 6 times

🗒️ 👤 **SIAMIANJI** Most Recent 🔍 8 months ago

On-Premises: Install Windows Admin Center and configure Azure Network Adapter.

Azure: Create an existing virtual network gateway

upvoted 2 times

🗒️ 👤 **Jacbin** 1 year, 1 month ago

correct answer

upvoted 1 times

🗒️ 👤 **RickySmith** 1 year, 3 months ago

Windows Admin Center

An Azure virtual network gateway

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter>

upvoted 2 times

🗒️ 👤 **Leocan** 2 years, 1 month ago

Azure Network Adapter uses Point-to-Site VPN connections, so a Virtual Network Gateway is required.

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter>

upvoted 4 times

🗒️ 👤 **Jawad1462** 2 years, 2 months ago

Given answers are correct

upvoted 2 times

🗒️ 👤 **Contactfornitish** 2 years, 4 months ago

Still valid, in exam on 23rd Aug'22

upvoted 3 times



## DRAG DROP -

You have a server named Server1 that has Windows Admin Center installed. The certificate used by Windows Admin Center was obtained from a certification authority (CA).

The certificate expires.

You need to replace the certificate.

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

Select and Place:

## Actions

- Obtain and install a new certificate.
- From Internet Information Services (IIS) Manager, bind a certificate.
- Run **Windows Admin Center Setup** and select **Remove**.
- Run **Windows Admin Center Setup** and select **Repair**.
- Run **Windows Admin Center Setup** and select **Change**.
- Copy the certificate thumbprint.

## Answer Area



## Correct Answer:

## Actions

- From Internet Information Services (IIS) Manager, bind a certificate.
- Run **Windows Admin Center Setup** and select **Remove**.
- Run **Windows Admin Center Setup** and select **Repair**.

## Answer Area

Run **Windows Admin Center Setup** and select **Change**.

Obtain and install a new certificate.

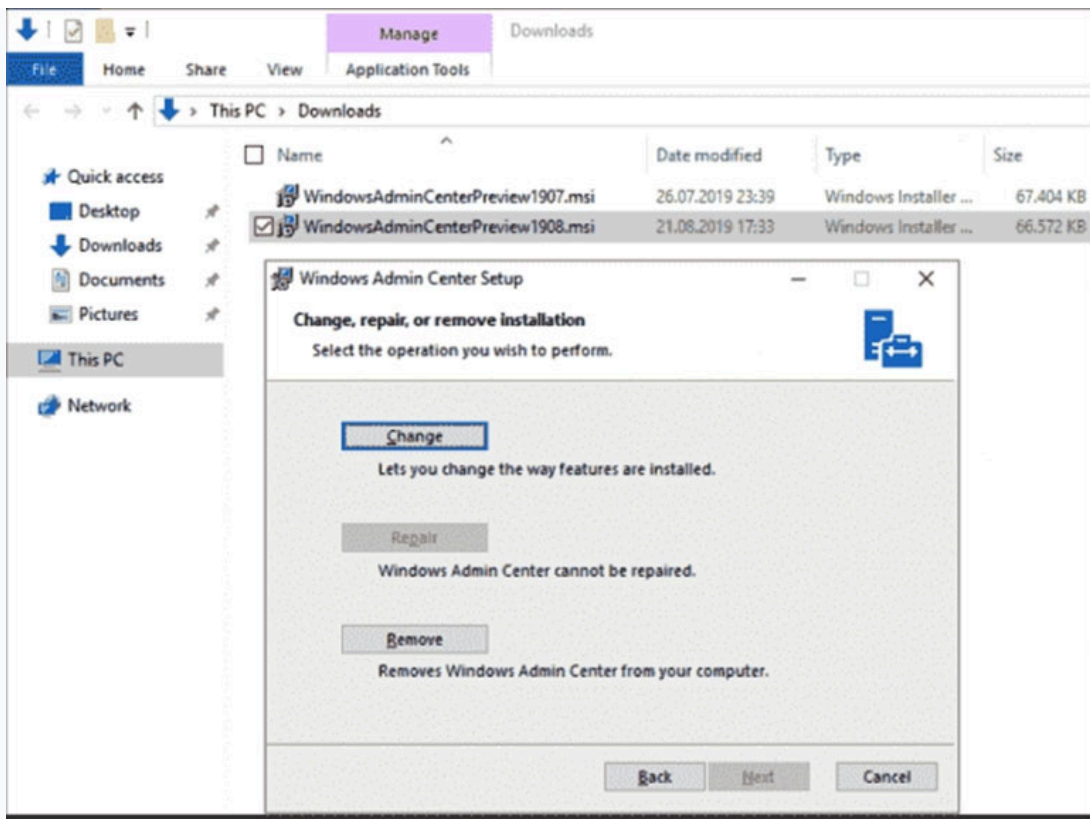
Copy the certificate thumbprint.



Step 1: Run Windows Admin Center Setup and select Change.

Updating the certificate used by Windows Admin Center

When you have Windows Admin Center deployed as a service, you must provide a certificate for HTTPS. To update this certificate at a later time, re-run the installer and choose change.



Step 2: Obtain and install a new certificate.

Step 3: Copy the certificate thumbprint.

The final step is to copy the certificate's thumbprint into the setup soon after installing it into the local store.

Reference:

<https://4sysops.com/archives/install-an-ssl-certificate-in-windows-admin-center/>

**Goofer** Highly Voted 1 year, 11 months ago

In my test on Wondows Server 2022

Request New Certificate, Open certificate and Copy Thumbprint

Go to Apps & Features, klik Windows Admin Center, Klik Modify, Klik Next

Klik Change, Paste Thumbprint, Klik Change, Klik Finish, Ready

Answers:

1. Obtain and install a new certificate
2. Copy the certificate thumbprint
3. Run Windows Admin Center Setup and select Change

upvoted 21 times

**lukiduc9625** Highly Voted 2 years, 3 months ago

In my opinion step 1 in suggested answer should be last one - when we start Windows Admin Center Setup and select Change we cannot continue until we have copied thumbprint of new certificate thus starting WAC Setup on the beginning isn't necessary

upvoted 20 times

**AnonChen** Most Recent 4 weeks, 1 day ago

ChatGPT:

To replace the certificate used by Windows Admin Center, you need to follow the correct sequence to obtain, identify, and assign the new certificate.

✓ Correct Sequence:

Obtain and install a new certificate.

You must have a valid certificate issued by a CA and install it on the server.

Copy the certificate thumbprint.

The thumbprint is used by Windows Admin Center Setup to identify the certificate.

Run Windows Admin Center Setup and select Change.

This allows you to specify the new certificate using the thumbprint.

upvoted 1 times

🗨️ 👤 **Joedn** 7 months ago

Valid 05/28/2024

upvoted 1 times

🗨️ 👤 **munti23** 7 months, 3 weeks ago

Obtain, Copy and Run WAC Setup and Select Change.

upvoted 2 times

🗨️ 👤 **boapaulo** 1 year ago

To replace the expired certificate in Windows Admin Center, you must follow these steps in sequence:

1 - Obtain and install a new certificate. You need to obtain a new certificate from a certificate authority (CA) and install it on the server.

2 - Copy the certificate thumbprint. After you install the new certificate, you must copy the thumbprint of the certificate.

3 - Run Windows Admin Center Setup and select Change. Run the Windows Admin Center installer and select the 'Change' option. During the process, you will need to provide the thumbprint of the new certificate

upvoted 3 times

🗨️ 👤 **Techbiz** 1 year, 5 months ago

The right answer is what Goofer presented. Do a little bit of research on that and you will see. The certificate needs to be installed on the server hosting the WAC and the certificate thumbprint gotten either via MMS snap-in or PowerShell, then you need to re-run the WAC setup and choose change to setup the new certificate. Then you're good to go.

upvoted 1 times

🗨️ 👤 **syu31svc** 1 year, 9 months ago

1) Obtain

2) Copy

3) Run change

This is the most logical flow to me

upvoted 7 times

🗨️ 👤 **MarkusSan** 2 years ago

obtain and install new cert

copy cert thumbprint

re-run the installer and choose change.

<http://coryretherford.com/Lists/Posts/Post.aspx?ID=418>

upvoted 3 times

🗨️ 👤 **joehoesofat** 2 years, 2 months ago

install cert, copy thumbprint, change install

upvoted 7 times

🗨️ 👤 **kijken** 2 years, 2 months ago

install cert, copy thumbprint, change install

upvoted 3 times

🗨️ 👤 **Bruk** 2 years, 2 months ago

I think its Install Cert , Copy Thumbprint en click Change in admin center <https://www.starwindsoftware.com/blog/change-the-windows-admin-center-certificate>

upvoted 3 times

🗨️ 👤 **ThomasMcThomasface** 2 years, 2 months ago

In the last exam I took (October 13th '22) it was change last

upvoted 2 times

🗨️ 👤 **rimvydukas** 2 years, 3 months ago

My order would be: install, copy, change

upvoted 4 times

## HOTSPOT -

You have an on-premises server named Server1 that runs Windows Server and has internet connectivity.

You have an Azure subscription.

You need to monitor Server1 by using Azure Monitor.

Which resources should you create in the subscription, and what should you install on Server1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

In the subscription, create:

- |   |
|---|
| <input type="checkbox"/>  |
| <input type="checkbox"/> An Azure Files storage account                           |
| <input type="checkbox"/> A Log Analytics workspace                                |
| <input type="checkbox"/> An Azure SQL database and a data collection rule         |
| <input type="checkbox"/> An Azure Blob Storage account and a data collection rule |

On Server1, install:

- |  |
|--|
| <input type="checkbox"/>   |
| <input type="checkbox"/> The Azure Monitor agent                   |
| <input type="checkbox"/> The Analytics gateway                     |
| <input type="checkbox"/> The Device Health Attestation server role |

Correct Answer:

**Answer Area**

In the subscription, create:


- |   |
|---|
| <input type="checkbox"/>  |
| <input type="checkbox"/> An Azure Files storage account                           |
| <input checked="" type="checkbox"/> A Log Analytics workspace                     |
| <input type="checkbox"/> An Azure SQL database and a data collection rule         |
| <input type="checkbox"/> An Azure Blob Storage account and a data collection rule |

On Server1, install:

- |  |
|--|
| <input type="checkbox"/>   |
| <input checked="" type="checkbox"/> The Azure Monitor agent        |
| <input type="checkbox"/> The Analytics gateway                     |
| <input type="checkbox"/> The Device Health Attestation server role |


Reference:

<https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-monitor>

 **examcrammer** Highly Voted 2 years, 2 months ago

If the server has internet connectivity, there is no need for a gateway. Gateways are for collecting and sending data to azure from non-internet-connected servers. Correct answers are A Log analytics workspace and The Azure monitor agent.

upvoted 36 times

 **odbjegli** Highly Voted 2 years, 1 month ago

Log analytics workspace & The Azure monitor agent.

<https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-monitor>

upvoted 19 times

🗲️ 👤 **Bolo92** Most Recent 7 months ago

valid 27.11.23

upvoted 2 times

🗲️ 👤 **syu31svc** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/media/azure-monitor-diagram.png>

Answer given is correct

upvoted 3 times

🗲️ 👤 **edykss** 1 year, 9 months ago

For 1st - Log Analytics workspace

For 2nd - Azure monitor Agent

upvoted 6 times

🗲️ 👤 **Contactfornitish** 1 year, 10 months ago

Still valid, in exam on 23rd Aug'22

upvoted 5 times

🗲️ 👤 **Contactfornitish** 1 year, 10 months ago

Analytics gateways are required only when you don't have internet connectivity. In those cases, those gateways collect data from other servers and then send to log analytics. If the server has direct connection, there is no point to bother with gateway

upvoted 2 times

🗲️ 👤 **ANDREVOX** 1 year, 11 months ago

<https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-monitor>

upvoted 1 times

🗲️ 👤 **AmineHZ** 2 years ago

the righth answer is Log analytics and Azure monitor Agent

upvoted 5 times

🗲️ 👤 **prepper666** 2 years, 1 month ago

Answer is Wrong. Correct answer li Log Analytics Workspace and Monitor Agent (MMA)

upvoted 5 times

🗲️ 👤 **TheUltimateHac** 2 years, 1 month ago

The Answer posted is correct.

\*Log Analytics Workspace

\*Analytics Gateway

upvoted 1 times

🗲️ 👤 **josepedroche** 1 year, 11 months ago

Why Analytics Gateway? : Connect computers without internet access by using the Log Analytics gateway in Azure Monitor

upvoted 2 times

🗲️ 👤 **AvoKikinha** 2 years, 1 month ago

Log Analytics workspace and install Azure Monitor agent

upvoted 8 times

🗲️ 👤 **orallony** 2 years, 1 month ago

Log anaylitics workspace for anylizing logs & Azure monitor agent to collect this logs.

upvoted 9 times

You have an on premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant. The domain contains two servers named Server1 and Server2.

A user named Admin1 is a member of the local Administrators group on Server1 and Server2.

You plan to manage Server1 and Server2 by using Azure Arc. Azure Arc objects will be added to a resource group named RG1.

You need to ensure that Admin1 can configure Server1 and Server2 to be managed by using Azure Arc.

What should you do first?

- A. From the Azure portal, generate a new onboarding script.
- B. Assign Admin1 the Azure Connected Machine Onboarding role for RG1.
- C. Hybrid Azure AD join Server1 and Server2.
- D. Create an Azure cloud-only account for Admin1.

**Correct Answer: B**

Community vote distribution



**MiMojo** Highly Voted 2 years, 2 months ago

**Selected Answer: A**

The Answer is "A". Hear me out. The question asks that "Admin1", a user account, has the appropriate permissions. The role of Azure Connected Machine Onboarding can only be assigned to a service principal, as confirmed by the link given to justify the wrong answer. Admin1 cannot be assigned this role, it's impossible, check it for yourself. Admin1, as a local server admin, has all the rights he/she needs. The correct answer is "A", generate a new onboarding script. One can onboard more than one server with the same script. Onboarding two certainly doesn't impose an administrative burden to use this method.

upvoted 21 times

**phi3nix** 2 years, 2 months ago

This is the correct answer. 1. I tested this in LAB. 2. Documentation: <https://learn.microsoft.com/en-us/azure/azure-arc/servers/onboard-portal>

---snap---

You can enable Azure Arc-enabled servers for one or a small number of Windows or Linux machines in your environment by performing a set of steps manually. Or you can use an automated method by running a template script that we provide. This script automates the download and installation of both agents.

This method requires that you have administrator permissions on the machine to install and configure the agent. On Linux, by using the root account, and on Windows, you are member of the Local Administrators group.

--snap--

upvoted 9 times

**phi3nix** 2 years, 2 months ago

A is the answer!

upvoted 2 times

**JP02021** 9 months, 1 week ago

OBS:

- "Admin1" is user in ADDS, and member of the local Administrators group on Server1 and Server2.

- ADDS is domain that syncs with an Azure Active Directory (Azure AD) tenant.

Answer is B "Assign Admin1 the Azure Connected Machine Onboarding role for RG1"

upvoted 1 times

**SantaClaws** 1 year, 6 months ago

It's not exclusive to service principals. But more importantly, OptionA simply doesn't satisfy the requirement of the question.

The question is not how to add resources to RG1. The question is explicitly about ensuring that Admin1 has the correct permissions. So option A can be completely disregarded as a possibility, because it's answering a completely different question.

upvoted 4 times

🗄️ 👤 **Bojana** Highly Voted 👍 3 years, 1 month ago

**Selected Answer: B**

correct

upvoted 13 times

🗄️ 👤 **RobBot** Most Recent 🕒 3 months, 3 weeks ago

**Selected Answer: D**

Although it does say the domain is sync'd the question doesn't mention whether Admin1 is a domain account. Best practice is for privileged users to have separate cloud only admin accounts, so D?

upvoted 1 times

🗄️ 👤 **Itkiller** 5 months ago

**Selected Answer: B**

Link from Phi3nix:

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/onboard-portal>

States its also best practice, that ends the discussion right there!

Follow best security practices and avoid using an Azure account with Owner access to onboard servers. Instead, use an account that only has the Azure Connected Machine onboarding or Azure Connected Machine resource administrator role assignment. See Azure Identity Management and access control security best practices for more information.

Role rights:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Search for: Azure Connected Machine Onboarding

upvoted 1 times

🗄️ 👤 **Ksk08** 8 months ago

Correct answer b

upvoted 1 times

🗄️ 👤 **JP02021** 9 months, 1 week ago

**Selected Answer: B**

-"Admin1" is user in ADDS, and member of the local Administrators group on Server1 and Server2.

-ADDS is domain that syncs with an Azure Active Directory (Azure AD) tenant.

Answer is B "Assign Admin1 the Azure Connected Machine Onboarding role for RG1"

upvoted 1 times

🗄️ 👤 **004b54b** 9 months, 2 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/onboard-portal#install-with-the-scripted-method>

Install with the scripted method

1. Log in to the server.

2. Open an elevated PowerShell command prompt. > local admin rights are required but sufficient

3. Change to the folder or share that you copied the script to, and execute it on the server by running the ./OnboardingScript.ps1 script.

upvoted 1 times

🗄️ 👤 **starseed** 9 months, 2 weeks ago

answer is B

upvoted 2 times

🗄️ 👤 **sardonique** 10 months, 3 weeks ago

Admin1 is an onpremises account, it does not exist in Azure AD therefore it cannot be assigned any role within the Azure Portal. Admin1 has enough power to configure Server1 and Server2 though. So A is the answer IMO

upvoted 1 times

🗄️ 👤 **JP02021** 9 months, 1 week ago

(AD DS) domain that "syncs" with an Azure Active Directory tenant....(Admin1 exist in Azure AD)

Answer is B

upvoted 1 times

🗄️ 👤 **Krayzr** 12 months ago

**Selected Answer: B**

B.

Reason: Azure Arc allows you to manage your servers as if they are running in Azure. To onboard a machine to Azure Arc, the user needs the Azure Connected Machine Onboarding role. This role gives the user the necessary permissions to register the machine with Azure Arc. In this case, Admin1 needs to be assigned this role for the resource group RG1, so they can configure Server1 and Server2 to be managed by Azure Arc. The other options do not directly address the requirement of enabling Admin1 to configure the servers with Azure Arc. Therefore, option B is the most appropriate first step.

upvoted 2 times

  **RemmyT** 1 year ago

**Selected Answer: B**

Tested in lab:

Admin1 without Azure Connected Machine onboarding role assigned on RG1 are unable to onboard any server to Azure.

Also are unable to see any machine in Azure Arc | Machines and as a result it cannot manage any server.

After assigning it the Azure Connected Machine onboarding role on RG1, Admin1 can see all the machines in Azure Arc, can manage the servers and can onboard the servers with the generated script.

Note:

Follow best security practices and avoid using an Azure account with Owner access to onboard servers. Instead, use an account that only has the Azure Connected Machine onboarding or Azure Connected Machine resource administrator role assignment. See Azure Identity Management and access control security best practices for more information.

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/onboard-portal>

upvoted 2 times

  **RemmyT** 1 year ago

You have an on premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant.

That means Admin1 is synced in Azure Entra ID and we can assign him the role Azure Connected Machine Onboarding on RG1 (where all Azure ARC servers will reside).

upvoted 1 times

  **nawtitoo** 1 year, 1 month ago

**Selected Answer: B**

with the appropriate role to Admin1 in the RG1 resource group, Admin1 will have the necessary permissions to configure Server1 and Server2 to be managed by Azure Arc.

upvoted 1 times

  **SIAMIANJI** 1 year, 1 month ago

**Selected Answer: B**

To ensure that Admin1 can configure Server1 and Server2 to be managed by using Azure Arc, the first step should be to assign Admin1 the appropriate role that grants the necessary permissions to onboard machines to Azure Arc. Specifically, Admin1 needs the Azure Connected Machine Onboarding role for the resource group RG1.

Here's the correct step to take:

B. Assign Admin1 the Azure Connected Machine Onboarding role for RG1.

This role grants the necessary permissions to onboard servers to Azure Arc, allowing Admin1 to generate the required onboarding script and complete the onboarding process.

upvoted 1 times

  **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: B**

To ensure that Admin1 can configure Server1 and Server2 to be managed by using Azure Arc, you should first assign Admin1 the necessary permissions in Azure, specifically the Azure Connected Machine Onboarding role for the resource group RG1.

Therefore, the correct answer is:

B. Assign Admin1 the Azure Connected Machine Onboarding role for RG1.



upvoted 1 times

🗨️ 👤 **RickySmith** 1 year, 6 months ago

**Selected Answer: B**

B

Assign Admin1 the Azure Connected Machine Onboarding role for RG1.

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/prerequisites#required-permissions>

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal> refer point 2

upvoted 2 times

🗨️ 👤 **boapaulo** 1 year, 6 months ago

Selected Answer:B

Generating a new integration script in the Azure portal is an important step in adding servers to Azure Arc, but it's not the first step when it comes to ensuring that a specific user, such as Admin1, has permission to configure the servers to be managed by Azure Arc.

The first step is to ensure that Admin1 has the necessary permissions within the Azure environment. This is done by assigning the correct role to the user. In the case of Admin1, assigning the Azure Connected Machine Integration role to resource group RG1 is essential for them to be able to perform the required actions in Azure Arc. Once Admin1 has the proper permissions, they can then proceed with generating and running the integration script to add Server1 and Server2 to Azure Arc.

upvoted 1 times

🗨️ 👤 **Payday123** 1 year, 7 months ago

Is Admin1 a local user or domain user added to local admins?

upvoted 1 times

## HOTSPOT -

Your network contains two Active Directory Domain Services (AD DS) forests named contoso.com and fabrikam.com. A two-way forest trust exists between the forests. Each forest contains a single domain.

The domains contain the servers shown in the following table.

Name	Domain	Description
Server1	contoso.com	Hosts a Windows Admin Center gateway
Server2	fabrikam.com	Hosts resources that will be managed remotely by using Windows Admin Center on Server1

You need to configure resource based constrained delegation so that the users in contoso.com can use Windows Admin Center on Server1 to connect to Server2.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Set-ADComputer -Identity

(Get-ADComputer server1.contoso.com )
(Get-ADComputer server2.fabrikam.com)
(Get-ADGroup 'Contoso\Domain Users')
(Get-ADGroup 'Fabrikam\Domain Users')

-PrincipalsAllowedToDelegateToAccount

(Get-ADComputer server1.contoso.com )
(Get-ADComputer server2.fabrikam.com )
(Get ADGroup 'Contoso\Domain Users')
(Get-ADGroup 'Fabrikam\Domain Users')

Correct Answer:

## Answer Area

Set-ADComputer -Identity

(Get-ADComputer server1.contoso.com )
(Get-ADComputer server2.fabrikam.com)
(Get-ADGroup 'Contoso\Domain Users')
(Get-ADGroup 'Fabrikam\Domain Users')


-PrincipalsAllowedToDelegateToAccount

(Get-ADComputer server1.contoso.com )
(Get-ADComputer server2.fabrikam.com )
(Get ADGroup 'Contoso\Domain Users')
(Get-ADGroup 'Fabrikam\Domain Users')

Reference:

<https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-constrained-delegation-overview>

<https://docs.microsoft.com/en-us/powershell/module/activedirectory/set-adcomputer?view=windowsserver2022-ps>

 **VinoTee** Highly Voted 3 years, 1 month ago


The answer should be:

Set-ADComputer -Identity (Get-ADComputer server2.fabrikam.com)

-PrincipalsAllowedToDelegateToAccount (Get-ADComputer server1.contoso.com)

Explanation: <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/user-access-control#:~:text=To%20configure%20Resource,Get%2DADComputer%20wac>

upvoted 37 times

 **Lu5ck** 2 years, 6 months ago


In general, what this command means is "server2.fabrikam.com" will accept any forwarded requests from "server1.contoso.com".

upvoted 8 times

 **sardonique** Most Recent 10 months, 3 weeks ago

looks correct to me

upvoted 2 times

 **phi3nix** 2 years, 2 months ago

The answer is correct. I did this in prod.

I usually do this way

\$MGMT = Get-ADComputer -Identity Server1

\$h4 = Get-ADComputer -Identity Server2

Set-ADComputer -Identity \$h4 -PrincipalsAllowedToDelegateToAccount \$MGMT

But you can write it:

Set-ADComputer -Identity (get-adcomputer server2.fabrika.com) -PrincipalsAllowedToDelegateToAccount (get-adcomputer server1/contoso.com)

upvoted 2 times

 **syu31svc** 2 years, 3 months ago

Get-ADGroup is completely wrong

"Server1 to connect to Server2"

Answer is correct

upvoted 2 times

🗨️ 👤 **Benjam** 2 years, 7 months ago

The correct answer is-

Set-ADComputer -Identity (Get-ADComputer server2.fabrikam.com)

PrincipalsAllowedToDelegateToAccount(Get-ADGroup'Fabrikam\Domain Users')

upvoted 4 times

🗨️ 👤 **Benjam** 2 years, 7 months ago

Sorry I made a mistake the Given answer is correct

Set-ADComputer -Identity \$Server2 -PrincipalsAllowedToDelegateToAccount \$Server1

upvoted 3 times

🗨️ 👤 **Verdural** 2 years, 10 months ago

Correct answer is:

Set-ADComputer -Identity (Get-ADComputer Server2.fabrikam.com) -PrincipalsAllowedToDelegateToAccount (Get-ADComputer Server1.contoso.com)

<https://purple.telstra.com.au/blog/kerberos-constrained-delegation>

upvoted 3 times

🗨️ 👤 **TheUltimateHac** 3 years, 1 month ago

Answer is wrong.

Should be

\*Server2.fabrikam

\*Contoso\Domain users

upvoted 3 times

🗨️ 👤 **AvoKikinha** 3 years, 1 month ago

Wrong !

From: <https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/ps-remoting-second-hop?view=powershell-7.2>

For ServerC to allow delegation from a PowerShell remoting session on ServerB, we must set the PrincipalsAllowedToDelegateToAccount parameter on ServerC to the computer object of ServerB:

PowerShell

Copy

# Grant resource-based Kerberos constrained delegation

Set-ADComputer -Identity \$ServerC -PrincipalsAllowedToDelegateToAccount \$ServerB

upvoted 4 times

🗨️ 👤 **AvoKikinha** 3 years, 1 month ago

Set-ADComputer -Identity server2..... -PrincipalsAllowedToDelegateToAccount server1.....

upvoted 10 times

## HOTSPOT -

You have a server named Server1 that runs Windows Server and has the Hyper-V server role installed.

You need to limit which Hyper-V module cmdlets helpdesk users can use when administering Server1 remotely.

You configure Just Enough Administration (JEA) and successfully build the role capabilities and session configuration files.

How should you complete the PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Enter-PSSession
New-PSSessionConfigurationFile
Register-PSSessionConfiguration

-Path .\HyperVJeaConfig

.ps1
.psm1
.psrc
.pssc

-Name 'HyperVJeaHelpDesk' -Force

Correct Answer:

### Answer Area

Enter-PSSession
New-PSSessionConfigurationFile
Register-PSSessionConfiguration


-Path .\HyperVJeaConfig

.ps1
.psm1
.psrc
.pssc

-Name 'HyperVJeaHelpDesk' -Force

Reference:

<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/register-jea?view=powershell-7.2>

 **examcrammer** Highly Voted 2 years, 8 months ago

the question clearly states the session configuration (.PSSC) file has been created. You must register the session. Answers are Register-PSSessionConfiguration and .pssc

upvoted 39 times

 **AnonymousJhb** 2 years, 5 months ago

Correct. New-PSSessionConfiguration has no -Force cmdlet

-Force only exists as part of Register-PSSessionConfigurationFile

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/register-pssessionconfiguration?view=powershell-7.2#examples>  
upvoted 7 times

🗒️ 👤 **dandirindan** Highly Voted 2 years, 7 months ago

<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/register-jea?view=powershell-7.2>  
upvoted 6 times

🗒️ 👤 **MichalGr** Most Recent 8 months, 3 weeks ago

might be wrong, but anyway "New-PSSessionConfigurationFile" is used to create a new session configuration file, but it does not automatically register it for use. Since we want to make the JEA session configuration available for use, we use "Register-PSSessionConfiguration" to accomplish this task

upvoted 1 times

🗒️ 👤 **Bolo92** 1 year, 1 month ago

valid 27.11.23

upvoted 2 times

🗒️ 👤 **mfmanue05** 1 year, 5 months ago

Answer is correct

upvoted 1 times

🗒️ 👤 **syu31svc** 1 year, 9 months ago

Answer is correct and link supports it

upvoted 2 times

🗒️ 👤 **edykss** 2 years, 3 months ago

Answer is Correct

upvoted 3 times

🗒️ 👤 **Contactfornitish** 2 years, 4 months ago

Still valid, in exam on 23rd Aug'22

upvoted 2 times

🗒️ 👤 **mazahaf** 2 years, 5 months ago

Answer: Register

upvoted 2 times

🗒️ 👤 **TheUltimateHac** 2 years, 7 months ago

Answer is Correct

upvoted 1 times

You have an Azure virtual machine named VM1 that runs Windows Server.  
 You have an Azure subscription that has Microsoft Defender for Cloud enabled.  
 You need to ensure that you can use the Azure Policy guest configuration feature to manage VM1.  
 What should you do?

- A. Add the PowerShell Desired State Configuration (DSC) extension to VM1.
- B. Configure VM1 to use a user-assigned managed identity.
- C. Configure VM1 to use a system-assigned managed identity.
- D. Add the Custom Script Extension to VM1.

**Correct Answer: C**


Community vote distribution

C (100%)

 **GoforIT21** Highly Voted 2 years, 12 months ago

**Selected Answer: C**

"For the machine to authenticate to the Guest Configuration service, the machine must have a System-Assigned Managed Identity." (see the given reference, <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/guest-configuration>)  
 upvoted 11 times

 **Contactfornitish** Highly Voted 2 years, 10 months ago

Still valid, in exam on 23rd Aug'22  
 upvoted 6 times

 **mhmyz** Most Recent 10 months ago

I tested Configuration Management for Azure VM, I could select system managed ID or User managed ID. So the answers are B and C.  
 upvoted 1 times

 **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: C**

To use the Azure Policy guest configuration feature to manage VM1, you need to ensure that VM1 is configured to use a system-assigned managed identity.

Therefore, the correct answer is:

C. Configure VM1 to use a system-assigned managed identity.  
 upvoted 2 times

 **afridi43** 1 year, 9 months ago

**Selected Answer: C**

Managed Identity: By configuring VM1 to use a system-assigned managed identity, you provide it with an identity within Azure Active Directory (Azure AD). This identity can be used for authentication when interacting with Azure services.  
 Azure Policy: Azure Policy can leverage managed identities to interact with VMs and enforce guest configurations. When a system-assigned managed identity is enabled on a VM, it simplifies the authentication process, and Azure Policy can use this identity to assess and enforce configurations on the VM.

So, by configuring VM1 to use a system-assigned managed identity, you enable Azure Policy Guest Configuration to manage and enforce policies on VM1 effectively.  
 upvoted 2 times

 **syu31svc** 2 years, 3 months ago

**Selected Answer: C**

C for correct and provided link supports it  
 upvoted 1 times

 **empee1977** 2 years, 4 months ago

Selected Answer: C

A system-assigned managed identity for an Azure virtual machine enables the virtual machine to use Azure services that support Azure AD authentication, without having to store the credentials in the application code. In order to use the Azure Policy guest configuration feature to manage VM1, you need to configure the virtual machine to use a system-assigned managed identity. Once the system-assigned managed identity is enabled, you can assign the necessary permissions to the managed identity and use Azure Policy guest configuration to manage the virtual machine's configuration.

upvoted 3 times

🗨️ 👤 **PEsty93** 2 years, 4 months ago

Microsoft are mean. They know we're learning about Desired State Configuration (DSC) as part of the objectives so they throw in it as an answer even though it is not at all relevant.

upvoted 4 times

🗨️ 👤 **King\_Laps** 2 years, 11 months ago

the correct answer is C

upvoted 5 times

🗨️ 👤 **prepper666** 3 years, 1 month ago

Answer is SYSTEM MANAGED IDENTITY

The identity is used to authenticate the machine as it reads and writes to the guest configuration service. The extension isn't required for Arc-enabled servers because it's included in the Arc Connected Machine agent.

upvoted 5 times



## HOTSPOT -

You have an Azure subscription named sub1 and 500 on-premises virtual machines that run Windows Server.

You plan to onboard the on-premises virtual machines to Azure Arc by running the Azure Arc deployment script.

You need to create an identity that will be used by the script to authenticate access to sub1. The solution must use the principle of least privilege.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

▼	-DisplayName 'Arc-for-servers' -Role	▼
New-AzADAppCredential		'Azure Connected Machine Onboarding'
New-AzADServicePrincipal		'Virtual Machine Contributor'
New-AzUserAssignedIdentity		'Virtual Machine User Login'

Correct Answer:

### Answer Area

▼	-DisplayName 'Arc-for-servers' -Role	▼
New-AzADAppCredential		'Azure Connected Machine Onboarding'
New-AzADServicePrincipal		'Virtual Machine Contributor'
New-AzUserAssignedIdentity		'Virtual Machine User Login'

Reference:

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal>

edykss Highly Voted 2 years, 3 months ago

Answer is Correct

upvoted 11 times

leegend Highly Voted 1 year, 7 months ago

Got this question 28-5-23

upvoted 5 times

boapaulo Most Recent 1 year ago

To create an identity that will be used by the script to authenticate access to the Azure subscription called sub1, following the principle of least privilege, you must use the New-AzADServicePrincipal command with the -Role parameter set to 'Azure Connected Machine Onboarding'

This command creates a new service principal in Azure Active Directory and assigns it the role that only allows machines to be onboarded to Azure Arc, with no additional permissions to reonboard or delete the resource from the machine.

The full command would be:

```
New-AzADServicePrincipal -DisplayName 'Arc-for-servers' -Role 'Azure Connected Machine Onboarding'
```

This command ensures that the identity created has only the permissions necessary to perform the task of onboarding the on-premises virtual machines to Azure Arc, without granting excessive privileges that could be improperly exploited.

upvoted 2 times

syu31svc 1 year, 9 months ago

Answer is correct and link given supports it

upvoted 4 times

You have an Azure virtual machine named VM1 that has a private IP address only.

You configure the Windows Admin Center extension on VM1.

You have an on-premises computer that runs Windows 11. You use the computer for server management.

You need to ensure that you can use Windows Admin Center from the Azure portal to manage VM1.

What should you configure?

- A. an Azure Bastion host on the virtual network that contains VM1.
- B. a VPN connection to the virtual network that contains VM1.
- C. a private endpoint on the virtual network that contains VM1.
- D. a network security group (NSG) rule that allows inbound traffic on port 443.

**Correct Answer:** D

Community vote distribution



**hchafloque** Highly Voted 2 years, 6 months ago

"You need to ensure that you can use Windows Admin Center from the Azure portal" - The portal use 443 port. No VPN required, the use is through Portal, not RDP access. Answer, D.

upvoted 12 times

**edykss** Highly Voted 2 years, 9 months ago

Answer is Correct

upvoted 9 times

**e489b39** Most Recent 3 weeks, 5 days ago

Selected Answer: A

use Windows Admin Center from the Azure portal to manage VM1 why should we have to setup VPN ? we are not going to access from on-premises

upvoted 1 times

**Tayhull2023** 2 months, 2 weeks ago

Selected Answer: A

I might be missing something here. I don't see anything about managing this VM1 and the Admin Center FROM the Windows 11 PC, we are just assuming that. With the Admin Center extension installed on VM1 in Azure, we could just use Bastion to connect to the VM, and run it on the Azure VM1 server without ever hitting a public IP. Answer to me is A, but seems like a really badly written question.

upvoted 2 times

**Opoveda** 3 months, 2 weeks ago

Selected Answer: A

Azure Bastion provides secure and seamless RDP and SSH connectivity to Azure VMs directly in the Azure portal, without requiring a public IP address on the VM. It allows you to manage VMs securely without exposing them to potential internet-based threats. This aligns with the scenario described in the question.

upvoted 2 times

**Opoveda** 3 months, 1 week ago

No... i think is B, azure bastion is ssh & rdp, but this question is about windows admin center

upvoted 1 times

**Itkiller** 4 months, 3 weeks ago

Selected Answer: B

VPN Connection: Setting up a Virtual Private Network (VPN) between your on-premises network and the Azure virtual network allows your on-premises computer to securely access resources within the Azure virtual network, including VM1. This is essential because VM1 has only a private IP address and is not directly accessible from the public internet.

<https://www.youtube.com/watch?v=GH-i6sOtyAo>

upvoted 1 times

**NoMedi** 5 months ago

Selected Answer: B



B:

To use Windows Admin Center from the Azure portal to manage VM1, which has only a private IP address, you should configure a VPN connection to the virtual network that contains VM1. This option allows secure access to the private network where VM1 is located, enabling you to manage the VM using Windows Admin Center through the Azure portal.

The other options are less suitable for this scenario:

- Azure Bastion is primarily used for RDP and SSH connections, not specifically for Windows Admin Center.
- A private endpoint is typically used for connecting to Azure PaaS services, not for managing VM.
- An NSG rule allowing inbound traffic on port 443 alone would not provide the necessary connectivity from your on-premises network to the Azure virtual network.

upvoted 1 times

  **wazza47** 6 months, 2 weeks ago

Selected Answer: A

manage VM1 from the Azure portal using the Windows Admin Center, you need to ensure secure and accessible connectivity to the VM that has a private IP address.

Among the provided options, the most suitable configuration is:

A. an Azure Bastion host on the virtual network that contains VM1.

Azure Bastion provides secure RDP and SSH connectivity to your virtual machines directly through the Azure portal. This eliminates the need for a public IP address, thereby ensuring security while allowing you to manage VM1 through the Windows Admin Center.

Setting up an Azure Bastion host will enable you to access VM1 securely from the Azure portal, maintaining the principles of least privilege and secure management practices

upvoted 1 times

  **Ksk08** 7 months, 2 weeks ago

B. a VPN connection to the virtual network that contains VM1.

upvoted 1 times

  **Ksk08** 8 months, 1 week ago

Answer is A

upvoted 1 times

  **NicolaF** 9 months, 2 weeks ago

no public ip so B is the correct answer. Private Endpoints allows you to access resources from Azure

upvoted 1 times

  **Mladen\_66** 1 year ago

Selected Answer: B

If your target Azure VMs don't have public IPs, and you want to manage these VMs from a Windows Admin Center gateway deployed in your on-premises network, you need to configure your on-premises network to have connectivity to the VNet on which the target VMs are connected. There are 3 ways you can do this: ExpressRoute, Site-to-Site VPN, or Point-to-Site VPN.

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/manage-azure-vms#connecting-to-vms-without-a-public-ip>

upvoted 4 times

  **[Removed]** 1 year ago

Answer is C.

The key word here is private IP address.

C. Private endpoints allow you to access Azure services (such as VM1) over a private IP address within the virtual network. By configuring a private endpoint for VM1, you can securely manage it using Windows Admin Center from the Azure portal.

upvoted 1 times

  **Kuikz** 1 year, 3 months ago

Selected Answer: B

I agree with B.

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/manage-vm>

upvoted 2 times

  **boapaulo** 1 year, 6 months ago



Better, scenario is the Bastion in security, however if we look at cost, without a doubt the NSG releasing port 443.

upvoted 2 times

  **dolphan904** 1 year, 6 months ago

The ON-PREM Windows 11 client is connecting to the Azure Portal which in turn then allows the admin to manage the Azure VM (VM1) via its extension. That connection happens inbound to the VM via PORT 443, therefore, you must allow inbound traffic for PORT 443 on the NSG attached to the VM or the subnet that is hosting it. The others make no sense here. You DO NOT need a VPN connection to manage an Azure resource via the Azure Portal. Nor should need to go to the trouble of putting one together to manage an Azure VM via the WAC tool. Its an HTTP tool. That is the whole point of using WAC.

upvoted 2 times

  **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 3 times

Your company has a main office and a branch office. The two offices are connected by using a WAN link. Each office contains a firewall that filters WAN traffic.

The network in the branch office contains 10 servers that run Windows Server. All servers are administered from the main office only.

You plan to manage the servers in the branch office by using a Windows Admin Center gateway.

On a server in the branch office, you install the Windows Admin Center gateway by using the defaults settings.

You need to configure the firewall in the branch office to allow the required inbound connection to the Windows Admin Center gateway.

Which inbound TCP port should you allow?

- A. 443
- B. 3389
- C. 5985
- D. 6516

**Correct Answer: A**

Community vote distribution

A (88%)

12%

 **DesolateMarauder** Highly Voted 2 years ago

A: Inbound 443 for HTTPS

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/deploy-wac-in-azure>

upvoted 5 times

 **nawtitoo** Most Recent 7 months ago

**Selected Answer: A**

Allowing inbound TCP traffic on port 443 will enable secure communication between the Windows Admin Center client (typically a web browser) in the main office and the Windows Admin Center gateway installed on the server in the branch office, facilitating remote management of the servers in the branch office.

upvoted 2 times

 **SIAMIANJI** 8 months ago


**Selected Answer: A**

To allow inbound connections to the Windows Admin Center gateway installed on a server in the branch office, you should configure the firewall to allow traffic on TCP port 443.

Therefore, the correct answer is:

A. 443

upvoted 2 times

 **Kuikz** 9 months ago

**Selected Answer: A**

correct

upvoted 1 times

 **rknichols01** 12 months ago

to access Windows Admin Center gateway it uses port TCP 443. from the gateway to the individual servers uses port 6516.

upvoted 1 times

 **RickySmith** 1 year, 3 months ago

**Selected Answer: D**

D

On a server in the branch office, you install the Windows Admin Center gateway by using the defaults settings.

Acc to <https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/manage-vm#creating-an-inbound-port-rule-for-connecting-from-specific-public-ip-addresses>, The default is 6516

upvoted 2 times

🗳️ 👤 **RickySmith** 1 year, 3 months ago

Please delete.

upvoted 1 times

🗳️ 👤 **afridi43** 1 year, 3 months ago

**Selected Answer: A**

To configure the firewall in the branch office to allow the required inbound connection to the Windows Admin Center gateway, you should allow inbound traffic on port 443 (option A).

Port 443 is the default port used for HTTPS traffic, and Windows Admin Center typically uses HTTPS for secure communication.

So, the correct answer is:

A. 443

upvoted 3 times

🗳️ 👤 **Returnerwesley** 1 year, 6 months ago

PORT FOR TCP IS 443

upvoted 1 times

🗳️ 👤 **syu31svc** 1 year, 9 months ago

**Selected Answer: A**

3389 is for RDP so B is wrong

5985 is for WinRM HTTPS so C is wrong

6516 is for Windows 10 so D is wrong

A is the answer

upvoted 4 times

🗳️ 👤 **BryRob** 1 year, 11 months ago

**Selected Answer: A**

Given answer is correct

upvoted 2 times

🗳️ 👤 **empee1977** 1 year, 11 months ago

**Selected Answer: A**

A:

Windows Admin Center Gateway listens on both ports 443 and 6516 by default. Port 443 is used for HTTPS connections, which encrypts the communication between the client and the gateway. Port 6516 is used for the Windows Remote Management (WinRM) protocol, which is a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows you to remotely manage Windows-based servers and clients.

upvoted 3 times

🗳️ 👤 **cifofs** 2 years ago

Answer is A

upvoted 3 times

🗳️ 👤 **Benjam** 2 years, 1 month ago

**Selected Answer: A**

Answer is A Port 443

upvoted 2 times

🗳️ 👤 **JohnO1971** 2 years, 2 months ago

**Selected Answer: A**

A is the answer based on

The default port for the Windows Admin Center Gateway Installation is Port 443 – it is recommended to use this default port.

<https://www.manfredhelber.de/installing-and-configuring-windows-admin-center-for-windows-server-2022-management/>

upvoted 4 times

🗳️ 👤 **Jawad1462** 2 years, 2 months ago

**Selected Answer: D**

Port 6516 used to open port in win admin center

upvoted 3 times

🗳️ 👤 **rimvydukas** 2 years, 2 months ago

You are wrong. 6516 port is used only when WAC installed on Windows 10. When WAC is installed in gateway mode on windows server - 443 port is used.

upvoted 3 times

  **kordisma123** 2 years, 2 months ago

Labas, have you passed the exam? Are most of the questions here in this website?

upvoted 1 times

You have an Azure subscription that contains the following resources.

- ⇒ An Azure Log Analytics workspace
- ⇒ An Azure Automation account
- ⇒ Azure Arc

You have an on-premises server named Server1 that is onboarded to Azure Arc.

You need to manage Microsoft updates on Server1 by using Azure Arc.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the Automation account, enable Update Management for Server1.
- B. From the Virtual machines data source of the Log Analytics workspace, connect Server1.
- C. On Server1, install the Azure Monitor agent
- D. Add Microsoft Sentinel to the Log Analytics workspace

**Correct Answer: AC**

Community vote distribution

AC (100%)

🗳️ **pewpewvx** Highly Voted 1 year, 2 months ago

**Selected Answer: AC**

Only A and C make sense.

Automation is needed for the Update Management, and for Arc to work you need the AMA Agent.

upvoted 8 times

🗳️ **empee1977** Highly Voted 1 year, 5 months ago

**Selected Answer: AC**

A: To manage Microsoft updates on Server1 by using Azure Arc, you need to enable Update Management for the server from the Automation account. Azure Arc Update Management enables you to manage updates for your Azure Arc-enabled servers from the Azure portal, using the same update management solution that you use for Azure VMs.

C: To enable Update Management for Server1, you also need to install the Azure Monitor agent on the server. The Azure Monitor agent is a lightweight process that runs on your servers and collects performance, event, and diagnostic data, and forwards it to Azure Monitor for analysis. This data is used to monitor the performance and health of your servers and to detect and diagnose issues.

upvoted 5 times

🗳️ **e489b39** Most Recent 3 weeks, 5 days ago

**Selected Answer: AC**

Correct

upvoted 1 times

🗳️ **mfmanue05** 11 months, 2 weeks ago

resposta correta.

upvoted 1 times

🗳️ **syu31svc** 1 year, 3 months ago

**Selected Answer: AC**

"manage Microsoft updates" so A is one of the answers

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent>

Use Azure Automation Update Management, Azure Automation State Configuration, or Azure Automation Change Tracking and Inventory to deliver comprehensive management of your Azure and non-Azure machines.

Important



The Log Analytics agent is on a deprecation path and won't be supported after August 31, 2024. If you use the Log Analytics agent to ingest data to Azure Monitor, migrate to the new Azure Monitor agent prior to that date.

C is the other answer



upvoted 2 times

  **Jawad1462** 1 year, 8 months ago

**Selected Answer: AC**

Correct answers

upvoted 4 times

  **edykss** 1 year, 9 months ago

Answer is Correct A,C

upvoted 5 times

## HOTSPOT -

You have an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant.

You have an on-premises web app named WebApp1 that only supports Kerberos authentication.

You need to ensure that users can access WebApp1 by using their Azure AD account. The solution must minimize administrative effort.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

In Azure AD: 

	▼
The Azure AD Application Proxy connector	
The Azure AD Application Proxy service	
Web Application Proxy	

On-premises: 

	▼
The Azure AD Application Proxy connector	
The Azure AD Application Proxy service	
Web Application Proxy	

## Answer Area

Correct Answer:

In Azure AD: 

	▼
The Azure AD Application Proxy connector	
The Azure AD Application Proxy service	
Web Application Proxy	

On-premises: 

	▼
The Azure AD Application Proxy connector	
The Azure AD Application Proxy service	
Web Application Proxy	

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

 **Leocan** Highly Voted 1 year, 1 month ago

To use Application Proxy, you need a Windows server running Windows Server 2012 R2 or later. You'll install the Application Proxy connector on the server.

upvoted 11 times

 **leegend** Most Recent 7 months ago

Got this question 28-5-23

upvoted 4 times

 **syu31svc** 9 months, 1 week ago

Answer is right

And Leocan has stated the key segment

upvoted 4 times

## SIMULATION

-

You need to collect errors from the System event log of SRV1 to a Log Analytics workspace.

The required source files are located in a folder named \\dc1.contoso.com\\install.

To complete this task, sign in the required computer or computers.

**Correct Answer:****Configure Windows event logs**

Configure Windows event logs from the Agents configuration menu for the Log Analytics workspace.

**Step 1:** Go to the Log Analytics workspaces menu in the Azure portal.

**Configure data sources**

To configure data sources for Log Analytics agents, go to the Log Analytics workspaces menu in the Azure portal and select a workspace.

**Step 2:** Select Agents configuration.

**Step 3:** Select the tab for the data source you want to configure.

In this case the Windows event log of SRV1.

**Step 4:** Select only Error option in the System Log row.

Azure Monitor only collects events from Windows event logs that are specified in the settings.

The screenshot shows the 'Agents configuration' page in the Azure portal for a workspace named 'my-workspace'. The 'Windows event logs' tab is active. Below the tab, there is a table with columns for 'Log name', 'Error', 'Warning', and 'Information'. The 'System' log is selected, and the 'Error' checkbox is checked and highlighted with a red box.

Log name	Error	Warning	Information
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Reference:** <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events>

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agent-data-sources#configure-data-sources>

**smorar** 7 months, 1 week ago

Could you tell me how to answer this question? In the exam, do we have to connect to another PC to run the exercise like a laboratory?

Thanks.

upvoted 3 times

**Abx\_01** 1 year ago



Correct one is by selecting the Legacy agents management under the select workspace

upvoted 4 times

**STFN2019** 1 year, 11 months ago

Correct: <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events>

upvoted 2 times

  **Krayzr** 6 months, 1 week ago

Yes, the interface has changed , a LOT  
upvoted 1 times

HOTSPOT

-

Your on-premises network contains an Active Directory domain named contoso.com and 500 servers that run Windows Server. All the servers are Azure Arc-enabled and joined to contoso.com.

You need to implement PowerShell Desired State Configuration (DSC) on all the servers. The solution must minimize administrative effort.

Where should you store the DSC scripts, and what should you use to apply DSC to the servers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Store in:	<div><div></div><div>An Azure App Configuration store</div><div>An Azure Automation account</div><div>An Azure Policy definition</div></div>
Use:	<div><div></div><div>A Group Policy Object (GPO) in Active Directory Domain Services (AD DS)</div><div>Azure virtual machines extensions</div><div>Guest configuration in Azure Policy</div></div>

Correct Answer:

**Answer Area**

Store in:

An Azure App Configuration store

An Azure Automation account

An Azure Policy definition

Use:

A Group Policy Object (GPO) in Active Directory Domain Services (AD DS)

Azure virtual machines extensions

Guest configuration in Azure Policy

**ala76nl** 2 years, 1 month ago

Correct answer in second part is use virtual machine extensions

Here's an overview of the process:

You store and compile your DSC scripts in your Azure Automation account. When the scripts are compiled, they become Node Configurations. To apply the DSC configurations to your VMs, you "Onboard" the VMs to Azure Automation DSC. This process involves installing the PowerShell DSC VM extension on the VMs (if it's not already installed), and registering the VMs with the Azure Automation DSC service.

As part of the onboarding process, you assign a Node Configuration to each VM. The PowerShell DSC VM extension on each VM then periodically checks with the Azure Automation DSC service, pulls the assigned Node Configuration, and ensures that the VM is configured according to that Node Configuration.

The compliance status of each VM (whether it's correctly configured according to its assigned Node Configuration) is then reported back to Azure Automation DSC, and you can view this status in the Azure portal.

upvoted 14 times

**Krayzr** 11 months, 4 weeks ago

Seems like correct

Store in:

An Azure Automation account: Azure Automation allows you to automate the creation, deployment, monitoring, and maintenance of resources in your Azure environment using a highly scalable and reliable workflow execution engine. It would be the best place to store the DSC scripts as it provides a way to manage configurations at scale using PowerShell DSC.

Use:

Azure virtual machines extensions: Azure VM extensions are small applications that provide post-deployment configuration and automation tasks on Azure virtual machines. In this case, the DSC extension for Windows will be used to apply the DSC configuration to the servers. This extension is directly integrated with Azure and provides a seamless experience for applying configuration.

upvoted 2 times

  **MR\_Eliot**  1 year, 9 months ago

Box1: 3

Box2: 3

<https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview?source=recommendations>

Before you enable Automation State Configuration, we would like you to know that a newer version of DSC is now generally available, managed by a feature of Azure Policy named guest configuration. The guest configuration service combines features of DSC Extension, Azure Automation State Configuration, and the most commonly requested features from customer feedback. Guest configuration also includes hybrid machine support through Arc-enabled servers.

upvoted 6 times

  **Anonymouse1312** 1 year, 3 months ago

you are CORRECT:

<https://blog.matrixpost.net/infrastructure-as-code-iac-part-5-azure-automanage-machine-configuration-formerly-called-azure-policy-guest-configuration/>

<https://blog.matrixpost.net/infrastructure-as-code-iac-part-4-azure-automation-state/>

In a nutshell, there are/ were two ways:

Azure Automation State Configuration

- DSC scripts are stored in an Automation Account under "State Configuration (DSC)"
- Seems to be deprecated as of October 2023
- Deployment happens after compiling the DSC config file, after which it is ready to be pulled by the server

Azure Automanage Machine Configuration

- The DSC config file is compiled into a MOF file, packaged, and used by machine configuration to create the Azure Policy definitions
- In order for VMs to be automanaged, they must have assigned a system assigned managed identity

So, boxes 3/3 are correct because Azure VM extension are not used to APPLY the DSC. They are a prerequisite for it to work

upvoted 3 times

  **Ksk08**  8 months, 2 weeks ago

Answer is correct

upvoted 1 times



  **lucacose** 1 year, 6 months ago

Azure Automation Account

Guest Configuration in Azure policy

<https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview?source=recommendations>

upvoted 2 times

  **Mtijnz0r** 1 year, 12 months ago

<https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview>

Before you enable Automation State Configuration, we would like you to know that a newer version of DSC is now generally available, managed by a feature of Azure Policy named guest configuration. The guest configuration service combines features of DSC Extension, Azure Automation State

Configuration, and the most commonly requested features from customer feedback. Guest configuration also includes hybrid machine support through Arc-enabled servers.

upvoted 1 times

🗨️ 👤 **Maup33** 1 year, 11 months ago

<https://learn.microsoft.com/en-us/azure/automation/automation-dsc-onboarding>

upvoted 1 times

🗨️ 👤 **Maup33** 1 year, 11 months ago

Azure Policy's guest configuration feature is in public preview for applying configurations to Azure virtual machines and Arc-enabled machines. Guest configuration is integrated with Azure Security Center, Azure Automanage and will continue to expand.

We have listened to your feedback, that it should be easy to configure the state of virtual machines in Azure and machines that are hybrid connected by Azure Arc. Top priorities include regulatory, security and operational compliance.

Using guest configuration, you can apply configurations provided by Microsoft, or create your own configuration packages using PowerShell DSC version 3.

upvoted 1 times

🗨️ 👤 **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 3 times

🗨️ 👤 **ala76nl** 2 years, 1 month ago

Wrong. You either go for the Azure automation method or by the Azure policy method. So you create a gues configuration package and reference this in a azure policy definition.

upvoted 2 times

🗨️ 👤 **syu31svc** 2 years, 3 months ago

<https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/overview>

<https://learn.microsoft.com/en-us/azure/governance/machine-configuration/overview>

Answer is correct

upvoted 4 times

🗨️ 👤 **STFN2019** 2 years, 4 months ago

Correct, ref: <https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

upvoted 3 times



## Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

## To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

## Overview -

## Company Information -

ADatum Corporation is a manufacturing company that has a main office in Seattle and two branch offices in Los Angeles and Montreal.

## Fabrikam Partnership -

ADatum recently partnered with 2 company named Fabrikam, Inc.

Fabrikam is a manufacturing company that has a main office in Boston and a branch office in Orlando.

Both companies intend to collaborate on several joint projects.

## Existing Environment -

## ADatum AD DS Environment -

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

The forest contains two domains named adatum.com and east.adatum.com and the domain controllers shown in the following table.

Name	Domain	Operations master roles
DC1	adatum.com	Schema master
DC2	adatum.com	None
DC3	east.adatum.com	PDC emulator, RID master

## Fabrikam AD DS Environment -

The on-premises network of Fabrikam contains an AD DS forest named fabrikam.com.

The forest contains two domains named fabrikam.com and south.fabrikam.com.

The fabrikam.com domain contains an organizational unit (OU) named Marketing.

#### Server Infrastructure -

The adatum.com domain contains the servers shown in the following table.

Name	Role
HyperV1	Hyper-V
SSPace1	File and Storage Services

HyperV1 contains the virtual machines shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2022 Datacenter	Joined to the adatum.com domain Contains a file share named Data1 and a local user named User1
VM2	Red Hat Enterprise Linux (RHEL)	Contains a local user named User2
VM3	Windows Server 2022 Standard	Joined to the adatum.com domain Has the File and Storage Services role installed

All the virtual machines on HyperV1 have only the default management tools installed.

SSPace1 contains the Storage Spaces virtual disks shown in the following table.

Name	Number of physical disks	Redundancy
Disk1	8	Three-way mirror
Disk2	12	Parity

#### Azure Resources -

ADatum has an Azure subscription that contains an Azure AD tenant. Azure AD Connect is configured to sync the adatum.com forest with Azure AD.

The subscription contains the virtual networks shown in the following table.

Name	Location	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	West US	SubnetA, SubnetB

The subscription contains the Azure Private DNS zones shown in the following table.

Name	Virtual network link
Zone1.com	VNet1
Zone2.com	VNet2
Zone3.com	None

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Security type
Server1	Windows Server 2022 Datacenter: Azure Edition	Trusted launch
Server2	Windows Server 2022 Datacenter: Azure Edition	Standard
Server3	Windows Server 2022 Datacenter	Standard
Server4	Windows Server 2019 Datacenter	Trusted launch

All the servers are in a workgroup.

The subscription contains a storage account named storage1 that has a file share named share1.

Requirements -

Planned Changes -

ADatum plans to implement the following changes:

- Sync Data1 to share1.
- Configure an Azure runbook named Task1.
- Enable Azure AD users to sign in to Server1.
- Create an Azure DNS Private Resolver that has the following configurations:
  - Name: Private1
  - Region: West US
  - Virtual network: VNet1
  - Inbound endpoint: SubnetB
- Enable users in the adatum.com domain to access the resources in the south.fabrikam.com domain.

Technical Requirements -

ADatum identifies the following technical requirements:

- The data on SSPE1 must be available always.
- DC2 must become the schema master if DC1 fails.
- VM3 must be configured to enable per-folder quotas.
- Trusts must allow access to only the required resources.
- The users in the Marketing OU must have access to storage1.
- Azure Automanager must be used on all supported Azure virtual machines.
- A direct SSH session must be used to manage all the supported virtual machines on HyperV1.

You need to implement the planned changes for Azure AD users to sign in to Server1.

Which PowerShell cmdlet should you run?

- A. New-ADComputer
- B. Set-AzVM
- C. Set-AzVMExtension
- D. Add-ADComputerServiceAccount

**Correct Answer: C**

Community vote distribution

C (100%)

 **Payday123** Highly Voted 1 year, 8 months ago

**Selected Answer: C**

To enable Azure AD users to sign in to Server1 (which is in a workgroup) you need to install AADLoginForWindows extension (full name: Azure AD based Windows Login, recently renamed to: Microsoft Entra login VM)

upvoted 6 times

  **sardonique** Most Recent 10 months, 3 weeks ago

As always the question is badly formulated. you need both B and C commands. you would need to enable System-Assigned Managed Identity anyways, which is done using the Set-AzVM cmdlet. and you need to configure the extension as well. The People behind these question are not up to the task.

upvoted 4 times

  **NazerRazer** 1 year, 8 months ago

To implement the planned change for Azure AD users to sign in to Server1, you should run the Set-AzVMExtension PowerShell cmdlet. This cmdlet is used to configure extensions on an Azure Virtual Machine (VM).

The specific extension you would configure in this case is likely the "Custom Script Extension" or similar, which would allow you to run scripts or commands on the VM to enable Azure AD users to sign in.

So, the correct answer is:

C. Set-AzVMExtension

upvoted 4 times

## Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

## To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

## Overview -

## Company Information -

ADatum Corporation is a manufacturing company that has a main office in Seattle and two branch offices in Los Angeles and Montreal.

## Fabrikam Partnership -

ADatum recently partnered with 2 company named Fabrikam, Inc.

Fabrikam is a manufacturing company that has a main office in Boston and a branch office in Orlando.

Both companies intend to collaborate on several joint projects.

## Existing Environment -

## ADatum AD DS Environment -

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

The forest contains two domains named adatum.com and east.adatum.com and the domain controllers shown in the following table.

Name	Domain	Operations master roles
DC1	adatum.com	Schema master
DC2	adatum.com	None
DC3	east.adatum.com	PDC emulator, RID master

## Fabrikam AD DS Environment -

The on-premises network of Fabrikam contains an AD DS forest named fabrikam.com.

The forest contains two domains named fabrikam.com and south.fabrikam.com.

The fabrikam.com domain contains an organizational unit (OU) named Marketing.

#### Server Infrastructure -

The adatum.com domain contains the servers shown in the following table.

Name	Role
HyperV1	Hyper-V
SSPace1	File and Storage Services

HyperV1 contains the virtual machines shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2022 Datacenter	Joined to the adatum.com domain Contains a file share named Data1 and a local user named User1
VM2	Red Hat Enterprise Linux (RHEL)	Contains a local user named User2
VM3	Windows Server 2022 Standard	Joined to the adatum.com domain Has the File and Storage Services role installed

All the virtual machines on HyperV1 have only the default management tools installed.

SSPace1 contains the Storage Spaces virtual disks shown in the following table.

Name	Number of physical disks	Redundancy
Disk1	8	Three-way mirror
Disk2	12	Parity

#### Azure Resources -

ADatum has an Azure subscription that contains an Azure AD tenant. Azure AD Connect is configured to sync the adatum.com forest with Azure AD.

The subscription contains the virtual networks shown in the following table.

Name	Location	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	West US	SubnetA, SubnetB

The subscription contains the Azure Private DNS zones shown in the following table.

Name	Virtual network link
Zone1.com	VNet1
Zone2.com	VNet2
Zone3.com	None

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Security type
Server1	Windows Server 2022 Datacenter: Azure Edition	Trusted launch
Server2	Windows Server 2022 Datacenter: Azure Edition	Standard
Server3	Windows Server 2022 Datacenter	Standard
Server4	Windows Server 2019 Datacenter	Trusted launch

All the servers are in a workgroup.

The subscription contains a storage account named storage1 that has a file share named share1.

Requirements -

Planned Changes -

ADatum plans to implement the following changes:

- Sync Data1 to share1.
- Configure an Azure runbook named Task1.
- Enable Azure AD users to sign in to Server1.
- Create an Azure DNS Private Resolver that has the following configurations:
  - Name: Private1
  - Region: West US
  - Virtual network: VNet1
  - Inbound endpoint: SubnetB
- Enable users in the adatum.com domain to access the resources in the south.fabrikam.com domain.

Technical Requirements -

ADatum identifies the following technical requirements:

- The data on SSPage1 must be available always.
- DC2 must become the schema master if DC1 fails.
- VM3 must be configured to enable per-folder quotas.
- Trusts must allow access to only the required resources.
- The users in the Marketing OU must have access to storage1.
- Azure Automanager must be used on all supported Azure virtual machines.
- A direct SSH session must be used to manage all the supported virtual machines on HyperV1.

Which two languages can you use for Task1? Each correct answer presents a complete solution.

- A. Bicep
- B. Python
- C. Java
- D. PowerShell
- E. JavaScript

**Correct Answer:** BD

*Community vote distribution*

BD (100%)

🗨️ 👤 SIAMIANJI 7 months, 3 weeks ago

**Selected Answer:** BD

For configuring an Azure runbook in Azure Automation, you can use two primary scripting languages:

**PowerShell:** PowerShell is the most commonly used language for creating Azure Automation runbooks. It provides a robust scripting environment with rich capabilities for automating tasks in Azure and other Microsoft environments. PowerShell scripts can interact with Azure resources using

Azure cmdlets and APIs.

Python: Azure Automation also supports Python as a scripting language for creating runbooks. Python is a popular and versatile language known for its simplicity and readability. With Python scripts, you can automate various tasks in Azure, just like you would with PowerShell.

upvoted 3 times

  **windowsmodulesinstallerworker** 1 year, 3 months ago

**Selected Answer: BD**

<https://learn.microsoft.com/en-us/azure/automation/automation-runbook-types>

upvoted 4 times



## Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

## To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

## Overview -

## Company Information -

ADatum Corporation is a manufacturing company that has a main office in Seattle and two branch offices in Los Angeles and Montreal.

## Fabrikam Partnership -

ADatum recently partnered with 2 company named Fabrikam, Inc.

Fabrikam is a manufacturing company that has a main office in Boston and a branch office in Orlando.

Both companies intend to collaborate on several joint projects.

## Existing Environment -

## ADatum AD DS Environment -

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

The forest contains two domains named adatum.com and east.adatum.com and the domain controllers shown in the following table.

Name	Domain	Operations master roles
DC1	adatum.com	Schema master
DC2	adatum.com	None
DC3	east.adatum.com	PDC emulator, RID master

## Fabrikam AD DS Environment -

The on-premises network of Fabrikam contains an AD DS forest named fabrikam.com.

The forest contains two domains named fabrikam.com and south.fabrikam.com.

The fabrikam.com domain contains an organizational unit (OU) named Marketing.

#### Server Infrastructure -

The adatum.com domain contains the servers shown in the following table.

Name	Role
HyperV1	Hyper-V
SSPace1	File and Storage Services

HyperV1 contains the virtual machines shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2022 Datacenter	Joined to the adatum.com domain Contains a file share named Data1 and a local user named User1
VM2	Red Hat Enterprise Linux (RHEL)	Contains a local user named User2
VM3	Windows Server 2022 Standard	Joined to the adatum.com domain Has the File and Storage Services role installed

All the virtual machines on HyperV1 have only the default management tools installed.

SSPace1 contains the Storage Spaces virtual disks shown in the following table.

Name	Number of physical disks	Redundancy
Disk1	8	Three-way mirror
Disk2	12	Parity

#### Azure Resources -

ADatum has an Azure subscription that contains an Azure AD tenant. Azure AD Connect is configured to sync the adatum.com forest with Azure AD.

The subscription contains the virtual networks shown in the following table.

Name	Location	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	West US	SubnetA, SubnetB

The subscription contains the Azure Private DNS zones shown in the following table.

Name	Virtual network link
Zone1.com	VNet1
Zone2.com	VNet2
Zone3.com	None

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Security type
Server1	Windows Server 2022 Datacenter: Azure Edition	Trusted launch
Server2	Windows Server 2022 Datacenter: Azure Edition	Standard
Server3	Windows Server 2022 Datacenter	Standard
Server4	Windows Server 2019 Datacenter	Trusted launch

All the servers are in a workgroup.

The subscription contains a storage account named storage1 that has a file share named share1.

Requirements -

Planned Changes -

ADatum plans to implement the following changes:

- Sync Data1 to share1.
- Configure an Azure runbook named Task1.
- Enable Azure AD users to sign in to Server1.
- Create an Azure DNS Private Resolver that has the following configurations:
  - Name: Private1
  - Region: West US
  - Virtual network: VNet1
  - Inbound endpoint: SubnetB
- Enable users in the adatum.com domain to access the resources in the south.fabrikam.com domain.

Technical Requirements -

ADatum identifies the following technical requirements:

- The data on SSPE1 must be available always.
- DC2 must become the schema master if DC1 fails.
- VM3 must be configured to enable per-folder quotas.
- Trusts must allow access to only the required resources.
- The users in the Marketing OU must have access to storage1.
- Azure Automanage must be used on all supported Azure virtual machines.
- A direct SSH session must be used to manage all the supported virtual machines on HyperV1.

You need to ensure that Automanage meets the technical requirements.

On which Azure virtual machines should you enable Automanage?

- A. Server1 only
- B. Server2 only
- C. Server1 and Server2 only
- D. Server2 and Server3 only
- E. Server1 and Server4 only

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Payday123** Highly Voted 1 year, 8 months ago

**Selected Answer: D**

"Automanage does not support Trusted Launch VMs"



<https://learn.microsoft.com/en-us/azure/automanage/overview-about>

upvoted 5 times

  **Ksk08** Most Recent 8 months ago

Answer is D

upvoted 1 times

  **Ksk08** 8 months, 1 week ago

Answer is C

upvoted 1 times

  **NazerRazer** 1 year, 8 months ago

Trusted Launch is not supported on Azure VMs and considering the options provided:

\* Server1 is a Windows Server 2022 Datacenter with Trusted Launch, so it should not have Azure Automanage enabled.

\* Server2 is a Windows Server 2022 Datacenter with a Standard security type, and Server3 is a Windows Server 2022 Datacenter with a Standard security type. Both Server2 and Server3 can have Azure Automanage enabled.

\* Server4 is a Windows Server 2019 Datacenter, and Trusted Launch is not supported on VMs, so it should not have Azure Automanage enabled.

Therefore, based on the information that Trusted Launch is not supported on VMs, you should enable Azure Automanage on:

D. Server2 and Server 3 only

Azure Automanage should be enabled on Server2 and Server3, as they both meet the criteria of using a supported operating system version (Windows Server 2022 with a Standard security type).

upvoted 3 times

  **windowsmodulesinstallerworker** 1 year, 9 months ago

Selected Answer: D

Automanage does not support Trusted Launch VMs

upvoted 4 times

  **FM221228** 1 year, 9 months ago

Wrong! Trusted launch is not supported with automanage.

upvoted 1 times

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains a server named Server1.

You implement Just Enough Administration (JEA) on Server1.

You need to perform remote administration tasks on Server by using only JEA.

What should you use?

- A. PowerShell only
- B. Remote Server Administration Tools (RSAT) only
- C. PowerShell or Remote Desktop only
- D. PowerShell or Remote Server Administration Tools (RSAT) only
- E. Remote Server Administration Tools (RSAT) or Remote Desktop only
- F. PowerShell, Remote Server Administration Tools (RSAT), or Remote Desktop

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **004b54b** 10 months, 1 week ago

**Selected Answer: A**

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell. (<https://learn.microsoft.com/en-us/powershell/scripting/security/remoting/jea/overview?view=powershell-7.4>)

Determine which commands to allow > meaning it is only available for PS cmdlets and not RSAT tools or RDP (<https://learn.microsoft.com/en-us/powershell/scripting/security/remoting/jea/role-capabilities?view=powershell-7.4#determine-which-commands-to-allow>)  
upvoted 1 times

🗳️ 👤 **Krayzr** 11 months, 4 weeks ago

**Selected Answer: A**

A. PowerShell only.

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything that can be managed with PowerShell. By using JEA, you can delegate specific tasks to non-administrative users without providing them full administrator rights.

Therefore, to perform remote administration tasks on Server1 by using only JEA, you should use PowerShell. Other tools like Remote Server Administration Tools (RSAT) or Remote Desktop are not necessary in this context. They provide broader administrative capabilities and are not limited to the specific roles and tasks that can be defined with JEA. So, the use of PowerShell aligns with the principle of least privilege, which is a key security benefit of JEA.  
upvoted 2 times

🗳️ 👤 **Payday123** 1 year, 7 months ago

**Selected Answer: A**

Corect  
upvoted 2 times

🗳️ 👤 **fabilo** 1 year, 8 months ago

**Selected Answer: A**

A is the answer  
upvoted 1 times

🗳️ 👤 **windowsmodulesinstallerworker** 1 year, 9 months ago

**Selected Answer: A**

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell.  
upvoted 4 times



You have an Azure subscription. The subscription contains a virtual machine named VM1 that runs Windows Server.

You plan to manage VM1 by using a PowerShell runbook.

You need to create the runbook.

What should you create first?

- A. an Azure Automation account
- B. an Azure workbook
- C. a Log Analytics workspace
- D. a Microsoft Power Automate flow

**Correct Answer: A**

*Community vote distribution*

A (100%)

004b54b 10 months, 1 week ago

**Selected Answer: A**

Given answer is right  
upvoted 1 times

Krayzr 11 months, 4 weeks ago

**Selected Answer: A**

A. an Azure Automation account.

Before you can create a PowerShell runbook, you need to create an Azure Automation account<sup>12</sup>. This account is where you will create and manage your runbooks. After creating the Automation account, you can then proceed to create the PowerShell runbook.

Please note that the other options (B. an Azure workbook, C. a Log Analytics workspace, D. a Microsoft Power Automate flow) are not the first steps in creating a PowerShell runbook in Azure Automation. They serve different purposes within the Azure ecosystem. For instance, an Azure workbook is used for data visualization and collaboration, a Log Analytics workspace is used for data collection and analysis, and a Microsoft Power Automate flow is used for automating workflows across applications and services. None of these are prerequisites for creating a PowerShell runbook in Azure Automation.

Therefore, the first step in creating a PowerShell runbook is to create an Azure Automation account.

upvoted 3 times

windowsmodulesinstallerworker 1 year, 9 months ago

**Selected Answer: A**

correct A  
upvoted 3 times

You have a server named Server1 that runs Windows Server and has the DHCP Server role installed. Server1 contains the following single scope:

- Scope: 192.168.16.0
- Address pool: 192.168.16.1-192.168.16.254
- Subnet mask: 255.255.255.0
- Lease duration: 8 days

You have four testing devices that are configured with static IP addresses as shown in the following table.

Name	IP address
TestDevice1	192.168.16.242
TestDevice2	192.168.16.243
TestDevice3	192.168.16.244
TestDevice4	192.168.16.245

The test devices are turned on once a month.

You need to prevent Server1 from assigning the IP addresses allocated to the test devices to other devices when the test devices are offline. The solution must minimize administrative effort.

What should you do?

- A. Create a policy.
- B. Create reservations.
- C. Configure the Scope options.
- D. Create an exclusion range.

**Correct Answer: D**

Community vote distribution

D (84%)

B (16%)

egdeeptha 10 months, 2 weeks ago

**Selected Answer: D**

Static IPs need to be excluded. If it was a DHCP client which needs to get the same IP over and over again when the lease expires reservations is the answer. But in this case EXCLUSIONS :)

upvoted 2 times

sardonique 10 months, 3 weeks ago

did it myself for many customers, you need to configure exclusions. Reservations are meant to statically assign IP based on mac address (so that whenever the host begs for an IP address, the DHCP server will always assign the same IP to that host)

upvoted 2 times

SIAMIANJI 1 year, 2 months ago

**Selected Answer: D**

You need to exclude static IPs.

Reservation are for DHCP assigned IPs.

upvoted 2 times

6de0f77 1 year, 4 months ago

**Selected Answer: D**

A reservation is for a DHCP request. A exclusion for fixed IP.

upvoted 3 times

SanMan\_NZ 1 year, 4 months ago

**Selected Answer: D**



An exclusion is required to ringfence IP's from DHCP Lease pool as they are static IPs. A reservation ties a leased IP to a constant MAC via DHCP control allowing perpetual fixed lease of IPs to the same servers.

upvoted 2 times

🗨️ 👤 **freddy** 1 year, 7 months ago

**Selected Answer: B**

D is wrong because you have to create \*two\* exclusions .242/31 and .244/31

If you make reservations DHCP won't lease those addresses. Though VMs won't use DHCP because they have static IPs, but this solution works.

B

upvoted 3 times

🗨️ 👤 **dolphan904** 1 year, 6 months ago

What are you talking about?? The IPs are in sequence on the 192.168.16/24 network. One exclusion works just fine by putting 242 as the first IP and 245 as the last IP with a mask of /24. Exclusion is the right answer as the servers have STATIC IPs which means they will not require DHCP leases for anything. RESERVATION would be correct only if they did require the leases against the same IP all the time which in this case they do not as explained before.

upvoted 6 times

🗨️ 👤 **freddy** 1 year, 7 months ago

I'm not right, delete :)

upvoted 3 times

🗨️ 👤 **Armoonbear** 1 year, 7 months ago

**Selected Answer: D**

Create an exclusion range to prevent DHCP from handing out addresses between 192.168.16.242 - 192.168.16.245

upvoted 3 times

🗨️ 👤 **windowsmodulesinstallerworker** 1 year, 9 months ago

**Selected Answer: D**

Since the devices are configured with static IP addresses which are defined on the network adapter of the devices, not by DHCP you should create an exclusion range which prevents the DHCP server to assign those IPs to other devices.

upvoted 4 times

🗨️ 👤 **FM221228** 1 year, 9 months ago

Wrong! The test devices have static IP addresses and thus reservations won't work. You must use an exclusion range.

upvoted 4 times

You have an Active Directory Domain Services (AD DS) domain. The domain contains three servers named Server1, Server2, and Server3 that run Windows Server.

You sign in to Server1 by using a domain account and start a remote PowerShell session to Server2. From the remote PowerShell session, you attempt to access a resource on Server3, but access to the resource is denied.

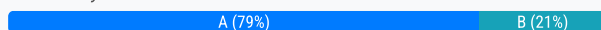
You need to ensure that your credentials are passed from Server1 to Server3. The solution must minimize administrative effort.

What should you do?

- A. Configure Kerberos constrained delegation.
- B. Configure Just Enough Administration (JEA).
- C. Configure selective authentication for the domain.
- D. Disable the Enforce user logon restrictions policy setting for the domain.

**Correct Answer: A**

Community vote distribution



🗲 👤 **Ksk08** 8 months ago

A: kerberos  
upvoted 1 times

🗲 👤 **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: A**

To ensure that your credentials are passed from Server1 to Server3 while minimizing administrative effort, you should configure Kerberos constrained delegation.

Therefore, the correct answer is:

A. Configure Kerberos constrained delegation.  
upvoted 4 times

🗲 👤 **Kuikz** 1 year, 3 months ago

**Selected Answer: A**

I will go with A, because the Questions says to minimize administrative effort.

The table in the liked source states, that Just Enough Administration (JEA) can provide the best security but requires more detailed configuration.

<https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/ps-remoting-second-hop?view=powershell-7.3>

upvoted 2 times

🗲 👤 **fbx01** 1 year, 4 months ago

**Selected Answer: A**

Configure Kerberos constrained delegation.  
upvoted 1 times

🗲 👤 **bdbea79** 1 year, 5 months ago

**Selected Answer: B**

I agree with B. In order to do Kerberos Constrained Delegation, you need domain admin permissions where it only mentions that you have a domain account. If it stated resource-based KCD then I would go with that but since not, then JEA it is according to Microsoft's preference list:

<https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/ps-remoting-second-hop?view=powershell-7.3>

upvoted 3 times

🗲 👤 **sardonique** 10 months, 3 weeks ago

a domain account without admin privileges cannot configure KCD, do you think that same account can configure JEA? good luck!  
upvoted 1 times

🗨️ 👤 **rknichols01** 1 year, 5 months ago

Option A, Configure Kerberos constrained delegation, would be the best solution for passing your credentials from Server1 to Server3. This option allows you to specify which services can use Kerberos to delegate the user's credentials to another service 1. By configuring constrained delegation, you can ensure that your credentials are passed from Server1 to Server3, and you can minimize administrative effort.

upvoted 3 times

🗨️ 👤 **dolphan904** 1 year, 6 months ago

FROM MS:

Just Enough Administration (JEA)

JEA allows you to restrict what commands an administrator can run during a PowerShell session. It can be used to solve the second hop problem.

upvoted 2 times

🗨️ 👤 **Aliabdo** 1 year, 7 months ago

**Selected Answer: A**

Configuring Kerberos constrained delegation allows you to pass your credentials from Server1 to Server3 when accessing a resource. Constrained delegation is a Kerberos feature that restricts the servers to which a service can delegate a user's credentials. This ensures that the delegation is secure and limited to specific services.

upvoted 2 times

🗨️ 👤 **cb0900** 1 year, 7 months ago

**Selected Answer: A**

I would edge towards A on this one. Solution to minimise administrative effort.

<https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/ps-remoting-second-hop?view=powershell-7.3>

upvoted 2 times

## SIMULATION

-

You need to collect the recommended Windows Performance Counters from SRV1 in a Log Analytics workspace.

The required files are stored in a shared folder named \\dc1\\install.

To complete this task, sign in to the required computer or computers.

**Correct Answer:**

## Microsoft Azure – Enable Windows Performance Counters in Azure for Monitoring

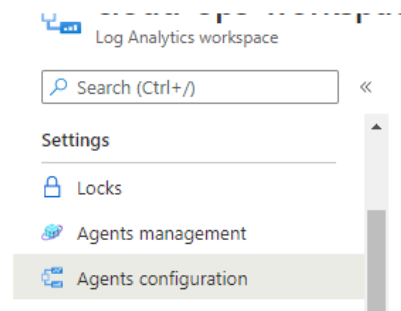
Collect windows performance counters from Log Analytics agents at custom intervals to gain insight into the performance of hardware components, operating systems, and applications.

### Implementation:

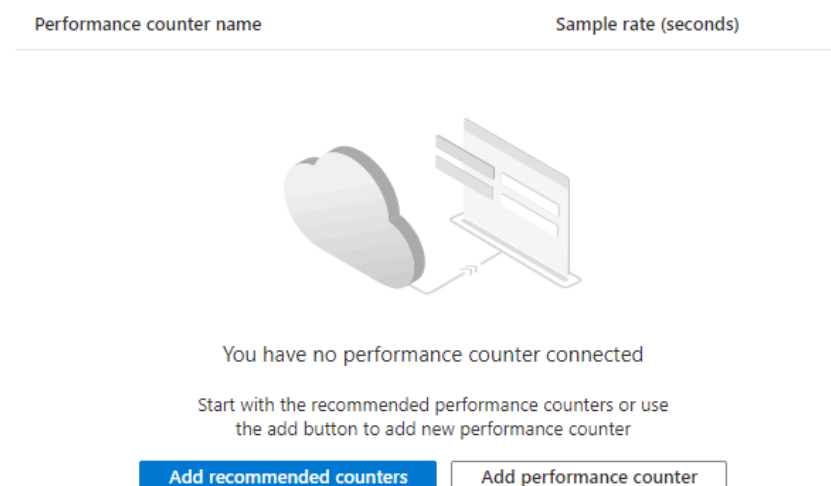
Step 1: Log in to Azure Portal.

Step 2: Access the Log Analytics Workspace >> Select your Log Analytics.

Step 3: After selecting the select Log Analytics Workspace, Navigate to Settings >> Agents Configuration



Step 4: Select Windows Performance Counters >> You can start with the recommended performance counters by clicking on Add recommended counters or using the add button to add a new performance counter.



Step 5: Click on + Add Performance Counter >> Select the Performance Counter name

Performance counter name	Sample rate (seconds)	
LogicalDisk(*)\% Free Space	60	
LogicalDisk(*)\Avg. Disk sec/Read	60	
LogicalDisk(*)\Avg. Disk sec/Write	60	
LogicalDisk(*)\Current Disk Queue Length	60	
LogicalDisk(*)\Disk Reads/sec	60	
LogicalDisk(*)\Disk Transfers/sec	60	
LogicalDisk(*)\Disk Writes/sec	60	
LogicalDisk(*)\Free Megabytes	60	
Memory(*)\% Committed Bytes In Use	60	
Memory(*)\Available MBytes	60	
Network Adapter(*)\Bytes Received/sec	120	
Network Adapter(*)\Bytes Sent/sec	120	
Network Interface(*)\Bytes Total/sec	120	
Processor(_Total)\% Processor Time	60	
SQLServer:Access Methods(*)\Forwarded Records/sec	60	
SQLServer:Access Methods(*)\Page Splits/sec	60	
SQLServer:Buffer Manager(*)\Buffer cache hit ratio	60	
SQLServer:Buffer Manager(*)\Page life expectancy	60	
SQLServer:Databases(*)\Backup/Restore Throughput/sec	60	
SQLServer:General Statistics(*)\Processes blocked	60	

Step 6: After adding the required Performance Counter name, click on Apply to make the changes.

That's it. You are done. At this point, we have successfully enabled Windows Performance Counters in Azure for Monitoring.

Reference:

<https://www.geeksforgeeks.org/microsoft-azure-enable-windows-performance-counters-in-azure-for-monitoring/>

📄 👤 **Krayzr** 10 months, 2 weeks ago

Step 5 should be

"Add recommended Counters"

According to the question

upvoted 2 times

You have an Active Directory Domain Services (AD DS) domain. The domain contains a member server named Server1 that runs Windows Server.

You need to ensure that you can manage password policies for the domain from Server1.

Which command should you run first on Server1?

- A. Install-WindowsFeature RSAT-AD-Tools
- B. Install-WindowsFeature RSAT-AD RMS
- C. Install-WindowsFeature GPMC
- D. Install-WindowsFeature RSAT-AD-PowerShell

**Correct Answer: A**

Community vote distribution



**sardonique** Highly Voted 10 months, 3 weeks ago

RsAT-AD-Tools include the following tools:

RSAT-AD-PowerShell

RSAT-AD LDS

and RSAT-AD DS, which has within it

RSAT-AD-AdminCenter

RSAT-AD DS-Tools

so if you install Rsat-AD-Tools you have pretty much everything you need, except GPMC which you might need to configure the GPOs, and the domain wide password settings. As always, the questions are ambiguous and dishonest made by frustrated guys with the purpose to set you up for failure.

upvoted 7 times

**formacionproxia** Most Recent 4 months, 2 weeks ago

**Selected Answer: D**

We only need RSAT-AD-PowerShell to define and assign Fine-Grained Password Policies, to manage passwords policies.

upvoted 1 times

**NoMedi** 5 months ago

**Selected Answer: A**

While the Group Policy Management Console (GPMC) is indeed a tool that can be used to manage password policies, it is not the most comprehensive option for this specific task.

The GPMC is primarily used for managing Group Policy Objects (GPOs), including the Default Domain Policy where the domain-wide password policy is typically configured. However, installing only the GPMC would not provide all the necessary tools for comprehensive password policy management, especially when it comes to more advanced features like Fine-Grained Password Policies (FGPP)

upvoted 2 times

**Ni\_yot** 8 months, 1 week ago

**Selected Answer: A**

A appears correct. After these conflicting comments i decided to use chatgpt and the answer is interesting. By installing RSAT and using the Group Policy Management Console, you can effectively manage password policies for your Active Directory domain from Server1. Since its a member server you install RSAT first, then GMPC

upvoted 1 times

**Ksk08** 8 months, 2 weeks ago

A is correct you have to install Install-WindowsFeature RSAT-AD DS before you can Install-WindowsFeature GPMC. The question is asking which one to perform first for the task

upvoted 1 times

**mhmyz** 9 months, 3 weeks ago

**Selected Answer: C**

RsAT-AD-Tools not support Windows Server and not include GPO management tool.



upvoted 1 times

🗨️ 👤 **Krayzr** 11 months, 4 weeks ago

**Selected Answer: A**

A. Install-WindowsFeature RSAT-AD-Tools.

The RSAT-AD-Tools feature includes command-line tools for managing Active Directory Domain Services (AD DS). These tools help you manage domains, users, and computers, effectively allowing you to manage password policies for the domain.

Here's why the other options are not the best choices:

C. Install-WindowsFeature GPMC: This command installs the Group Policy Management Console. While GPMC is used to manage Group Policies, it is not specifically required to manage password policies from a member server.

Remember, after installing the RSAT-AD-Tools feature, you can use the Group Policy Management Console or Active Directory Administrative Center to manage password policies. You can also use PowerShell commands to manage password policies.

upvoted 3 times

🗨️ 👤 **AK\_1234** 1 year, 1 month ago

Answer C

upvoted 2 times

🗨️ 👤 **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: C**

Group Policy Management Console

upvoted 2 times

🗨️ 👤 **IcE** 1 year, 2 months ago

**Selected Answer: C**

Group Policy Management Console (GPMC)

upvoted 2 times

🗨️ 👤 **DATS720** 1 year, 2 months ago

**Selected Answer: C**

C: You need to edit a GPO for this. You need GPMC.

upvoted 3 times

🗨️ 👤 **pnewcap** 1 year, 2 months ago

**Selected Answer: A**

A I GUESS

upvoted 2 times

## SIMULATION

-

You need to ensure that you can manage DC1 by using Windows Admin Center on SRV1.

The required source files are located in a folder named \\dc1.contoso.com\install.

To complete this task, sign in the required computer or computers.

## Correct Answer:

**Install Windows Admin Center on DC1**

**Step 1:** On dc1 locate folder \\dc1.contoso.com\install, start installation, complete Wizard.

Once the install is complete, open a browser from a remote computer and navigate to URL presented in the last step of the installer.

**Step 2:** On SRV1 use the URL from the installation process, and complete the installation.

**Reference:**

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/deploy/install>

🗨️ 👤 **Krayzr** 11 months, 4 weeks ago

Install Windows Admin Center on SRV1: You can download the installer from the official Microsoft website and run it on SRV1. During installation, choose the appropriate options for your environment.

Add DC1 to Windows Admin Center: After installation, open Windows Admin Center and click on Add in the All Connections pane. In the Add Server Connection pane, enter the name of the server (DC1) you want to manage and click on Submit.

upvoted 3 times

🗨️ 👤 **PressFfive** 6 months ago

yea, you cannot install Admin Center on DC1, why tf this website wrong answers to many questions? we paid this website to get correct answer, instead community has to correct. I will never come back here study again.

upvoted 3 times

🗨️ 👤 **e489b39** 3 weeks, 4 days ago

You are right me also i will never pay cent here again no one study and keeps choosing random answers

upvoted 1 times

🗨️ 👤 **Krayzr** 9 months, 2 weeks ago

\* get the files for WAC from \\dc1.contoso.com\install (as per the question)

upvoted 1 times

🗨️ 👤 **Jothar** 1 year, 1 month ago

Given answer has you installing WAC on a dc which is not supported.

<https://techcommunity.microsoft.com/t5/windows-admin-center/installing-windows-admin-center-on-domain-controller-solved/m-p/4041774>

upvoted 4 times

## SIMULATION

-

You need to monitor the security configuration of DC1 by using Microsoft Defender for Cloud.

The required source files are located in a folder named \\dc1.contoso.com\install.

To complete this task, sign in the required computer or computers.

**Correct Answer:**

You can connect your non-Azure computers in any of the following ways:

- \* Onboarding with Azure Arc:
  - By using Azure Arc-enabled servers (recommended)
  - >By using the Azure portal
- \* Onboarding directly with Microsoft Defender for Endpoint

Connect on-premises machines by using the Azure portal

After you connect Defender for Cloud to your Azure subscription, you can start connecting your on-premises machines from the Getting started page in Defender for Cloud.

Step 1: Sign in to the Azure portal.

Step 2: Search for and select Microsoft Defender for Cloud.

Step 3: On the Defender for Cloud menu, select Getting started.

Step 4: Select the Get started tab.

Step 5: Find Add non-Azure servers and select Configure.

A list of your Log Analytics workspaces appears.

Step 6: (Optional) If you don't already have a Log Analytics workspace in which to store the data, select Create new workspace, and follow the on-screen guidance.

Step 7: From the list of workspaces, select Upgrade for the relevant workspace to turn on Defender for Cloud paid plans for 30 free days.

Step 8: From the list of workspaces, select Add Servers for the relevant workspace.

On the Agents management page, choose one of the following procedures, depending on the type of machines you're onboarding (Either Windows or Linux)

Onboard your Windows server

When you add a Windows server, you need to get the information on the Agents management page and download the appropriate agent file (32 bit or 64 bit).

To onboard a Windows server:

Step 1: Select Windows servers.

Step 2: Select the Download Windows Agent link that's applicable to your computer processor type to download the setup file.

Step 3: From the Agents management page, copy the Workspace ID and Primary Key values into Notepad.

Step 4: Copy the downloaded setup file to the target computer and run it.

Step 5: Follow the installation wizard (select Next > I Agree > Next > Next).

Step 6: On the Azure Log Analytics page, paste the Workspace ID and Primary Key values that you copied into Notepad.

Step 7: If the computer should report to a Log Analytics workspace in the Azure Government cloud, select Azure US Government from the Azure Cloud dropdown list.

Step 8: If the computer needs to communicate through a proxy server to the Log Analytics service, select Advanced. Then provide the URL and port number of the proxy server.

Step 9: When you finish entering all of the configuration settings, select Next.

Step 10: On the Ready to Install page, review the settings to be applied and select Install.

Step 11: On the Configuration completed successfully page, select Finish.

When the process is complete, Microsoft Monitoring agent appears in Control Panel. You can review your configuration there and verify that the agent is connected.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines>

Currently there are no comments in this discussion, be the first to comment!

## SIMULATION

-

You plan to create group managed service accounts (gMSAs).

You need to configure the domain to support the creation of gMSAs.

To complete this task, sign in the required computer or computers.

**Correct Answer:****Getting Started with Group Managed Service Accounts****Preparing the domain**

Perform these steps to prepare the domain:

Step 1: Run ADPrep /domainPrep

You will then see:

```
PS D:\support\adprep> .\adprep.exe /domainPrep
Adprep successfully updated the domain-wide information.
```

Note: Active Directory Domain Service requirements


The Active Directory schema in the gMSA domain's forest needs to be updated to Windows Server 2012 to create a gMSA.

\*-> You can update the schema by installing a domain controller that runs Windows Server 2012 or by running the version of adprep.exe from a computer running Windows Server 2012 . The object-version attribute value for the object CN=Schema,CN=Configuration,DC=Contoso,DC=Com must be 52.

Reference:


<https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>

<https://www.koolaid.info/dude-wheres-my-managed-service-accounts/>

 **LuLaCeK** 5 months, 1 week ago

Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))

upvoted 1 times

 **stonwall12** 5 months, 3 weeks ago

To configure a domain to support the creation of group Managed Service Accounts (gMSAs), you need to run the following PowerShell command:

Add-KdsRootKey -EffectiveImmediately

This command creates a new Key Distribution Services (KDS) root key, which is required for gMSAs to generate and maintain their passwords.

Reference: <https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/create-the-key-distribution-services-kds-root-key>

upvoted 1 times

 **Jothar** 7 months, 2 weeks ago

Should be add-kdsrootkey

upvoted 1 times

 **Krayzr** 6 months, 3 weeks ago

Add-KdsRootKey -EffectiveImmediately

upvoted 2 times

 **7dbb96a** 10 months, 1 week ago

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-managed-service-accounts/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>

upvoted 2 times

 **sardonique** 10 months, 3 weeks ago

this doesn't seem a correct answer. You need to create a KDS root in order to be able to use GMSAs  
upvoted 3 times



## DRAG DROP

-

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains two servers named Server1 and Server2 that run Windows Server 2022.

You plan to deploy an app named App1 that will be load balanced between Server1 and Server2.

You need to create an identity that will be used to run App1 on Server1 and Server2. The solution must meet the following requirements:

- The password for the identity must be changed regularly.
- Administrative effort must be minimized.

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.

## Actions

- Create a standalone managed service account (sMSA).
- Create a service principal name (SPN).
- Enable constrained delegation for Server1 and Server2.
- Create a Key Distribution Services (KDS) root key.
- Create a group managed service account (gMSA).
- Install the service account on Server1 and Server2.

## Answer Area

- 1
- 2
- 3



## Correct Answer:

- Answer Area**
- 1 Create a Key Distribution Services (KDS) root key.
  - 2 Create a group managed service account (gMSA).
  - 3 Install the service account on Server1 and Server2.

**stonwall12** 5 months, 3 weeks ago

Answer:

1. Create a Key Distribution Services (KDS) root key
2. Create a group managed service account (gMSA)
3. Install the service account on Server1 and Server2

1. The KDS root key must be created first as it's a prerequisite for creating gMSAs. It enables the domain to generate and distribute passwords for gMSAs.
2. Next create the gMSA after the KDS root key is in place.
3. Finally, install the gMSA on both servers where App1 will run. This allows the servers to retrieve and use the gMSA's credentials.

Reference: <https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>

upvoted 1 times

**Krayzr** 7 months, 2 weeks ago

Given answer correct

Create a Key Distribution Services (KDS) root key: This is necessary for creating group managed service accounts (gMSAs).

Create a group managed service account (gMSA): gMSAs are designed to be used across multiple servers and automatically handle password management.

Install the service account on Server1 and Server2: This step ensures that both servers can use the gMSA to run App1.

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

Answer is correct

upvoted 1 times

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains a server named Server1.

On Server1, you install Windows Admin Center and use Windows Admin Center to remove BUILTIN\Users from the allowed groups.

You discover that all users can still sign in to Windows Admin Center.

You need to prevent unauthorized users from signing in to Windows Admin Center.

What should you do in Windows Admin Center?

- A. Set Performance Profile to On.
- B. Set Require manage-as sessions to re-authenticate to On.
- C. From the Proxy settings, configure a bypass list.
- D. Add a security group to the allowed groups.

**Correct Answer:** D

Community vote distribution

D (100%)

  **stonwall12** 5 months, 3 weeks ago

**Selected Answer:** D

Answer: D, security group

After removing BUILTIN\Users, you must add a specific security group to the allowed groups list. Without adding an allowed group, Windows Admin Center defaults to allowing all users despite removing BUILTIN\Users. Adding a security group provides proper access control.

Reference: <https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options>  
upvoted 1 times

  **Krayzr** 7 months, 2 weeks ago

**Selected Answer:** D

By adding a specific security group to the allowed groups, you can control which users have access to Windows Admin Center. This ensures that only authorized users within that security group can sign in

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options>  
upvoted 1 times

  **Ni\_yot** 8 months ago

**Selected Answer:** D

there are a number of ways Windows Admin Center can be secured - <https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options>  
upvoted 2 times

  **Ksk08** 8 months, 2 weeks ago

Answer should be D  
upvoted 3 times

You have on-premises servers that run Windows Server as shown in the following table.

Name	Type
Server1	Physical server
VM2	Hyper-V virtual machine

You have an Azure subscription that contains a virtual machine named VM1.

You need to ensure that you can manage all the servers by using Azure Arc. The solution must minimize administrative effort.


On which servers should you install the Azure Connected Machine agent?

- A. Server1 only
- B. VM1 only
- C. VM2 only
- D. VM1 and VM2 only
- E. Server1 and VM2 only
- F. Server1, VM1, and VM2

**Correct Answer: E**

Community vote distribution

E (100%)

 **stonwall12** 5 months, 3 weeks ago

**Selected Answer: E**

Answer: E, Server1 and VM2 only

Azure Connected Machine agent is required for on-premises servers only. Native Azure VMs like VM1 are already managed by Azure natively. This minimizes administrative effort by avoiding unnecessary agent installation on VM1.

Reference: <https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview>

upvoted 1 times

 **db94** 7 months, 3 weeks ago

**Selected Answer: E**

You shouldn't install Azure Arc on virtual machines hosted in Azure, Azure Stack Hub, or Azure Stack Edge, as they already have similar capabilities. You can, however, use an Azure VM to simulate an on-premises environment for testing purposes, only.

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/prerequisites>

upvoted 3 times

 **Ksk08** 8 months, 3 weeks ago

Answer E

upvoted 4 times

## HOTSPOT

-

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains the servers shown in the following table.

Name	Type
DC1	Domain controller
Server1	Member server
Server2	Member server

The domain contains the users shown in the following table.

Name	Member of
User1	Contoso\Administrators
User2	Contoso\Remote Management Users
User3	Server2\Power Users

On Server2, you run the Enable-PSRemoting cmdlet.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.


NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 can establish a PowerShell remoting session from Server1 to Server2.	<input type="radio"/>	<input type="radio"/>
User2 can establish a PowerShell remoting session from Server2 to DC1.	<input type="radio"/>	<input type="radio"/>
User3 can establish a PowerShell remoting session from Server1 to Server2.	<input type="radio"/>	<input type="radio"/>

## Correct Answer:

Statements	Yes	No
User1 can establish a PowerShell remoting session from Server1 to Server2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can establish a PowerShell remoting session from Server2 to DC1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can establish a PowerShell remoting session from Server1 to Server2.	<input type="radio"/>	<input checked="" type="radio"/>

 **LionelS** 3 months, 1 week ago

No No No

By default, remoting requires admin access on the target computer.

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_requirements](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements)

The only account with admin access is User1, but it's not member of the Domain Admins group, only of the built-in Administrators group of the domain, that has admin access on the Domain Controllers only. The only working scenario would be User1 remoting to DC1.

upvoted 2 times

 **Opoveda** 3 months, 1 week ago

I think is Y N N

upvoted 1 times

 **Krayzr** 7 months, 2 weeks ago

YNN

User1 can establish a PowerShell remoting session from Server1 to Server2.

\*\*Yes. User1 is a member of the Contoso\Administrators group, which typically has the necessary permissions to establish a PowerShell remoting

session.



User2 can establish a PowerShell remoting session from Server2 to DC1.

\*\*No. User2 is a member of the Contoso\Remote Management Users group, which allows remote management but does not necessarily grant permissions to connect to a domain controller unless explicitly configured.

User3 can establish a PowerShell remoting session from Server1 to Server2.

\*\*No. User3 is a member of the Server2\Power Users group, which grants elevated privileges on Server2 but does not inherently provide permissions to establish a remote session from another server.

upvoted 2 times

  **LuLaCeK** 5 months, 3 weeks ago

Not true. Contoso\Administrators is build in group for Domain Controller. Not for Server2.

So it won't work.

upvoted 2 times

  **e489b39** 3 weeks, 4 days ago

Contoso\Administrators is Domain Admins group since Contoso is the domain not the computer

upvoted 1 times

  **Jothar** 7 months, 2 weeks ago

Remote Management users is a built-in local group. Needs to be granted on server2 itself. So YNN by default- only domain admins who are part of the built-in local administrators.

upvoted 1 times

  **Ni\_yot** 8 months ago

YNN. The Enable-PSRemoting command is a PowerShell cmdlet that configures the local computer to receive Windows PowerShell remote commands. This is essential for enabling PowerShell remoting, which allows you to run PowerShell commands and scripts on remote computers.

Power users do not have permissions to logon remotely

upvoted 2 times

  **Ksk08** 8 months, 2 weeks ago

Answer is Yes No No

upvoted 3 times

  **Ksk08** 8 months, 3 weeks ago

Correct answer

upvoted 1 times

  **Ksk08** 8 months, 2 weeks ago

sorry this is wrong

upvoted 1 times

Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains a user named User1 and the servers shown in the following table.

Name	Operating system
Server1	Windows Server 2016
Server2	Windows Server 2022
Backup1	Windows Server 2019

User1 is a member of the Protected Users security group.

User1 performs the following actions:

- From Server1, establishes a remote PowerShell session on Server2
- From the PowerShell session on Server2, attempts to access a resource on Backup1

The request to access the resource on Backup1 is denied.

You need to ensure that User1 can access the resources on Backup1 by using the PowerShell session on Server2. The solution must follow the principle of least privilege and minimize administrative effort.


What should you configure?

- A. Kerberos delegation (unconstrained)
- B. CredSSP
- C. PSSessionConfiguration by using RunAs
- D. resource-based Kerberos constrained delegation

**Correct Answer: D**

Community vote distribution

D (100%)

 **stonwall12** 5 months, 3 weeks ago

**Selected Answer: D**

Answer: D, resource-based Kerberos constrained delegation

This scenario requires double-hop authentication from Server1 to Server2 via PowerShell, then from Server2 to Backup1 for resource access. Resource-based Kerberos constrained delegation is the most appropriate solution as it follows the principle of least privilege by configuring delegation at the resource level (Backup1) and minimizes administrative effort without requiring domain admin rights.

Reference: <https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-constrained-delegation-overview>  
upvoted 1 times

 **Krayzr** 7 months, 2 weeks ago

**Selected Answer: D**

Resource-based Kerberos constrained delegation

Resource-based Kerberos constrained delegation allows you to specify which services can delegate to which resources, providing a more secure and controlled delegation compared to unconstrained delegation. This setup ensures that User1 can access the necessary resources without granting excessive permissions  
upvoted 1 times

 **Ksk08** 8 months, 3 weeks ago

Answer: D

upvoted 1 times

You have 50 on-premises servers that run Windows Server.

You have an Azure subscription.

You plan to monitor the on-premises servers by using Azure Monitor.

You need to collect event logs from the on-premises servers.

What should you do first?

- A. From the Azure portal, create a storage account.
- B. From the Azure portal, create a Log Analytics workspace.
- C. From the on-premises servers, run `azuremonitoragentclientsetup.msi`.
- D. From the Azure portal, create a data collection rule (DCR) in Azure Monitor.

**Correct Answer: B**

*Community vote distribution*

B (83%)

C (17%)

 **stonwall12** 5 months, 3 weeks ago

**Selected Answer: B**

Answer: B, create a Log Analytics workspace

To monitor on-premises servers with Azure Monitor, a Log Analytics workspace must be created first as it's the foundation for storing and analyzing log data.

Reference: <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview>  
upvoted 2 times

 **Krayzr** 7 months, 2 weeks ago

**Selected Answer: B**

A Log Analytics workspace is essential for storing and analyzing the data collected from your servers. Once the workspace is set up, you can proceed with installing the Azure Monitor agent on your servers and configuring data collection rules  
upvoted 3 times

 **Webcatman** 7 months, 3 weeks ago

**Selected Answer: C**

The Answer is C. Setup a monitor agent first.

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview>  
upvoted 1 times

 **e489b39** 3 weeks, 4 days ago

The agent requires specific configuration details from the workspace to function correctly  
upvoted 1 times

 **e489b39** 3 weeks, 4 days ago

Without a Log Analytics the Agent cannot be properly configured to send data  
upvoted 1 times

 **Ksk08** 8 months, 2 weeks ago

B is Correct

upvoted 1 times



You have a server named Host1 that has the Hyper-V server role installed. Host1 hosts a virtual machine named VM1.

You have a management server named Server1 that runs Windows Server. You remotely manage Host1 from Server1 by using Hyper-V Manager.

You need to ensure that you can access a USB hard drive connected to Server1 when you connect to VM1 by using Virtual Machine Connection.

Which two actions should you perform? Each correct answer presents part of the solution.


NOTE: Each correct selection is worth one point.

- A. From the Hyper-V Settings of Host1, select Allow enhanced session mode.
- B. From Virtual Machine Connection, select Show Options, and then select the USB hard drive.
- C. From Virtual Machine Connection, switch to a basic session.
- D. From Disk Management on Host1, select Rescan Disks.
- E. From Disk Management on Host1, attach a virtual hard disk.

**Correct Answer:** AB

Community vote distribution


AB (100%)

 **AvoKikinha** Highly Voted 3 years, 1 month ago

**Selected Answer:** AB


Correct A + B

upvoted 15 times

 **georgecuba** Highly Voted 3 years, 2 months ago

I believe B + D are correct

upvoted 6 times

 **AvoKikinha** 3 years, 1 month ago

From: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/learn-more/use-local-resources-on-hyper-v-virtual-machine-with-vmconnect>

As you can see on link in "Choose a local resource" section

Open VMConnect.

Select the virtual machine that you want to connect to.

Click Show options.


Select Local resources.

Click More.

Select the drive that you want to use on the virtual machine and click Ok.

A+B are the correct

upvoted 9 times

 **Starburst** 2 years, 11 months ago

Why???

upvoted 2 times

 **stonwall12** Most Recent 5 months, 3 weeks ago

**Selected Answer:** AB

Answer: A and B

To enable USB device redirection in a Hyper-V virtual machine connection from a remote management server:

A. Enable enhanced session mode on Host1 (option A) because:

- Enhanced sessions are required for device redirection
- This setting must be configured on the Hyper-V host

B. Select the USB drive from Virtual Machine Connection options because:

- After enhanced session mode is enabled, devices can be selected for redirection

- This allows the VM to access the USB drive connected to Server1

Reference: <https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/learn-more/use-local-resources-on-hyper-v-virtual-machine-with-vmconnect>

upvoted 1 times

🗨️ 👤 **sardonique** 10 months, 3 weeks ago

A and B, Tested in LAB, A because it allows the local resources to be exposed to the VMs, B because you would get the same options as RDP where you can choose PlugPlay devices, local hard disks, and so on (you can even pass your microphone to the VM)

upvoted 2 times

🗨️ 👤 **fbx01** 1 year, 4 months ago

**Selected Answer: AB**

Correct A + B

upvoted 1 times

🗨️ 👤 **SanMan\_NZ** 1 year, 4 months ago

**Selected Answer: AB**

A + B are correct from my recollection.

upvoted 1 times

🗨️ 👤 **afridi43** 1 year, 9 months ago

**Selected Answer: AB**

A.

This allows enhanced session mode, which can provide USB redirection and other features.

B.

When connecting to VM1 using VMConnect, you can configure local resources, including USB devices, through the "Show Options" menu.

So, the correct actions to perform are A and B, as they allow you to enable enhanced session mode and configure USB device redirection to access the USB hard drive connected to Server1 when connecting to VM1 using VMConnect.

upvoted 3 times

🗨️ 👤 **syu31svc** 2 years, 3 months ago

**Selected Answer: AB**

A and B are correct as supported by link given

upvoted 4 times

🗨️ 👤 **Contactfornitish** 2 years, 10 months ago

**Selected Answer: AB**

There are couple of ways to do this but since it's asked that drive should be available when connect via VM connect, A+B is correct. Choose local drive under local resources, no need to re scan

upvoted 5 times

🗨️ 👤 **VinoTee** 3 years, 2 months ago

Correct

upvoted 4 times

You have a Windows Server container host named Server1 and a container image named image1.  
 You need to start a container from image1. The solution must run the container on a Hyper-V virtual machine.  
 Which parameter should you specify when you run the docker run command?

- A. --expose
- B. --privileged
- C. --runtime
- D. --isolation
- E. --entrypoint

**Correct Answer: D**

Community vote distribution

D (90%)

10%

 **Larcomb** Highly Voted 2 years, 7 months ago

Should be D --isolation  
 upvoted 16 times

 **nefaxto** Highly Voted 2 years, 6 months ago

D  
<https://docs.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container>  
 upvoted 8 times

 **GoforIT21** 2 years, 5 months ago

Thanks! You're right, I withdraw my comment (figuratively, as I can't delete it here :-).  
 upvoted 4 times

 **stonwall12** Most Recent 5 months, 3 weeks ago

**Selected Answer: D**

Answer: D, isolation

To run a Windows Server container in Hyper-V isolation mode, you need to use the --isolation parameter with the value "hyperv" in the docker run command. This tells Docker to create the container inside a Hyper-V virtual machine instead of sharing the host's kernel.

Reference: <https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container>

upvoted 1 times

 **nawtitoo** 7 months ago

**Selected Answer: D**

Hyper-V isolation provides stronger isolation by running each container in a lightweight virtual machine, which is useful for running containers that need a higher level of security and isolation from the host and other containers.  
 upvoted 2 times

 **SIAMIANJI** 8 months ago

**Selected Answer: D**

To run a container on a Hyper-V virtual machine, you should specify the --isolation parameter with the value hyperv.  
 upvoted 3 times

 **Shailesh866** 1 year ago

Answer is D  
 docker run --isolation hyperv image1  
 upvoted 1 times

 **Bolo92** 1 year, 1 month ago

valid 27.11.23  
 upvoted 2 times

🗳️ 👤 **afridi43** 1 year, 3 months ago

**Selected Answer: D**

Here's how you would run the container with Hyper-V isolation:

```
docker run --isolation hyperv image1
```

To run a container on a Hyper-V virtual machine, you should specify the `--isolation` parameter with the value set to `hyperv` when you run the `docker run` command. This parameter instructs Docker to use Hyper-V isolation for the container.

upvoted 1 times

🗳️ 👤 **leegend** 1 year, 7 months ago

Got this question 28-5-23

upvoted 2 times

🗳️ 👤 **syu31svc** 1 year, 9 months ago

**Selected Answer: D**

D is correct and provided link supports it

upvoted 1 times

🗳️ 👤 **King\_Laps** 2 years, 4 months ago

It should be D - Isolation

upvoted 2 times

🗳️ 👤 **SJHCI** 2 years, 5 months ago

**Selected Answer: D**

Should be D: <https://docs.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container>

upvoted 4 times

🗳️ 👤 **[Removed]** 2 years, 5 months ago

**Selected Answer: D**

Isolation

upvoted 2 times

🗳️ 👤 **mazahaf** 2 years, 5 months ago

D Isolation

upvoted 3 times

🗳️ 👤 **ANDREVOX** 2 years, 5 months ago

The solution must run the container on a Hyper-V virtual machine.

Operating system requirements: The Hyper-V role must be installed before running Hyper-V isolation.

`--isolation` = Container isolation technology where `--entrypoint` = Overwrite the default ENTRYPOINT of the image.

Answer: D

upvoted 4 times

🗳️ 👤 **GoforIT21** 2 years, 6 months ago

**Selected Answer: B**

Well, I'm certainly not a Docker expert, ok? But if I read things up on the official Docker reference site for the `run` command

(<https://docs.docker.com/engine/reference/run/>) I do notice that "`--isolation`" doesn't (seem to) exist as a parameter for that command.

The only answer that does make some sense to me is B (`--privileged`).

I'm happy to be corrected (sources please!), but I do wonder where the unanimity about answer D comes from...

upvoted 2 times

🗳️ 👤 **CJCoolio** 2 years, 7 months ago

**Selected Answer: D**

Should be D

upvoted 5 times

🗳️ 👤 **Bojana** 2 years, 7 months ago

correct, it's D

upvoted 2 times

You plan to deploy a containerized application that requires .NET Core.  
 You need to create a container image for the application. The image must be as small as possible.  
 Which base image should you use?

- A. Windows Server
- B. Nano Server
- C. Windows
- D. Server Core

**Correct Answer: B**

Community vote distribution

B (100%)

🗲️ 👤 **AvoKikinha** Highly Voted 👍 2 years, 7 months ago

**Selected Answer: B**

Nano Server base container image

This is our smallest base container image. As mentioned above, this means less APIs available. For Nano Server, we focused on scenarios where developers will be writing new applications on which the framework can target the specific APIs of Nano Server. Examples of frameworks, languages, or apps that are supported on Nano Server are .Net Core (now called .Net)  
 upvoted 5 times

🗲️ 👤 **SDK76** Most Recent 🕒 2 months, 1 week ago

**Selected Answer: B**

Here's a brief overview of the different container images and their best use cases:

1. Nano Server:
    - o Best for lightweight, modern applications built on .NET Core or similar frameworks.
    - o Ideal for scenarios requiring minimal APIs and fast scaling.
  2. Server Core:
    - o Suitable for "lift-and-shift" scenarios where existing Windows Server applications are moved to containers without code changes.
    - o Provides medium-sized API support.
  3. Windows:
    - o Offers full Windows API support, making it ideal for applications requiring extensive Windows libraries.
    - o Largest image, suitable for workloads needing comprehensive compatibility.
  4. Windows Server:
    - o Similar to the Windows image but slightly smaller.
    - o Supports server-specific features and applications.
- upvoted 1 times

🗲️ 👤 **stonwall12** 5 months, 3 weeks ago

Answer: B, Nano Server

Nano Server is the smallest Windows container base image available and is specifically optimized for running .NET Core applications in containers.

Reference: <https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/container-base-images>  
 upvoted 1 times

🗲️ 👤 **knotcz** 10 months, 1 week ago

<https://learn.microsoft.com/en-gb/virtualization/windowscontainers/manage-containers/container-base-images>  
 upvoted 1 times

🗲️ 👤 **Bolo92** 1 year, 1 month ago

valid 27.11.23  
 upvoted 2 times

🗲️ 👤 **afridi43** 1 year, 3 months ago

**Selected Answer: B**

Nano Server is a lightweight, minimal-footprint version of Windows Server designed specifically for containerized applications. It has a smaller image size compared to Server Core and is well-suited for running .NET Core applications in containers, helping to reduce the overall image size and resource usage.

upvoted 1 times


🗉  **syu31svc** 1 year, 9 months ago

**Selected Answer: B**

"as small as possible"

B is correct then

upvoted 2 times

🗉  **scribe** 1 year, 11 months ago

Nano server in 2022/2023 - nano version is abandoned in with 2016 Server

upvoted 2 times

🗉  **King\_Laps** 2 years, 5 months ago

Nano server is correct: B

upvoted 2 times

🗉  **amunator** 2 years, 5 months ago

**Selected Answer: B**

Nano Server is correct answer.

upvoted 2 times

🗉  **TheUltimateHac** 2 years, 7 months ago

**Selected Answer: B**

Answer is Correct Nano Server

upvoted 3 times

You have an Azure virtual machine named VM1 that runs Windows Server.

You perform the following actions on VM1:

- ⇒ Create a folder named Folder1 on volume C.
- ⇒ Create a folder named Folder2 on volume D.
- ⇒ Add a new data disk to VM1 and create a new volume that is assigned drive letter E.
- ⇒ Install an app named App1 on volume E.

You plan to resize VM1.

Which objects will present after you resize VM1?

- A. Folder1, volume E, and App1 only
- B. Folder1 only
- C. Folder1 and Folder2 only
- D. Folder1, Folder2, App1, and volume E

**Correct Answer: A**

Community vote distribution

A (77%)

D (23%)

🗳️ 👤 **Ipkramit** Highly Voted 3 years, 1 month ago

the answer is A, folder 2 is on D: which by default is the scratch disk that is wiped on a re-boot, a re-size of the VM requires a reboot of the VM, therefore the upvoted 44 times

🗳️ 👤 **VinoTee** 3 years, 1 month ago

This is correct. Volume D is a default temporary storage, hence, anything that you store on that volume letter will be wiped.

See link below with the highlighted answer:

<https://www.cloudelicious.net/azure-vms-and-their-temporary-storage/#:~:text=For%20Windows%20Server%2C%20the%20temporary%20disk%20is%20mounted%20as%20D%3A%5C.%20Linux%20based%20VM%E2%8>

upvoted 5 times

🗳️ 👤 **JimmyC** 1 year ago

The idea that most Azure VMs include a temp disk is very incorrect - many commonly-used VM SKUs do not. However, based on the wording of the question, the answer is A. upvoted 2 times

🗳️ 👤 **NigHtHunter2000** 3 years, 1 month ago

Correct

Link to verify

<https://docs.microsoft.com/en-us/answers/questions/235/can-i-use-the-temporary-disk-the-d-drive-by-default.html>

upvoted 3 times

🗳️ 👤 **NigHtHunter2000** 3 years, 1 month ago

I mean Answer A is correct

upvoted 8 times

🗳️ 👤 **Bojana** Highly Voted 3 years, 1 month ago

**Selected Answer: A**

the answer is A

upvoted 9 times

🗳️ 👤 **e489b39** Most Recent 3 weeks, 4 days ago

**Selected Answer: D**

If volume D is not data disk the new attached volume will not be E

C os, D Data disk and E data disk

upvoted 1 times

🗳️ 👤 **Ksk08** 8 months ago

fter resizing VM1:


Folder1 (on C:) will persist.

Folder2 (on D:) will be lost because D: is likely a temporary disk.

Volume E and App1 installed on it will persist because they are on a persistent data disk.

Thus, the correct answer is indeed A. Folder1, volume E, and App1 only.

upvoted 1 times

  **Ksk08** 8 months, 1 week ago

D is the correct answer

upvoted 1 times



  **RemmyT** 1 year ago

**Selected Answer: A**

Tested in lab:



After the resize (up or down) volume D: is re-initialized with default settings.

upvoted 1 times

  **Joedn** 1 year, 1 month ago

Valid 05/28/2024

upvoted 2 times

  **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: D**

After resizing VM1, both Folder1 (created on volume C) and Folder2 (created on volume D) will still be present. Additionally, App1 (installed on volume E) and Volume E (created after adding the new data disk) will also remain.

Therefore, the correct answer is:


D. Folder1, Folder2, App1, and volume E

upvoted 2 times

  **MichalGr** 1 year, 2 months ago

By default, most Azure virtual machines (VMs) are provisioned with a temporary disk, which is often labeled as the D: drive in Windows VMs. Also, with default settings for a new volume E, which typically includes using Azure managed disks, both volume E and the application installed on it (App1) are likely to stay intact after resizing the Azure virtual machine (VM).

upvoted 1 times

  **gargaditya** 1 year, 6 months ago

Answer D is correct.

As per <https://learn.microsoft.com/en-us/azure/virtual-machines/resize-vm?tabs=portal>,

- After you create a virtual machine (VM), you can scale the VM up or down by changing the VM size.
- In some cases, you must deallocate(STOP) the VM first <NOT ALWAYS>. Deallocation may be necessary if the new size isn't available on the same hardware cluster that is currently hosting the VM.
- If the virtual machine is currently running, changing its size will cause it to restart.
- If your VM is still running and you don't see the size you want in the list, stopping the virtual machine may reveal more sizes.

In summary,here, a reboot will take place.

Temporary disk(usually D if not labeled as data disk) is wiped on a stop ; but it persists on a standard reboot.

<https://learn.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview#temporary-disk>

Hence, all of folder1, folder2, E drive and app remain intact on REBOOT.

Had there been a mention of state of app or user connection, that would NOT be maintained post reboot.



upvoted 2 times

  **PXAbstraction** 1 year, 7 months ago

**Selected Answer: A**

A is correct. D is for temp volumes in Azure defaults.

upvoted 3 times

  **Jacbin** 1 year, 7 months ago

**Selected Answer: D**



Resizing an Azure VM will not affect data on existing disks. Therefore, after resizing VM1, all of the following objects will be preserved:

D. Folder1, Folder2, App1 and volume E

Adding a new data disk and volume, as well as installing the App1 application on volume E, will not be affected by resizing the virtual machine. Only virtual machine settings, such as CPU and memory size, will be changed.

upvoted 1 times

🗲️ 👤 **afridi43** 1 year, 9 months ago

**Selected Answer: D**

Correct D. Folder1, Folder2, App1, and volume E

After resizing VM1, all the folders and data created within the virtual machine will still be present.

upvoted 1 times

🗲️ 👤 **PXAbstraction** 1 year, 10 months ago

**Selected Answer: D**

I understand the assumption that the D: drive is temporary but not every Azure VM SKU has a temp disk and the question doesn't mention one so I don't think it can be assumed.

upvoted 4 times

🗲️ 👤 **Returnerwesley** 2 years ago

Should be D since there isn't anything mention about temporary disk on the question

upvoted 3 times

🗲️ 👤 **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 3 times

🗲️ 👤 **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 1 times

You have an Azure virtual machine named VM1 that runs Windows Server and has the following configurations:

- ⇒ Size: D2s\_v4
- ⇒ Operating system disk: 127-GiB standard SSD
- ⇒ Data disk 128-GiB standard SSD
- ⇒ Virtual machine generation: Gen 2

You plan to perform the following changes to VM1:

- ⇒ Change the virtual machine size to D4s\_v4.
- ⇒ Detach the data disk.
- ⇒ Add a new standard SSD.

Which changes require downtime for VM1?

- A. Detaching the data disk only and adding a new standard SSD.
- B. Detaching the data disk only.
- C. Changing the virtual machine size only.
- D. Adding a new standard SSD only.

**Correct Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Scoff** Highly Voted 2 years, 8 months ago

**Selected Answer: C**

C - Changing the virtual machine size requires downtime

<https://docs.microsoft.com/en-us/azure/virtual-machines/resize-vm?tabs=portal>

upvoted 27 times

🗳️ 👤 **AS007** 2 years, 8 months ago

Correct

upvoted 4 times

🗳️ 👤 **HKEX388** 2 years, 6 months ago

Try it in test environment. When re-size the machine, VM in Azure will be restarted automatically.

upvoted 2 times

🗳️ 👤 **TheUltimateHac** Highly Voted 2 years, 8 months ago

**Selected Answer: C**

c is correct

upvoted 6 times

🗳️ 👤 **MichalGr** Most Recent 8 months, 2 weeks ago

Downtime required in Azure atm:

Resizing the VM

Changing the VM series or family

Adding or removing data disks

Changing virtual network (VNet) settings

Changing the OS disk size

Changing availability sets or availability zones

Changing encryption settings

Updating VM extensions

Changing certain VM settings

Redeploying the VM

Updating the VM's image or operating system



Performing maintenance tasks through Azure portal or PowerShell commands

Applying certain security configurations or patches

Migrating the VM to a different Azure region or subscription

Changing the VM's resource group

upvoted 3 times

  **MichalGr** 8 months, 2 weeks ago

not 4th from the top!

upvoted 1 times

  **Shailesh866** 1 year ago

**Selected Answer: C**

Answer is C. We can attach disks on the fly and doesn't require a downtime

upvoted 1 times

  **afridi43** 1 year, 3 months ago

**Selected Answer: C**

C. Changing the virtual machine size only.

Changing the virtual machine size (resizing) usually requires a VM restart,

Which results in downtime during the restart process.

So, changing the VM size does require downtime.

upvoted 1 times

  **syu31svc** 1 year, 9 months ago

**Selected Answer: C**

This is C for sure

upvoted 2 times

  **Skylark\_** 2 years, 4 months ago

**Selected Answer: C**

Answer is C

upvoted 2 times

  **Contactfornitish** 2 years, 4 months ago

**Selected Answer: C**

Had done the same two years back. Change of Size (plan) needs reboot so YES downtime applicable

upvoted 1 times



  **Nizhnoynovogorod** 2 years, 4 months ago

**Selected Answer: C**

Answer is C as Data Disks can be "hot" removed.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/detach-disk>

upvoted 1 times

  **airfrog** 2 years, 5 months ago

**Selected Answer: C**

C is correct. Resizing a VM will cause it reboot. You can add and remove data disks without rebooting.

upvoted 4 times

  **Zenax** 2 years, 7 months ago

**Selected Answer: C**

C definitely



upvoted 5 times

  **VinoTee** 2 years, 7 months ago

**Selected Answer: C**

I second this

upvoted 4 times

  **AS007** 2 years, 8 months ago

**Selected Answer: C**

C is correct

upvoted 6 times

## HOTSPOT -

You have a Windows Server container host named Server1 that has a single disk.

On Server1, you plan to start the containers shown in the following table.

Name	Description
Container1	Container1 is a Windows container that contains a web app in development. The container must <b>NOT</b> share a kernel with other containers.
Container2	Container2 is a Linux container that runs a web app. The container requires two static IP addresses.
Container3	Container3 is a Windows container that runs a database. The container requires a static IP address.

Which isolation mode can you use for each container? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Container1:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container2:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container3:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Correct Answer:

## Answer Area

Container1:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container2:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container3:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Reference:

<https://docs.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container>

 **darshanajayathilake** Highly Voted 2 years, 3 months ago

Answer should be

1-Hyper-v

2-hyper-v or process (we can install wsl and configure process isolation for linux containers , earlier wsl didn't support window 2019 or 2022 .

<https://learn.microsoft.com/en-us/windows/wsl/install-on-server>)

3-Hyper-v or process

upvoted 14 times

 **NazerRazer** 1 year, 8 months ago

The link you provided is not working anymore.

upvoted 2 times

 **Lu5ck** Highly Voted 2 years, 6 months ago

Container1: Hyper-V

Container2: Hyper-V

Container3: Hyper-V or Process

AFAIK, container running as process will utilize system's kernel. Obviously, linux cannot use window's kernel. Container, regardless of the mode, can have the capability to distribute multiple IP addresses, not just ports.

upvoted 13 times

 **mrmichael1389** 1 year, 11 months ago

You can use WSL in server 2022 to host Linux containers using process isolation mode.

upvoted 2 times

 **Mrcert82** Most Recent 2 months, 2 weeks ago

1.Hyper-V isolation only

2.Hyper-V isolation only

3.Hyper-V isolation only

Hyper-V Isolation: This isolation mode runs each container in a lightweight, highly optimized Hyper-V virtual machine. Each Hyper-V isolated container gets its own dedicated kernel, network stack, and resources. This allows you to configure network interfaces within the container's virtual

machine, including assigning multiple static IP addresses

Process Isolation Limitations: While process isolation provides resource and process separation for Windows containers, it shares the host's network stack. Assigning a dedicated static IP address directly to a process-isolated Windows container is not a standard or straightforward configuration. You would typically rely on port mapping to access the database service on the host's IP address and a specific port. This doesn't fulfill the requirement of the container itself having a dedicated static IP address.

upvoted 1 times

🗲️ 👤 **Ksk08** 8 months ago

Container1: Hyper-V isolation only

Container2: Hyper-V isolation only

Container3: Hyper-V isolation or process isolation

upvoted 3 times

🗲️ 👤 **Ksk08** 8 months, 1 week ago

Hyper-V isolation

Hyper-V isolation

Hyper-V or process

upvoted 1 times

🗲️ 👤 **AK\_1234** 1 year, 1 month ago

All the above answers are correct

- Hyper V

- Process

- Hyper V or Process isolation

upvoted 4 times

🗲️ 👤 **RickySmith** 1 year, 9 months ago

1 - <https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container#hyper-v-isolation>

3 - <https://ubuntu.com/tutorials/windows-ubuntu-hyperv-containers#7-run-an-ubuntu-container-on-hyperv>

3 - <https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container>

upvoted 2 times

🗲️ 👤 **afridi43** 1 year, 9 months ago

Container1: - Hyper-V isolation only

This is a Windows container that must NOT share a kernel with other containers.

To achieve this, you can use Hyper-V isolation.

Container2: - Process isolation only

This is a Linux container that requires two static IP addresses. In Windows Server, Linux containers cannot use Hyper-V isolation;

To achieve this, you can only use process isolation.

Container3: - Hyper-V isolation or process isolation

This is a Windows container that runs a database and requires a static IP address. For Windows containers, you can use either Hyper-V isolation or process isolation, and it depends on your specific requirements.

Since there are no specific constraints mentioned, you have the flexibility to choose either isolation mode.

upvoted 10 times

🗲️ 👤 **SDK76** 2 months, 1 week ago

However, Linux containers cannot run in process isolation mode on Windows. This is because process isolation relies on sharing the host's kernel, and Linux containers require a Linux kernel, which is not natively available on Windows.

upvoted 1 times

🗲️ 👤 **syu31svc** 2 years, 3 months ago

Containers 1 and 2 should use Hyper-V isolation

3 can use both

upvoted 6 times

🗲️ 👤 **wyindualizer** 2 years, 5 months ago

If running in Process isolation mode, you must run on the same type of kernel (OS) as the host; Hyper-V isolation mode provides more

flexibility when running non-Windows containers on Windows



hosts. so Container2: Hyper-V

upvoted 2 times

  **rimvydukas** 2 years, 9 months ago

As I can understand, Linux container must use Hyper-V isolation mode, not process isolation.

upvoted 3 times

  **Leocan** 2 years, 7 months ago

Process isolation - When running in this mode, containers share the same kernel with each other and with the host OS.

I don't think a Linux container can share the same kernel with the Windows host OS.

upvoted 4 times

  **lukiduc9625** 2 years, 9 months ago

In referenced document there is no information about what isolation type is possible for linux containers. Could anyone explain me (and give references) why linux container can use process isolation only? Some articles which I found in Internet suggests rather HyperV isolation only...

upvoted 3 times

  **Rel2002** 2 years, 9 months ago

Well in he link mentioned in the answer there is a sentence:

When running in this mode, containers share the same kernel with the host as well as each other. This is approximately the same as how Linux containers run.

upvoted 1 times

  **arsh807** 2 years, 6 months ago

That statement in the given reference link means that the Linux containers run the same as Windows containers, but it did not specify whether both the containers can run by sharing the same Kernel or not.

upvoted 3 times

  **Fakecon** 2 years ago

By Measure Up answer is same as provided here:

Hyper-V

Process

Hyper-V or Process

Reason for 3rd option being Hyper-V or Process is because of IP as it requires single IP and by that you can use both options as ideal.

2nd is not related to Linux but requirement for 2 IP addresses and for that reason process isolation is better option

upvoted 2 times

## DRAG DROP -

You have a server named Server1 that runs Windows Server and has the Hyper V server role installed. Server1 hosts a virtual machine named VM1.

Server1 has an NVMe storage device. The device is currently assigned to VM1 by using Discrete Device Assignment.

You need to make the device available to Server1.

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

Select and Place:

## Actions

From Server1, stop VM1.

From Server1, run the `Remove-VMAssignableDevice` cmdlet.

From Server1, run the `Mount-VMHostAssignableDevice` cmdlet.

From Server1, enable the device by using Device Manager.

From VM1, disable the device by using Device Manager.

## Answer Area



## Correct Answer:

## Actions

From VM1, disable the device by using Device Manager.

## Answer Area

From Server1, stop VM1.

From Server1, run the `Remove-VMAssignableDevice` cmdlet.

From Server1, run the `Mount-VMHostAssignableDevice` cmdlet.

From Server1, enable the device by using Device Manager.



## Reference:

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/deploying-storage-devices-using-dda>

**nazgul250** Highly Voted 3 years, 1 month ago

Correct.

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/deploying-graphics-devices-using-dda#removing-a-device-and-returning-it-to-the-host>

upvoted 16 times

**DavidThe2nd** Highly Voted 2 years ago

Stop

Remove

Mount

Enable

upvoted 5 times

**Ksk08** Most Recent 8 months ago



Correct order of actions:



From Server1, stop VM1.

From Server1, run the Remove-VMAssignableDevice cmdlet.

From Server1, run the Mount-VMHostAssignableDevice cmdlet.

From Server1, enable the device by using Device Manager.

upvoted 1 times

  **afриди43** 1 year, 9 months ago

1. From Server1, Stop VM1. (You need to stop VM1 to release the NVMe storage device from the virtual machine.)
2. From Server1, run the Remove-VMAssignableDevice cmdlet. (This step detaches the device from the virtual machine.)
3. From Server1, run the Mount-VMHostAssignableDevice cmdlet. (Now that the device is no longer assigned to VM1, This makes the NVMe storage device available to Server1.)
4. From Server1, enable the device by using Device Manager. (Once the device is attached to Server1, you should enable it in Device Manager to make it usable by the host server.)

upvoted 2 times

  **syu31svc** 2 years, 3 months ago

From the links given by nazgul250, Jawad1462 and alexandrasexy

If you want to return the device back to its original state, you will need to stop the VM and issue the following:

Copy

#Remove the device from the VM

Remove-VMAssignableDevice -LocationPath \$locationPath -VMName VMName



#Mount the device back in the host

Mount-VMHostAssignableDevice -LocationPath \$locationPath

You can then re-enable the device in device manager and the host operating system will be able to interact with the device again.

Answer is correct

upvoted 4 times

  **Jawad1462** 2 years, 8 months ago

Answer is Correct

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/deploying-graphics-devices-using-dda#removing-a-device-and-returning-it-to-the-host>

upvoted 3 times

  **alexandrasexy** 2 years, 11 months ago

The answer is Correct.

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/deploying-graphics-devices-using-dda#removing-a-device-and-returning-it-to-the-host>

upvoted 4 times

You have a server named Server1 that hosts Windows containers.

You plan to deploy an application that will have multiple containers. Each container will be on the same subnet. Each container requires a separate MAC address and IP address. Each container must be able to communicate by using its IP address.

You need to create a Docker network that supports the deployment of the application.

Which type of network should you create?

- A. NAT
- B. transparent
- C. I2bridge
- D. I2tunnel

**Correct Answer: B**

Community vote distribution

B (100%)

 **AvoKikinha** Highly Voted 3 years, 1 month ago

**Selected Answer: B**

Wrong

From: <https://docs.microsoft.com/en-us/virtualization/windowscontainers/container-networking/network-drivers-topologies>

transparent network driver

Containers attached to a network created with the 'transparent' driver will be directly connected to the physical network through an external Hyper-V switch. IPs from the physical network can be assigned statically (requires user-specified --subnet option) or dynamically using an external DHCP server.

L2bridge network driver

Containers attached to a network created with the 'I2bridge' driver will be connected to the physical network through an external Hyper-V switch. In I2bridge, container network traffic will have the same MAC address as the host due to Layer-2 address translation (MAC re-write) operation on ingress and egress. In datacenters, this helps alleviate the stress on switches having to learn MAC addresses of sometimes short-lived containers. L2bridge networks can be configured in 2 different ways

upvoted 14 times


 **AnonymousJhb** 2 years, 11 months ago

the question states "Each container requires a separate MAC address and IP address" thus I2bridge cannot be used since with I2bridge, "container network traffic will have the same MAC address as the host, due to Layer-2 address translation (MAC re-write) operation on ingress and egress. In datacenters, this helps alleviate the stress on switches having to learn MAC addresses of sometimes short-lived containers. Hence all the containers will have the same MAC addy. So L2bridge is out.

with I2bridge > this driver should only be used in a Microsoft Cloud Stack (Azure). The only difference over I2bridge is that all container traffic is sent to the virtualization host.

NAT is onl used for test/dev

upvoted 6 times

 **AvoKikinha** 3 years, 1 month ago

More info

Transparent Same Subnet: Bridged connection Routed through container host

L2Bridge Same Subnet: Bridged connection through Hyper-V virtual switch Cross Subnet: Container MAC address re-written on ingress and egress and routed Container MAC address re-written on ingress and egress

upvoted 3 times

 **Bojana** Highly Voted 3 years, 1 month ago

**Selected Answer: B**

transparent

upvoted 8 times

🗲️ 👤 **Ksk08** Most Recent 8 months, 1 week ago

Answer is B

upvoted 1 times

🗲️ 👤 **Joedn** 1 year, 1 month ago

Valid 05/28/2024

upvoted 2 times

🗲️ 👤 **fabilo** 1 year, 8 months ago

Selected Answer: B

B:Transparent

upvoted 2 times

🗲️ 👤 **afridi43** 1 year, 9 months ago

Selected Answer: B

B. transparent

To create a Docker network that allows each container to have a separate MAC address and IP address while being on the same subnet and able to communicate using their respective IP addresses, you should use the "transparent" network mode.

upvoted 2 times

🗲️ 👤 **syu31svc** 2 years, 3 months ago

Selected Answer: B

"supports the deployment of the application"

<https://learn.microsoft.com/en-us/virtualization/windowscontainers/container-networking/network-drivers-topologies>

Transparent Good for Developers or small deployments

Answer is B

upvoted 3 times

🗲️ 👤 **darshanajayathilake** 2 years, 3 months ago

Answer is transparent

<https://learn.microsoft.com/en-us/virtualization/windowscontainers/container-networking/network-drivers-topologies>

upvoted 1 times

🗲️ 👤 **arsh807** 2 years, 6 months ago

Option B, as MAC Address Spoofing is required in Transparent mode only.

upvoted 3 times

🗲️ 👤 **joehoesofat** 2 years, 8 months ago

Answer is C- the I2bridge is used for the most common Azure setups" kubernetes and SDN- the others are corner cases - would those corner cases be on an exam? i dont think so <https://learn.microsoft.com/en-us/virtualization/windowscontainers/container-networking/network-drivers-topologies>

upvoted 1 times

You have an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant. You plan deploy 100 new Azure virtual machines that will run Windows Server. You need to ensure that each new virtual machine is joined to the AD DS domain. What should you use?

- A. an Azure Resource Manager (ARM) template
- B. a Group Policy Object (GPO)
- C. Azure AD Connect
- D. an Azure management group

**Correct Answer: A**

Community vote distribution

A (100%)

  **syu31svc**  2 years, 3 months ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/join-windows-vm-template>

To automate the deployment and configuration of Azure virtual machines (VMs), you can use a Resource Manager template. These templates let you create consistent deployments each time. Extensions can also be included in templates to automatically configure a VM as part of the deployment. One useful extension joins VMs to a domain, which can be used with Azure Active Directory Domain Services (Azure AD DS) managed domains.




Answer is A

upvoted 8 times

  **edykss**  2 years, 9 months ago

Answer is correct


upvoted 5 times

  **Ksk08**  8 months ago

Correct Answer: A. Azure Resource Manager (ARM) template

Using an ARM template with the appropriate extensions (such as JsonAddDomainExtension) is the best way to ensure that your new Azure VMs are automatically joined to your on-premises AD DS domain during deployment. This approach allows you to automate and scale the process efficiently


upvoted 1 times

  **tomasek88** 1 year, 11 months ago

**Selected Answer: A**



A --> is correct and only make sense

upvoted 1 times

  **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 3 times

  **Rosviul** 2 years, 4 months ago

official article from MS:

<https://learn.microsoft.com/en-us/azure/active-directory-domain-services/join-windows-vm-template>

upvoted 5 times

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains three servers that run

Windows Server and have the Hyper-V server role installed. Each server has a Switch Embedded Teaming (SET) team.

You need to verify that Remote Direct Memory Access (RDMA) and all the required Windows Server settings are configured properly on each server to support an

Azure Stack HCI cluster.

What should you use?

- A. Server Manager
- B. the Get-NetAdapter cmdlet
- C. Failover Cluster Manager
- D. the Validate-DCB cmdlet

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **syu31svc** Highly Voted 2 years, 3 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/azure-stack/hci/deploy/validate>

After deploying a server cluster, run the Validate-DCB tool to test networking.


After updating a server cluster, depending on your scenario, run both validation options to troubleshoot cluster issues.

After setting up replication with Storage Replica, validate that the replication is proceeding normally by checking some specific events and running a couple commands.

After creating a server cluster, run the Validate-DCB tool before placing it into production.

D is correct

upvoted 5 times

 **empee1977** Highly Voted 2 years, 5 months ago

**Selected Answer: D**

D. the Validate-DCB cmdlet

You can use the Validate-DCB cmdlet to verify that Remote Direct Memory Access (RDMA) and all the required Windows Server settings are configured properly on each server to support an Azure Stack HCI cluster. The Validate-DCB cmdlet checks that the settings on the local computer are configured correctly for Data Center Bridging (DCB) and RDMA. This includes checking for the presence of the required software and hardware, such as the RDMA network adapter and the DCB feature, and verifying that the settings on the network adapter are configured correctly.

upvoted 5 times

 **Ksk08** Most Recent 8 months, 1 week ago

Answer is D

upvoted 1 times


 **PrettyFlyWifi** 1 year ago

Probably an out of date question now...

"Validate DCB is no longer the recommended tool to set up or test your host networking configuration on Azure Stack HCI. We recommend using Network ATC to configure your host networking set-up for Azure Stack HCI. Network ATC always supersedes Validate DCB on Azure Stack HCI." -

<https://learn.microsoft.com/en-us/azure-stack/hci/deploy/validate>

upvoted 2 times

 **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 2 times

🗨️ 👤 **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 4 times

🗨️ 👤 **phi3nix** 2 years, 2 months ago

If B would be "Get-NetAdapterRdma" the answer would be B.

I set up RDMA a few weeks ago; this is how you do it.

Get-NetAdapterRdma

Enable-NetAdapterRDMA

But I think that answer is D.

<https://learn.microsoft.com/en-us/azure-stack/hci/deploy/validate#install-and-run-the-validate-dcb-tool>

upvoted 2 times

🗨️ 👤 **Rosviul** 2 years, 4 months ago

<https://learn.microsoft.com/en-us/azure-stack/hci/deploy/validate#install-and-run-the-validate-dcb-tool>

upvoted 2 times

🗨️ 👤 **arsh807** 2 years, 6 months ago

<https://learn.microsoft.com/en-us/azure-stack/hci/deploy/validate>

upvoted 5 times

## HOTSPOT -

You plan to deploy an Azure virtual machine that will run Windows Server.

You need to ensure that an Azure Active Directory (Azure AD) user named user1@contoso.com can connect to the virtual machine by using the Azure Serial Console.

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

Configure on the Azure virtual machine:

	▼
Boot diagnostics with a custom storage account	
Operating system guest diagnostics	
A system-assigned managed identity	

Assign the following role to User1:

	▼
Virtual Machine Contributor	
Virtual Machine Administrator Login	
Virtual Machine User Login	

Correct Answer:

## Answer Area

Configure on the Azure virtual machine:

	▼
Boot diagnostics with a custom storage account	
Operating system guest diagnostics	
A system-assigned managed identity	

Assign the following role to User1:

	▼
Virtual Machine Contributor	
Virtual Machine Administrator Login	
Virtual Machine User Login	

Reference:

<https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/serial-console-overview>

 **sloky** Highly Voted 2 years, 8 months ago

Answer is correct:

<https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/serial-console-overview>

"Boot diagnostics must be enabled for the VM"


"The Azure account accessing Serial Console must have Virtual Machine Contributor role for both the VM and the boot diagnostics storage account"

upvoted 10 times

 **ppardav** Most Recent 1 month, 2 weeks ago

what if the question is related to connect to operative system and not to the machine. Shouldn't be the answers "boot diagnostic" & "administrator login"?

upvoted 1 times

 **Ksk08** 8 months, 1 week ago

answer is correct

upvoted 1 times

🗨️ 👤 **Ksk08** 8 months, 1 week ago

Answer is boot diagnostics and administrator login.

upvoted 2 times

🗨️ 👤 **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 4 times

🗨️ 👤 **syu31svc** 2 years, 3 months ago

Answer is correct

From link

Prerequisites to access the Azure Serial Console

To access the Serial Console on your VM or virtual machine scale set instance, you will need the following:

Boot diagnostics must be enabled for the VM

A user account that uses password authentication must exist within the VM. You can create a password-based user with the reset password function of the VM access extension. Select Reset password from the Help section.

The Azure account accessing Serial Console must have Virtual Machine Contributor role for both the VM and the boot diagnostics storage account

upvoted 3 times



## HOTSPOT -

You have a Windows Server container host named Server1 and an Azure subscription.

You deploy an Azure container registry named Registry1 to the subscription.

On Server1, you create a container image named image1.

You need to store image1 in Registry1.

Which command should you run on Server1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

	▼		▼	Registry1.Azurecr.io/image1
docker		export		
azcopy		import		
xcopy		pull		
git		push		

## Answer Area

Correct Answer:

	▼		▼	Registry1.Azurecr.io/image1
docker		export		
azcopy		import		
xcopy		pull		
git		push		

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-docker-cli?tabs=azure-cli#push-the-image-to-your-registry>

🗨️ **Burnie** Highly Voted 2 years, 7 months ago

Push the image to your registry

Now that you've tagged the image with the fully qualified path to your private registry, you can push it to the registry with docker push:

docker push myregistry.azurecr.io/samples/nginx

<https://learn.microsoft.com/en-us/azure/container-registry/container-registry-get-started-docker-cli?tabs=azure-cli#push-the-image-to-your-registry>  
upvoted 9 times

🗨️ **Ksk08** Most Recent 8 months, 1 week ago

Docker and push is correct

upvoted 1 times

🗨️ **afri43** 1 year, 9 months ago

Answer is correct

This command will push the image1 container image to the Azure Container Registry named Registry1.

docker push Registry1.Azurecr.io/image1

upvoted 2 times

🗨️ **syu31svc** 2 years, 3 months ago

Answer is correct

Docker push is the command to use  
upvoted 4 times

## HOTSPOT -

You plan to deploy an Azure virtual machine that will run Windows Server. The virtual machine will host an Active Directory Domain Services (AD DS) domain controller and a drive named F: on a new virtual disk.

You need to configure storage for the virtual machine. The solution must meet the following requirements:

- \* Maximize resiliency for AD DS.
- \* Prevent accidental data loss.

How should you configure the storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Volume for the AD DS database:

C
D
F

Caching configuration for the volume that hosts the database:

NONE
READ
READ/WRITE

## Correct Answer:

Volume for the AD DS database:

C
D
F

Caching configuration for the volume that hosts the database:

NONE
READ
READ/WRITE

Box 1: F -

Create a separate virtual data disk for storing the database, logs, and sysvol folder for Active Directory. Do not store these items on the same disk as the operating system.

Box 2: None -

By default, data disks that are attached to a VM use write-through caching. However, this form of caching can conflict with the requirements of AD DS. For this reason, set the Host Cache Preference setting on the data disk to None.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/adds-extend-domain>

 **Lu5ck** Highly Voted 2 years, 6 months ago

Correct.

<https://learn.microsoft.com/en-us/windows-server/administration/performance-tuning/role/active-directory-server/hardware-considerations>  
upvoted 8 times

 **Ksk08** Most Recent 8 months, 1 week ago

the answer is correct  
upvoted 1 times

 **SIAMIANJI** 1 year, 1 month ago

The answer is correct:

Create a separate virtual data disk for storing the database, logs, and sysvol folder for Active Directory. Don't store these items on the same disk as the operating system.

By default, data disks are attached to a VM using write-through caching. However, this form of caching can conflict with the requirements of AD DS. For this reason, set the Host Cache Preference setting on the data disk to None.

upvoted 2 times



  **lucacose** 1 year, 6 months ago

F: and none

By default, data disks are attached to a VM using write-through caching. However, this form of caching can conflict with the requirements of AD DS. For this reason, set the Host Cache Preference setting on the data disk to None.

<https://learn.microsoft.com/en-us/azure/architecture/example-scenario/identity/adds-extend-domain>

upvoted 3 times

  **Bolo92** 1 year, 7 months ago

valid 27.11.23

upvoted 2 times

  **leegend** 2 years, 1 month ago

Got this question 28-5-23

upvoted 3 times

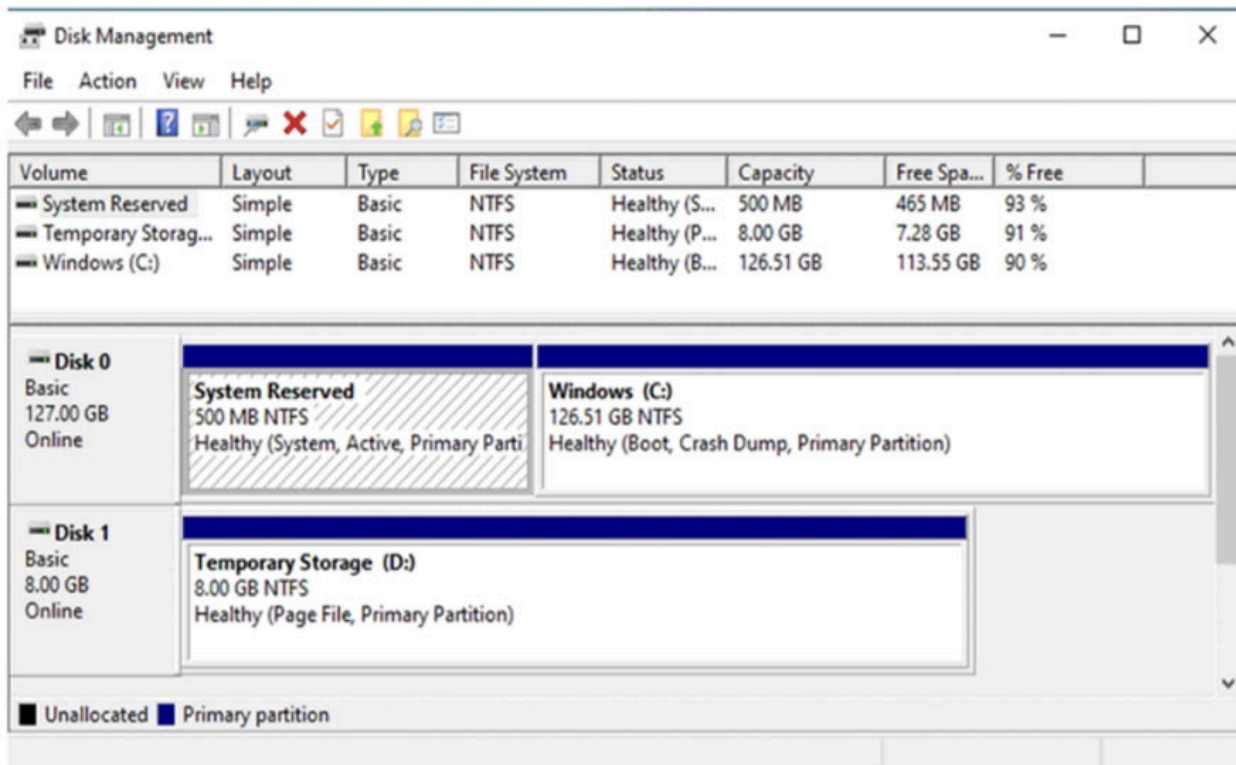
  **syu31svc** 2 years, 3 months ago

Answer is correct and link provided supports it

upvoted 3 times

## DRAG DROP -

You create an Azure virtual machine named Server1 that runs Windows Server.  
Server1 has the disk configurations shown in the following exhibit.



You need to create a new 100-GB volume on Server1.

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

Select and Place:

### Actions

Shut down Server1.

Initialize the disk.

Create a new simple volume.

Start Server1.

Create and attach a new data disk.

Create a new spanned volume.

### Answer Area



Correct Answer:

#### Actions

Shut down Server1.

Start Server1.

Create a new spanned volume.

#### Answer Area

Create and attach a new data disk.

Initialize the disk.

Create a new simple volume.

Step 1: Create and attach a new data disk

Add a data disk.

1. Sign in to the Azure portal.
2. Search for and select Virtual machines.
3. Select a virtual machine from the list.
4. On the Virtual machine pane, select Disks.
5. On the Disks pane, select Create and attach a new disk.
6. In the drop-downs for the new disk, make the selections you want, and name the disk.
7. Select Save to create and attach the new data disk to the VM.

Step 2: Initialize the disk -

Initialize a new data disk.

1. Connect to the VM.
2. Select the Windows Start menu inside the running VM and enter diskmgmt.msc in the search box. The Disk Management console opens.
3. Disk Management recognizes that you have a new, uninitialized disk and the Initialize Disk window appears.
4. Verify the new disk is selected and then select OK to initialize it.
5. The new disk appears as unallocated. Right-click anywhere on the disk and select New simple volume. The New Simple Volume Wizard window opens.
6. Etc.

Step 3: Create a new simple volume



Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/attach-managed-disk-portal>

 **sloky**  2 years, 2 months ago

Correct. You do not need to shut down/start a VM to add a new disk, and the question has not specified any special requirements to the volume so it uses the default simple volume. That leaves three answers.

upvoted 9 times

 **Jawad1462**  2 years, 2 months ago


Answer is Correct

upvoted 5 times

 **Joedn**  7 months ago

Valid 05/28/2024

upvoted 2 times

 **fabilo** 1 year, 2 months ago

right answer

upvoted 2 times

 **stormyR** 1 year, 7 months ago

Provided answer is correct

upvoted 3 times

🗨️ 👤 **syu31svc** 1 year, 9 months ago  
Provided answer is 100% correct  
upvoted 2 times

🗨️ 👤 **BryRob** 2 years ago  
Given Answer is correct  
upvoted 5 times

You have an Azure virtual machine named Server1 that runs a network management application. Server1 has the following network configurations:

- \* Network interface: Nic1
- \* IP address: 10.1.1.1/24
- \* Connected to: Vnet1/Subnet1

You need to connect Server1 to an additional subnet named Vnet1/Subnet2.

What should you do?

- A. Modify the IP configurations of Nic1.
- B. Add an IP configuration to Nic1.
- C. Add a network interface to Server1.
- D. Create a private endpoint on Subnet2.

**Correct Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Ksk08** 8 months ago

Answer is C

upvoted 1 times

🗳️ 👤 **Ksk08** 8 months, 1 week ago

I would say B

How to Connect Server1 to Another Subnet

What You Need to Do:

Add an IP Configuration to Nic1.

Why This Works:

Single Network Interface (NIC): Server1 has one NIC (Nic1). You can add more settings (IP configurations) to this NIC.

Multiple Subnets: By adding an IP configuration, you can give Nic1 an IP address from the new subnet (Subnet2). This lets Server1 talk to devices in that subnet.

Easier Management: It's simpler to manage one NIC with multiple IPs than to create a whole new NIC.

Why Not Add a New NIC?

Adding a new NIC means you have to stop the VM, create the new NIC, and connect it. That's more work and not necessary when you can just add an IP to the existing NIC.

upvoted 1 times

🗳️ 👤 **e489b39** 3 weeks, 4 days ago

Single NIC can only connect to one subnet

upvoted 1 times

🗳️ 👤 **004b54b** 10 months ago

**Selected Answer: C**

New NIC, because as highlighted by mohamed1999, adding a secondary IP configuration to the existing NIC won't be possible:

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-multiple-ip-addresses-portal>

Note

All IP configurations on a single NIC must be associated to the **\*\*same subnet\*\***.

If multiple IPs on different subnets are desired, multiple NICs on a VM can be used. To learn more about multiple NICs on a VM in Azure, see [Create VM with Multiple NICs](#).

upvoted 2 times

🗳️ 👤 **sardonique** 10 months, 3 weeks ago



correct, this one is a no brainer

upvoted 1 times

🗨️ 👤 **SIAMIANJI** 1 year, 1 month ago

**Selected Answer: C**

You need a new NIC.

upvoted 2 times

🗨️ 👤 **dfguss** 1 year, 2 months ago

Add a secondary IP configuration to the existing network interface (Nic1). This is the simplest and most efficient way to achieve connectivity in basic scenarios.

upvoted 1 times

🗨️ 👤 **004b54b** 10 months ago

As highlighted by mohamed1999, adding a secondary IP configuration to the existing NIC won't be possible:

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-multiple-ip-addresses-portal>

Note

All IP configurations on a single NIC must be associated to the **\*\*same subnet\*\***.

If multiple IPs on different subnets are desired, multiple NICs on a VM can be used. To learn more about multiple NICs on a VM in Azure, see [Create VM with Multiple NICs](#).

upvoted 2 times

🗨️ 👤 **mohamed1999** 1 year, 1 month ago

This will give you a second IP in the same subnet. This will not help you.

upvoted 2 times

🗨️ 👤 **MichalGr** 1 year, 2 months ago

I would say B.

upvoted 1 times

🗨️ 👤 **syu31svc** 2 years, 3 months ago

**Selected Answer: C**

A network interface (NIC) is the interconnection between a virtual machine and a virtual network. A virtual machine must have at least one NIC. A virtual machine can have more than one NIC, depending on the size of the VM you create. To learn about the number of NICs each virtual machine size supports, see [VM sizes](#).

You can create a VM with multiple NICs, and add or remove NICs through the lifecycle of a VM. Multiple NICs allow a VM to connect to different subnets.

C for correct

upvoted 3 times

🗨️ 👤 **MasterMani** 2 years, 9 months ago

**Selected Answer: C**

Correct Answer:C

<https://learn.microsoft.com/en-us/azure/virtual-network/network-overview>

upvoted 4 times

🗨️ 👤 **edykss** 2 years, 9 months ago

Answer is correct

upvoted 3 times

You have a server named Server1 that runs Windows Server 2019 and hosts a container named Container1. Container1 uses a Windows Server 2019 base image that was built by using a Docker file.

You upgrade Server1 to Windows Server 2022.

You need to ensure that Container1 will run on Server1. The solution must minimize administrative effort.

What should you do?

- A. Start Container1 in Hyper-V isolation mode.
- B. Modify the Docker file.
- C. Start Container1 in process isolation mode.
- D. Rebuild the base image for Container1.

**Correct Answer: A**

*Community vote distribution*

A (75%)

B (25%)

🗲️ 👤 **ppardav** 1 month, 2 weeks ago

**Selected Answer: B**

Why not B? <https://learn.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/upgrade-windows-containers>  
upvoted 1 times

🗲️ 👤 **Krayzr** 7 months ago

**Selected Answer: A**

HyperV isolation it is  
upvoted 1 times

🗲️ 👤 **Ni\_yot** 8 months ago

**Selected Answer: A**

Start in HyperV mode, the least admin effort.  
upvoted 2 times

🗲️ 👤 **Ksk08** 8 months, 1 week ago

Answer is A  
upvoted 1 times

## SIMULATION

-

You need to enable nested virtualization for a virtual machine named VM1 on SRV1.

To complete this task, sign in the required computer or computers.

### Configure Nested Virtualization

Step 1: While the virtual machine is in the OFF state, run the following command on the physical Hyper-V host, in this case on SRV1. This enables nested virtualization for the virtual machine.

Step 2: Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions \$true  
In our case: Set-VMProcessor -VMName VM1 -ExposeVirtualizationExtensions \$true

Step 3: Start the virtual machine.

Install Hyper-V within the virtual machine, just like you would for a physical server.  
Enable the Hyper-V role through Settings

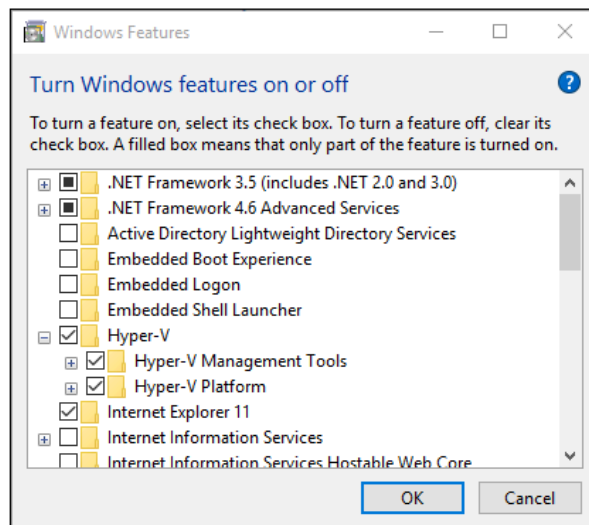
Step 4: Right click on the Windows button and select 'Apps and Features'.

Step 5: Select Programs and Features on the right under related settings.

Step 6: Select Turn Windows Features on or off.

Step 7: Select Hyper-V and click OK.

Correct Answer:



When the installation has completed you are prompted to restart your computer.

Reference: <https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization>  
<https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v>

Itkiller 5 months ago

It is correct, however, step 4 to 7 are not needed, you don't have the Set-VMProcessor command if Hyper-v role is not installed, the role needs to be installed first.

upvoted 2 times



Shuvankar\_roy 1 year ago

Powershell command in elevated mode.

-----

Set-VMProcessor -VMName [VMName] -ExposeVirtualizationExtensions \$true

upvoted 2 times

  **Goofer** 1 year, 4 months ago

<https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization>

upvoted 3 times

## SIMULATION

-

SRV1 contains a virtual machine named VM1.

You need attach c:\vhds\Disk1.vhdx to VM1. The solution must ensure that Disk1 can be expanded dynamically when VM1 runs.

To complete this task, sign in the required computer or computers.

**Correct Answer:**

Step 1: Sign in to the Azure portal.

Step 2: Search for and select Virtual machines. Select VM1 from the list..

Step 3: On the Virtual machine pane, select Disks.

Step 4: On the Disks pane, select Create and attach a new disk.

Step 5: In the drop-downs for the new disk, select attach c:\vhds\Disk1.vhdx

Step 6: Specify that the disk is managed.

Step 7: Select Save to create and attach the new data disk to the VM.

Reference: <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/attach-managed-disk-portal>

 **sa66ath**  9 months, 2 weeks ago

Open Hyper-V Manager on SRV1.

Select the virtual machine (VM1) to which you want to attach the virtual hard disk.

Right-click on the virtual machine and select "Settings" from the context menu.

In the left pane of the Settings window, select "SCSI Controller".

In the right pane, click "Add".

In the Add Hardware window, select "Hard Drive" and click "Add".

In the New Virtual Hard Disk Wizard, select "Use an existing virtual hard disk" and browse to c:\vhds\Disk1.vhdx.

Select "Dynamically expanding" as the disk type and click "Finish".

Click "OK" to save the changes and close the Settings window.


Start the virtual machine (VM1) and verify that Disk1 is available and can be expanded dynamically.

upvoted 22 times

 **jonards**  10 months, 3 weeks ago

Correct!

upvoted 2 times

 **sa66ath** 9 months, 2 weeks ago

It can't be correct as it seems to be Hyper-V, not Azure

upvoted 6 times

 **AliRi** 8 months, 1 week ago

Azure does not support .vhdx disks so Hyper-V console is correct way to do. Also in Azure disk needs to be fixed size, not dynamically expanded

upvoted 7 times

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Location
VNet1	Subnet11, Subnet12	West US
VNet2	Subnet21	West US
VNet3	Subnet31	Central US

You deploy a virtual machine named VM1 that runs Windows Server. VM1 is connected to Subnet11.

You plan to add an additional network interface named NIC1 to VM1.

To which subnets can NIC1 be attached?

- A. Subnet11 only
- B. Subnet12 only
- C. Subnet11 and Subnet12 only
- D. Subnet12 and Subnet21 only
- E. Subnet11, Subnet12, Subnet21, and Subnet31

**Correct Answer:** C

Community vote distribution

C (81%)

B (19%)

🗳️ **sa66ath** Highly Voted 2 years, 4 months ago

C: is correct, it is possible to attach many NICs to the same subnet so additional NIC to subnet11 is also possible.

upvoted 10 times

🗳️ **Kaiser10** Most Recent 3 days, 2 hours ago

**Selected Answer: C**

C is correct by <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/multiple-nics#create-a-vm-with-multiple-nics>

You can associate multiple NICs on a VM to multiple subnets, but those subnets must all reside in the same virtual network (vNet).

upvoted 1 times

🗳️ **PonbharathiMahalingam** 6 months ago

**Selected Answer: C**

Because questions is that "which subnets not a subnet " we can add

upvoted 1 times

🗳️ **Ksk08** 8 months, 1 week ago

C is correct answer

upvoted 1 times

🗳️ **sardonique** 10 months, 2 weeks ago

you should not attach 2 nics within the same subnet, try that in a physical switch you're going to have troubles.

upvoted 2 times

🗳️ **SIAMIANJI** 1 year, 2 months ago

**Selected Answer: C**

Subnet21 and Subnet31 do not belong to VNet1. Thank you for pointing that out! ☺

To clarify, NIC1 can only be attached to Subnet12 within VNet1.

upvoted 2 times

🗳️ **Kuikz** 1 year, 2 months ago

**Selected Answer: C**

C. Subnet11 and Subnet12 only

upvoted 2 times

🗨️ 👤 **PapaLion** 1 year, 5 months ago

the best practices say that do not make sense to have 2 NIC on an Azure VM connected to the same Subnet (Subnet11) , is better to configure multiple IP addresses on the same NIC instead....so for me the correct answer is the B only Subnet12.

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/multiple-nics>

upvoted 2 times

🗨️ 👤 **mohamed1999** 1 year, 1 month ago

but it says "CAN". you can attach to both 11 and 12

upvoted 2 times

🗨️ 👤 **RickySmith** 1 year, 6 months ago

**Selected Answer: C**

Can be connected to any non-Bastion\Gateway Subnet in the same vnet.

upvoted 2 times

🗨️ 👤 **Aliabdo** 1 year, 7 months ago

**Selected Answer: B**

Answer is correct.

you cant add second interface to the same subnet. VM cant be on other than one VNET.

upvoted 2 times

🗨️ 👤 **MattR2** 1 year ago

"you cant add second interface to the same subnet." yes you can. Should you? probably not. but you can do it.

upvoted 2 times

🗨️ 👤 **fabilo** 1 year, 8 months ago

**Selected Answer: C**

C: is the most obvious solution for me

upvoted 1 times

🗨️ 👤 **afridi43** 1 year, 9 months ago

**Selected Answer: C**

Correct Answer: C. Subnet11 and Subnet12 only

VM1 is connected to Subnet11 in VNet1.

When adding NIC1 to VM1, NIC1 can be attached to subnets within the same VNet as VM1 (VNet1) because VM1 is in VNet1.

So, NIC1 can be attached to:

C. Subnet11 and Subnet12 only

It cannot be attached to Subnet21 in VNet2 or Subnet31 in VNet3 directly, as they are in different VNets.

upvoted 4 times

🗨️ 👤 **Tiago\_MP** 1 year, 10 months ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/multiple-nics>

C!

upvoted 2 times

🗨️ 👤 **fran199** 2 years, 1 month ago

**Selected Answer: C**

C... correct answer

upvoted 4 times

🗨️ 👤 **phi3nix** 2 years, 1 month ago

One VM can be only in one VNET! This means that only the C option is valid. You can assign VNIC to both of the subnets.

upvoted 4 times

🗨️ 👤 **dan2dam** 2 years, 2 months ago

Note



All IP configurations on a single NIC must be associated to the same subnet. If multiple IPs on different subnets are desired, multiple NICs on a VM can be used. To learn more about multiple NICs on a VM in Azure, see [Create VM with Multiple NICs](#).

upvoted 1 times

 **syu31svc** 2 years, 3 months ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/multiple-nics>

You can associate multiple NICs on a VM to multiple subnets, but those subnets must all reside in the same virtual network (vNet)

Answer is C

upvoted 4 times

## DRAG DROP

-

You have an Azure subscription. The subscription contains a virtual machine named VM1 that runs Windows Server. VM1 contains a 128-GB operating system disk.

You need to increase the size of volume C on VM1 to 250 GB.

Which four actions should you perform in sequence.

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions		Answer Area
Redeploy VM1.		
Resize VM1.		
Start VM1.	➤	⬆
Resize the operating system disk.	⬅	⬇
Resize volume C.		
Stop VM1.		

## Correct Answer:

Answer Area
Stop VM1.
Resize the operating system disk.
Start VM1.
Resize volume C.

**syu31svc** Highly Voted 1 year, 9 months ago

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/expand-os-disk>

Refer to PowerShell segment

Answer is correct

upvoted 6 times

**SIAMIANJI** Most Recent 8 months ago

- 1) Stop VM1
- 2) Resize the operating system disk
- 3) Start VM1
- 4) Resize volume C:

upvoted 3 times

**Kuikz** 8 months, 4 weeks ago

Correct.

Expanding without downtime is only supported for data disks.

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/expand-os-disk>

upvoted 3 times

**fabilo** 1 year, 2 months ago

Right!!!

upvoted 1 times

**MR\_Eliot** 1 year, 3 months ago

Correct

upvoted 1 times

**SJHCI** 1 year, 10 months ago

Correct!

upvoted 2 times

You have an Azure subscription that contains a virtual machine named VM1 as shown in the following exhibit.

**VM1**  
Virtual machine

Connect ▾ ▶ Start ↺ Restart □ Stop 📦 Capture 🗑 Delete ↻ Refresh 📱 Open in mobile 📄 CLI / PS ...

⌵ **Essentials** JSON View

Resource group <a href="#">(move)</a> <a href="#">RG1</a>	Operating system Windows (Windows Server 2022 Datacenter Azure Edition)
Status Running	Size Standard D8s v3 (8 vcpus, 32 GiB memory)
Location East US (Zone 1)	Public IP address <a href="#">20.84.95.86</a>
Subscription <a href="#">(move)</a> <a href="#">Virtual Studio Enterprise Subscription</a>	Virtual network/subnet <a href="#">VNet1/Subnet2</a>
Subscription ID 7fef66e-8694-4b54-beae-17fd819d4873	DNS name <a href="#">Not configured</a>
Availability zone 1	
Tags <a href="#">(edit)</a> <a href="#">Click here to add tags</a>	

The subscription has the disks shown in the following table.

Name	Resource group	Location	Availability zone
Disk1	RG1	East US	None
Disk2	RG2	East US	1
Disk3	RG1	Central US	None
Disk4	RG1	Central US	1

Which disks can you attach as data disks to VM1?

- A. Disk2 only
- B. Disk4 only
- C. Disk1 and Disk2 only
- D. Disk2 and Disk4 only
- E. Disk1, Disk3, and Disk4 only
- F. Disk1, Disk2, Disk3, and Disk4

**Correct Answer: A**

Community vote distribution

A (52%) C (48%)

👤 **nap61** Highly Voted 1 year, 11 months ago

I have build the lab and allowed to attach only the disk in the same location + availability zone, so only disk 2, even in another RG.  
upvoted 26 times

👤 **fabilo** 1 year, 8 months ago

yeah it's true  
upvoted 2 times

👤 **e489b39** Most Recent 3 weeks, 4 days ago

**Selected Answer: C**

Non-Zonal doesn't mean you can't attach it's mean the Disk not assigned to specific zone so you can attach regionally to any zone within the region  
upvoted 1 times

🗳️ 👤 **Opoveda** 3 months, 1 week ago

**Selected Answer: C**

Disks Analysis:

Disk1: Located in East US, No availability zone, so it can be attached to VM1.

Disk2: Located in East US, Availability Zone 1, same as VM1, so it can be attached.

Disk3: Located in Central US, different region, so it cannot be attached.

Disk4: Located in Central US, different region, so it cannot be attached.

Conclusion:

The disks that can be attached as data disks to VM1 are Disk1 and Disk2.

Correct answer: C. Disk1 and Disk2 only.

upvoted 1 times

🗳️ 👤 **SDK76** 2 months, 1 week ago

A Disk that is not in an AZ, cannot be attached to a VM that is in an AZ zone. If so, this would defeat the reason for the VM being inside the AZ.

Disks must be in the same AZ as the VM they are attached too. Answer is A.

upvoted 1 times

🗳️ 👤 **Krayzr** 7 months, 1 week ago

**Selected Answer: C**

its C unfortunately

upvoted 1 times

🗳️ 👤 **004b54b** 10 months ago

**Selected Answer: A**

Can I attach a disk to a VM in another region?

No. All managed disks, even shared disks, must be in the same region as the VM they're attaching to.

(<https://learn.microsoft.com/en-us/azure/virtual-machines/faq-for-disks?tabs=azure-portal#can-i-attach-a-disk-to-a-vm-in-another-region->)

For VMs and disks distributed across multiple availability zones, the disks and their parent VMs are respectively collocated in the same zone, which prevents multiple VMs from going down even if an entire zone experiences an outage.

(<https://learn.microsoft.com/en-us/azure/virtual-machines/disks-high-availability#distribute-vms-and-disks-across-availability-zones>)

So for me the correct answer is A, as Disk 3 & Disk 4 are not in same region, and if Availability zone = None for Disk 1, it's not the same zone as the VM.

upvoted 1 times

🗳️ 👤 **TONPL\_Team** 1 year, 1 month ago

Disk 2 only can existing attach from RG2 so Correct answer: A , tested in Lab

upvoted 2 times

🗳️ 👤 **SIAMIANJI** 1 year, 1 month ago

**Selected Answer: C**

C is correct. Only they should be in the same region. Other parameters do not matter.

Disk 1 & Disk 2

upvoted 1 times

🗳️ 👤 **SDK76** 2 months, 1 week ago

All disks must be in the same AZ at the VM, otherwise it defeats the purpose of the AZ.

upvoted 1 times

🗳️ 👤 **Kuikz** 1 year, 2 months ago

**Selected Answer: A**

I also tested it and i can only choose the disk in the same availability zone.

Correct answer is A.

upvoted 4 times

🗳️ 👤 **jp01021234555** 1 year, 3 months ago

correct answer is A. tested in Lab

upvoted 3 times

🗲️ 👤 **Payday123** 1 year, 7 months ago

**Selected Answer: A**

If no zone is specified for the resource it can be placed in any availability zone and this means the disk can be in a different zone than Zone1

I vote for A

upvoted 2 times

🗲️ 👤 **infavolante** 1 year, 7 months ago

**Selected Answer: A**

A is the correct answer

upvoted 3 times

🗲️ 👤 **NazerRazer** 1 year, 8 months ago

**Selected Answer: C**

To attach data disks to VM1 in Azure, you need to consider the following factors:

The disks must be in the same location (East US, Zone 1 in this case) as the virtual machine to ensure low-latency access.

Azure Virtual Machines in availability zones can attach data disks that are located in the same availability zone or "None" availability zone.

Disk 1 is in the same location (East US), but it has "availability zone None," which is compatible with VM1's "availability zone 1." You can attach Disk 1 to VM1.

Disk 2 is in the same location (East US) and is in "availability zone 1," which is compatible with VM1's "availability zone 1." You can attach Disk 2 to VM1.

C. Disk1 and Disk2 only

upvoted 3 times

🗲️ 👤 **mossrin** 1 year, 10 months ago

**Selected Answer: A**

maybe A

upvoted 1 times

🗲️ 👤 **Joepelus** 1 year, 11 months ago

Going with B because of the availability zone.

upvoted 2 times

🗲️ 👤 **joesmith99** 2 years ago

**Selected Answer: C**

As long as the location is good you can attach

upvoted 3 times

## HOTSPOT

-

Your on-premises network contains a server named Server1 and uses an IP address space of 192.168.10.0/24.

You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 uses an IP address space of 192.168.10.0/24.

You need to migrate Server1 to Subnet1. You must use Azure Extended Network to maintain the existing IP address of Server1.

What is the minimum number of virtual machines that you should deploy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Virtual machines that run Windows Server 2022 Azure Edition:

	▼
0	
1	
2	

Virtual machines that run Windows Server 2019 or Windows Server 2022:

	▼
0	
1	
2	

**Answer Area**

Correct Answer:

Virtual machines that run Windows Server 2022 Azure Edition:

	▼
0	
1	
2	

Virtual machines that run Windows Server 2019 or Windows Server 2022:

	▼
0	
1	
2	

Maup33 Highly Voted 1 year, 12 months ago

you're 2 appliances, 1 prem, 1 azure

<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network>

upvoted 6 times

004b54b 10 months ago

More details, based on link provided by Maup33:

Extended network for Azure should only be used for machines that cannot have their IP address changed when migrating to Azure. It is always better to change the IP address and connect it to a subnet that wholly exists in Azure, if that is an option.

(<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network#overview>)

Extended network for Azure requires Windows Server 2022 Azure Edition for the VM that is running in Azure.

(<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network#configuration-in-azure>)

On-prem:

2. Create a Windows Server 2019 or 2022 VM on any hypervisor that supports nested virtualization.

(<https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network#on-premises-configuration>)

upvoted 1 times

Ksk08 Most Recent 8 months, 1 week ago

Answer is correct

upvoted 1 times

  **JimmyC** 1 year ago

This is correct, though the question is oddly ambiguous when it comes to Server1. Shouldn't you have to create a third VM for Server1 in the process of migrating it to Azure? Otherwise you haven't actually performed the task. But the question doesn't mention the server edition of Server1 at all, so none of the answers could be valid for it - I guess we are ignoring it.

upvoted 2 times

  **lucacose** 1 year, 7 months ago

2 NVA - Network Virtual Appliance:

- On prem: WinSrv 2019 or 2022

- Azure: WinSrv 2022 Azure Edition

upvoted 2 times

  **lucacose** 1 year, 9 months ago

Each subnet that you are going to extend requires one pair of appliances.

Extended network for Azure requires Windows Server 2022 Azure Edition for the VM that is running in Azure.

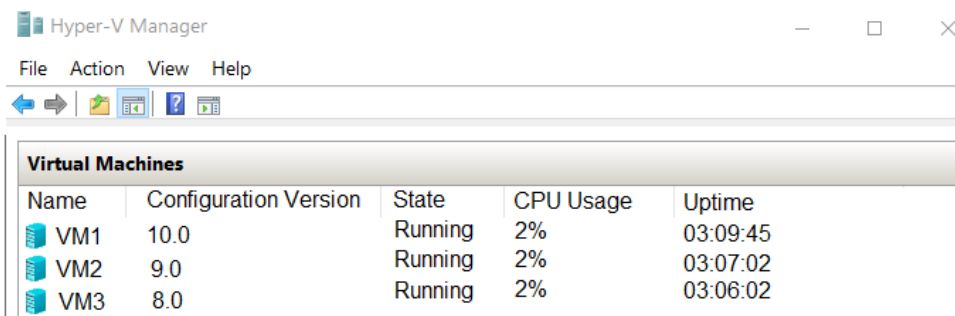
upvoted 2 times



## HOTSPOT

-

You have a server named Server1 that has the Hyper-V server role installed. Server1 hosts the virtual machines shown in the following exhibit.



Virtual Machines				
Name	Configuration Version	State	CPU Usage	Uptime
VM1	10.0	Running	2%	03:09:45
VM2	9.0	Running	2%	03:07:02
VM3	8.0	Running	2%	03:06:02

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.

**Answer Area**

[Answer choice] can have production checkpoints.

Only VM1  
Only VM1 and VM2  
VM1, VM2, and VM3

[Answer choice] can be hibernated.

Only VM1  
Only VM1 and VM2  
VM1, VM2, and VM3

**Answer Area**


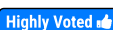
Correct Answer:

[Answer choice] can have production checkpoints.

Only VM1  
Only VM1 and VM2  
VM1, VM2, and VM3

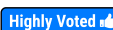
[Answer choice] can be hibernated.

Only VM1  
Only VM1 and VM2  
VM1, VM2, and VM3

 **ahenriquez02**  1 year, 12 months ago



<https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/upgrade-virtual-machine-version-in-hyper-v-on-windows-or-windows-server>

upvoted 5 times

 **skycrap**  2 years ago

Seems correct: Production checkpoints from server 2016 (c version 8.0), Hybernate from server 2019 (conf version 9)

upvoted 5 times

 **e489b39**  3 weeks, 4 days ago

Correct



upvoted 1 times

 **ppardav** 1 month, 2 weeks ago

It looks correct for hibernation [https://learn.microsoft.com/en-us/azure/virtual-machines/windows/hibernate-resume-windows?](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/hibernate-resume-windows?tabs=enableWithPortal%2CenableWithCLIXisting%2CPortalDoHiber%2CPortalStatCheck%2CPortalStartHiber%2CPortalImageGallery)

[tabs=enableWithPortal%2CenableWithCLIXisting%2CPortalDoHiber%2CPortalStatCheck%2CPortalStartHiber%2CPortalImageGallery](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/hibernate-resume-windows?tabs=enableWithPortal%2CenableWithCLIXisting%2CPortalDoHiber%2CPortalStatCheck%2CPortalStartHiber%2CPortalImageGallery)

upvoted 1 times

  **Ksk08** 8 months, 1 week ago

answer is correct

upvoted 1 times

  **MR\_Eliot** 1 year, 9 months ago

Correcto

upvoted 3 times

You have an Azure subscription. The subscription contains a virtual machine named VM1 that runs Windows Server.

You build an app named App1.

You need to configure continuous integration and continuous deployment (CI/CD) of App1 to VM1.

What should you create first?

- A. an App Service Environment
- B. an Azure DevOps organization
- C. a managed identity
- D. an Azure Automation account

**Correct Answer: B**

*Community vote distribution*

B (100%)

🗳️ 👤 **Ksk08** 8 months, 1 week ago

an Azure DevOps organization  
upvoted 1 times

🗳️ 👤 **Krayzr** 11 months, 3 weeks ago

**Selected Answer: B**

B. an Azure DevOps organization.

Azure DevOps provides developer services to support teams to plan work, collaborate on code development, and build and deploy applications. It includes Azure Pipelines, which is a CI/CD platform that can automate your build and deployment processes. Once you have an Azure DevOps organization and a project set up, you can create a pipeline for your app and configure it to deploy to your VM.

Please note that while the other options are also Azure services, they serve different purposes and are not the first thing you would need to set up for CI/CD in this scenario. An App Service Environment is a fully isolated and dedicated environment for running Azure App Service apps securely at high scale, a managed identity is a feature of Azure Active Directory, and an Azure Automation account is used to manage automation services including runbooks and configurations.

upvoted 2 times

🗳️ 👤 **JimmyC** 1 year ago

Important to note here that the app is being deployed to VM1. If the app was being hosted in an Azure App Service, it could handle CI/CD through other methods. But DevOps is the only option here that makes sense for a VM-hosted app.

upvoted 4 times

🗳️ 👤 **ahenriquez02** 1 year, 12 months ago

Azure DevOps (Visual Studio Team Services / Team Foundation Server) consists of a set of tools and services that help developers implement DevOps, Continuous Integration, and Continuous Deployment processes for their development projects.

upvoted 4 times

🗳️ 👤 **skycrap** 2 years ago

<https://learn.microsoft.com/en-us/sharepoint/dev/spfx/toolchain/implement-ci-cd-with-azure-devops>

upvoted 4 times

HOTSPOT

-

You have a Windows Server container host named Server1.

You start the containers on Server1 as shown in the following table.

Name	Image	Uses Hyper-V isolation	Process running on container
Container1	microsoft/iis	No	ProcessA
Container2	microsoft/iis	No	ProcessB
Container3	microsoft/iis	Yes	ProcessC
Container4	microsoft/iis	Yes	ProcessD

You need to validate the status of ProcessA and ProcessC.

Where can you verify that ProcessA and ProcessC are in a running state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

ProcessA:  ▼

- Container1 only
- Container1 and Container2 only
- Container1 and Server1 only
- Container1, Container2, and Server1 only
- All the containers and Server1

ProcessC:  ▼

- Container3 only
- Container3 and Container4 only
- Container3 and Server1 only
- Container3, Container4, and Server1 only
- All the containers and Server1

### Answer Area

Correct Answer:

ProcessA:  ▼

- Container1 only
- Container1 and Container2 only
- Container1 and Server1 only
- Container1, Container2, and Server1 only
- All the containers and Server1

ProcessC:  ▼

- Container3 only
- Container3 and Container4 only
- Container3 and Server1 only
- Container3, Container4, and Server1 only
- All the containers and Server1

 smith288  1 year, 11 months ago

Incorrect.

ProcessA is in a container that has process isolation. So, both Container1 and the host (Server1) can see the process. Per this article "When you have a Windows container running in process isolation mode, all processes are isolated between the containers so they have no influence on each other. However, the security boundary between container host and containers is simply the process isolation itself, which means the container host has visibility into the processes running inside the container." <https://argonsys.com/microsoft-cloud/library/how-to-identify-processes-running-inside-a>

windows-container-from-the-container-host/

ProcessC is in a hyper-V isolation container in contrast, so only Container3 can see the process.

So, Container1 and Server1 only for the first answer. Container3 only for the second one.

upvoted 31 times

  **MichalGr** 1 year, 2 months ago

All fine apart from the beginning "ProcessA is in a container that has process isolation." - not according to the table.

upvoted 2 times

  **sardonique** 10 months, 2 weeks ago



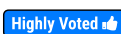
you have 2 types of isolation: Process isolation and Kernel isolation. so ProcessA has definitely process isolation. Smith288 knows what he's talking about, you don't

upvoted 3 times

  **Ksk08** 8 months, 2 weeks ago

correct

upvoted 1 times

  **JackBauer**  1 year, 8 months ago

I would say ProcessA : Container 1, Container 2 and Server1 only. 1 and 2 are not using HyperV isolation so they can talk to each other, and the host can see them too. 3 and 4 are in hyper-v isolation so they cannot see anything outside of themselves.

Process C is in hyperV isolation, so only itself can check processes. Even the host cannot. So Container3 only for the second box

This question does not ask about process isolation, which would make the answers different.

upvoted 12 times

  **004b54b** 10 months ago

I did believe as you, but i was wrong:

What gets isolated:

Windows containers virtualize access to various operating system namespaces. A namespace provides access to information, objects, or resources via a name. For example, the file system is probably the best-known namespace. There are numerous namespaces on Windows that get isolated on a per-container basis:

- file system
- registry
- network ports
- \*\*process\*\* and thread ID \*\*space\*\*
- Object Manager namespace

(<https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container#what-gets-isolated>)


Then, smith288 is right: both Container1 and the host (Server1) can see the process.

upvoted 1 times

  **Jothar**  7 months, 2 weeks ago

This seems to support smith288: <https://techcommunity.microsoft.com/blog/itopstalkblog/how-to-identify-processes-running-inside-a-windows-container-from-the-container-/3453297>

upvoted 1 times

  **Ksk08** 8 months, 1 week ago

ProcessA: Container1 and Server1 only

ProcessC: Container3 only

upvoted 4 times

HOTSPOT

-

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2022 Datacenter: Azure Edition
VM2	Windows Server 2022 Datacenter: Azure Edition Core
VM3	Windows Server 2022 Datacenter
VM4	Windows Server 2019 Datacenter

You plan to implement Azure Automanage for Windows Server.

You need to identify the operating system prerequisites.

Which virtual machines support Hotpatch, and which virtual machines support SMB over QUIC? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Hotpatch:

- VM1 only
- VM2 only
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

SMB over QUIC:

- VM1 only
- VM2 only
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

**Answer Area**

Hotpatch:

- VM1 only
- VM2 only**
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

**Correct Answer:**

SMB over QUIC:

- VM1 only**
- VM2 only
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

 **Kuikz** Highly Voted 1 year, 2 months ago

Hotpatch: VM1 and VM2

SMB over QUIC: VM1 and VM2


upvoted 9 times

 **Ksk08** Most Recent 8 months, 1 week ago

Hotpatch: VM1, VM2,

SMB over QUIC: VM1, VM2,

upvoted 3 times

  **andib126** 11 months, 2 weeks ago

<https://learn.microsoft.com/en-us/windows-server/get-started/editions-comparison-windows-server-2022?tabs=full-comparison>

VM1 and VM2 for both

upvoted 3 times

  **004b54b** 10 months ago

According to your link, all versions of Win Server 2022 support Hotpatch, but not Win Serv 2019, so first answer is VM1 + VM2 + VM3

Only Win Serv 2022 Datacenter Azure edition supports SMB over QUIC, so only VM1 + VM2 for the second answer

upvoted 1 times

  **rknichols01** 1 year, 5 months ago

sorry, did not post the hot patch support list.

Hotpatch is supported only on VMs and Azure Stack HCI created from images with the exact combination of publisher, offer and sku from the below OS images list. Windows Server container base images or Custom images or any other publisher, offer, sku combinations aren't supported.

Publisher OS Offer Sku

MicrosoftWindowsServer WindowsServer 2022-Datacenter-Azure-Edition-Core

MicrosoftWindowsServer WindowsServer 2022-Datacenter-Azure-Edition-Core-smalldisk

MicrosoftWindowsServer WindowsServer 2022-Datacenter-Azure-Edition-Hotpatch

MicrosoftWindowsServer WindowsServer 2022-Datacenter-Azure-Edition-Hotpatch-smalldisk

<https://learn.microsoft.com/en-us/windows-server/get-started/hotpatch>

upvoted 1 times

  **rknichols01** 1 year, 5 months ago

the answers are correct.

Automanage supports the following Windows versions:

Windows Server 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

Windows Server 2022 Azure Edition

Windows 10

<https://learn.microsoft.com/en-us/azure/automanage/automanage-windows-server>

Create an Azure VM with the Windows Server 2022 Datacenter: Azure Edition image to get the Automanage for Windows Server capabilities, including SMB over QUIC.

<https://learn.microsoft.com/en-us/azure/automanage/automanage-smb-over-quic>

upvoted 1 times

  **MR\_Eliot** 1 year, 9 months ago

Hotpatch:

<https://learn.microsoft.com/en-us/windows-server/get-started/hotpatch>

Supported platforms

Hotpatch is supported on the following operating systems for VMs running on Azure and Azure Stack HCI:

Windows Server 2022 Datacenter: Azure Edition Core

Windows Server 2022 Datacenter: Azure Edition with Desktop Experience

SMB over QUIC:

<https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-over-quic>

Prerequisites

To use SMB over QUIC, you need the following things:



-A file server running Windows Server 2022 Datacenter: Azure Edition (Microsoft Server Operating Systems)

-A Windows 11 computer (Windows for business)

Windows Admin Center (Homepage)

A Public Key Infrastructure to issue certificates like Active Directory Certificate Server or access to a trusted third party certificate issuer like Verisign, Digicert, Let's Encrypt, and so on.

upvoted 4 times

  **MR\_Eliot** 1 year, 9 months ago

Windows Server 2022 is the latest Long-Term Servicing Channel (LTSC) release with five years of mainstream support + five years of extended support. Choose the image that is right for your application needs.

- Server with Desktop Experience includes all roles and a graphical user interface (GUI).

Server Core omits the GUI for a smaller OS footprint.

- Azure Edition with Desktop Experience- includes additional new functionality such as >>Hotpatch, SMB over QUIC<<, extended network for Azure, and is optimized to run in Azure.

- Azure Edition Core - includes additional new functionality such as >>Hotpatch, SMB over QUIC<<, extended network for Azure, and is optimized to run in Azure.

So answer is "VM1" & "VM2" for both instances.

upvoted 9 times

  **ARZIMMADAR** 1 year, 6 months ago

so what would the answer be?

upvoted 1 times

  **AndsSkov** 1 year, 9 months ago

Hotpatch should be VM1 and VM2: <https://learn.microsoft.com/en-us/windows-server/get-started/hotpatch#:~:text=Windows%20Server%202022,with%20Desktop%20Experience>

SMB over QUIC is correct

upvoted 2 times

  **c7d45f4** 1 year, 9 months ago

i think you are right as shown here as well <https://learn.microsoft.com/en-us/windows-server/get-started/editions-comparison-windows-server-2022?tabs=version-differences>

upvoted 1 times

  **c7d45f4** 1 year, 9 months ago

edit SMB over QUIC applies to vm1 and vm2 as well

upvoted 2 times



## HOTSPOT

-

You have an Azure subscription that contains a virtual network named VNet1. Vnet1 contains three subnets named Subnet1, Subnet2, and Subnet3.

You deploy a virtual machine that has the following settings:

- Name: VM1
- Subnet: Subnet2
- Network interface name: NIC1
- Operating system: Windows Server 2022

You need to ensure that VM1 can route traffic between Subnet1 and Subnet3. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

From the Azure portal:

Associate a routing table with Subnet2.  
Attach two additional interfaces to VM1.  
Enable IP forwarding for NIC1.

On VM1:

Install and configure a network controller.  
Install and configure Routing and Remote Access.  
Run the route add command.

Correct Answer:

### Answer Area

From the Azure portal:

Associate a routing table with Subnet2.  
Attach two additional interfaces to VM1.  
Enable IP forwarding for NIC1.

On VM1:

Install and configure a network controller.  
Install and configure Routing and Remote Access.  
Run the route add command.

 **Ksk08** 8 months, 1 week ago

To ensure that VM1 can route traffic between Subnet1 and Subnet3 with minimal administrative effort, follow these steps:

From the Azure portal:



Enable IP forwarding for NIC1.

On VM1:

Install and configure Routing and Remote Access.

These actions will allow VM1 to act as a router between the subnets. Enabling IP forwarding allows the VM to forward traffic, and configuring Routing and Remote Access sets up the necessary routing functionality.

upvoted 1 times

  **Ksk08** 7 months, 1 week ago

Sorry, provided answer should be correct



upvoted 1 times

  **nap61** 1 year ago

Answers are correct!

<https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal>

upvoted 3 times

  **Kuikz** 1 year, 2 months ago

Box 1: It has to be IP forwarding for NIC1 because a routing table would be assigned to subnet 1 and 3. Here I only have the option to assign it to subnet 2.

Box 2: with the step "run the route add command" they assume there is already a routing table and you are adding a route to the table.

upvoted 4 times

  **MR\_Eliot** 1 year, 9 months ago

DYOR, answer seems correct:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface?tabs=azure-portal>

upvoted 2 times

## HOTSPOT

-

## Case Study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

## To start the case study

-

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

## Overview

-

## Company Information

-

ADatum Corporation is a manufacturing company that has a main office in Seattle and two branch offices in Los Angeles and Montreal.

## Fabrikam Partnership

-

ADatum recently partnered with 2 company named Fabrikam, Inc.

Fabrikam is a manufacturing company that has a main office in Boston and a branch office in Orlando.

Both companies intend to collaborate on several joint projects.

## Existing Environment

-

## ADatum AD DS Environment

-

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

The forest contains two domains named adatum.com and east.adatum.com and the domain controllers shown in the following table.

Name	Domain	Operations master roles
DC1	adatum.com	Schema master
DC2	adatum.com	None
DC3	east.adatum.com	PDC emulator, RID master

Fabrikam AD DS Environment

-

The on-premises network of Fabrikam contains an AD DS forest named fabrikam.com.

The forest contains two domains named fabrikam.com and south.fabrikam.com.

The fabrikam.com domain contains an organizational unit (OU) named Marketing.

Server Infrastructure

-

The adatum.com domain contains the servers shown in the following table.

Name	Role
HyperV1	Hyper-V
SSPace1	File and Storage Services

HyperV1 contains the virtual machines shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2022 Datacenter	Joined to the adatum.com domain Contains a file share named Data1 and a local user named User1
VM2	Red Hat Enterprise Linux (RHEL)	Contains a local user named User2
VM3	Windows Server 2022 Standard	Joined to the adatum.com domain Has the File and Storage Services role installed

All the virtual machines on HyperV1 have only the default management tools installed.

SSPace1 contains the Storage Spaces virtual disks shown in the following table.

Name	Number of physical disks	Redundancy
Disk1	8	Three-way mirror
Disk2	12	Parity

Azure Resources

-

ADatum has an Azure subscription that contains an Azure AD tenant. Azure AD Connect is configured to sync the adatum.com forest with Azure AD.

The subscription contains the virtual networks shown in the following table.

Name	Location	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	West US	SubnetA, SubnetB

The subscription contains the Azure Private DNS zones shown in the following table.

Name	Virtual network link
Zone1.com	VNet1
Zone2.com	VNet2
Zone3.com	None

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Security type
Server1	Windows Server 2022 Datacenter: Azure Edition	Trusted launch
Server2	Windows Server 2022 Datacenter: Azure Edition	Standard
Server3	Windows Server 2022 Datacenter	Standard
Server4	Windows Server 2019 Datacenter	Trusted launch

All the servers are in a workgroup.

The subscription contains a storage account named storage1 that has a file share named share1.

#### Requirements

-

#### Planned Changes

-

ADatum plans to implement the following changes:

- Sync Data1 to share1.
- Configure an Azure runbook named Task1.
- Enable Azure AD users to sign in to Server1.
- Create an Azure DNS Private Resolver that has the following configurations:
  - Name: Private1
  - Region: West US
  - Virtual network: VNet1
  - Inbound endpoint: SubnetB
- Enable users in the adatum.com domain to access the resources in the south.fabrikam.com domain.

#### Technical Requirements

-

ADatum identifies the following technical requirements:

- The data on SSPace1 must be available always.
- DC2 must become the schema master if DC1 fails.
- VM3 must be configured to enable per-folder quotas.
- Trusts must allow access to only the required resources.
- The users in the Marketing OU must have access to storage1.
- Azure Automanage must be used on all supported Azure virtual machines.
- A direct SSH session must be used to manage all the supported virtual machines on HyperV1.

You need to meet technical requirements for HyperV1.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

<div>▼</div> <div>Connect-PSession Connect-WSMan hvc.exe mstsc.exe</div>	ssh	<div>▼</div> <div>User1@VM1 User1@VM2 User2@VM2 VM1</div>
--	-----	---

Correct Answer:

### Answer Area

<div>▼</div> <div>Connect-PSession Connect-WSMan <b>hvc.exe</b> mstsc.exe</div>	ssh	<div>▼</div> <div>User1@VM1 User1@VM2 <b>User2@VM2</b> VM1</div>
---	-----	--

**Payday123** Highly Voted 1 year, 7 months ago

Correct

By default only Linux has SSH enabled

upvoted 5 times

**espek** Highly Voted 1 year, 7 months ago

Correct.

here the explanation:

-> <https://www.thomasmaurer.ch/2018/04/hvc-ssh-direct-for-linux-vm-on-hyper-v/>

upvoted 5 times

**HardeWerker433** Most Recent 3 months, 1 week ago

I am so confused, why connect to that machine specifically!?

upvoted 1 times

**Ksk08** 8 months ago

Answer correct

The correct selections would be:

For Connection Type: hvc.exe

This is the Hyper-V Virtual Machine Connection tool

Used for SSH connections to virtual machines

For SSH: User2@VM2

User2 is the local user created on VM2

VM2 is the Linux machine that natively supports SSH

The format User2@VM2 is the correct SSH connection string format

upvoted 1 times

## HOTSPOT

-

You have an Azure subscription and a computer named Computer1 that runs Windows 11.

From the Azure portal, you deploy a virtual machine named VM1 that runs Windows Server. You configure VM1 to use the default settings.

You need to ensure that you can connect to VM1 by using PowerShell remoting.

Which cmdlet should you run, and what should you use to run the cmdlet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Run from:   
A PowerShell session on Computer1  
A PowerShell session on VM1  
Azure Cloud Shell


Cmdlet:   
Enable-AzVMPSRemoting  
Enable-PSRemoting -Force  
Enable-PSSessionConfiguration

**Answer Area**

Correct Answer:

Run from:   
A PowerShell session on Computer1  
A PowerShell session on VM1  
Azure Cloud Shell

Cmdlet:   
Enable-AzVMPSRemoting  
Enable-PSRemoting -Force  
Enable-PSSessionConfiguration

 **rknichols01** Highly Voted 1 year, 5 months ago

Azure Cloud Shell

Enable-AzVMPSRemoting.

<https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-connecting-to-vms-with-azure-psremoting/ba-p/428403>

upvoted 5 times

 **formacaotismic** Most Recent 7 months, 2 weeks ago

Forma de garantir que se pode conectar à VM1 usando PowerShell remoting é utilizando o Azure Cloud Shell com o comando Enable-AzVMPSRemoting.

Run from: Azure Cloud Shell

Cmdlet: Enable-AzVMPSRemoting

Essa abordagem é prática, especialmente porque o Azure Cloud Shell já vem com os módulos necessários pré-instalados, facilitando a execução do comando sem configurações adicionais.

upvoted 1 times

 **Ksk08** 8 months ago

Run from: Azure Cloud Shell.

Cmdlet: Enable-AzVMPSRemoting.

upvoted 1 times

🗨️ 👤 **Ksk08** 8 months, 1 week ago

Set-VMProcessor VM1 -ExposeVirtualizationExtensions \$true

upvoted 1 times

🗨️ 👤 **Ksk08** 8 months, 1 week ago

Sorry please delete, accidentally paste here

upvoted 1 times

🗨️ 👤 **Kuikz** 1 year, 2 months ago

Box 1: Azure Cloud Shell

Box 2: Enable-AzVMPSRemoting

There is no command Enable-PSRemoting in Cloud Shell. This command is local to Windows and is needed only on non server Windows

upvoted 4 times

🗨️ 👤 **RickySmith** 1 year, 6 months ago

Azure Cloud Shell - <https://learn.microsoft.com/en-us/azure/cloud-shell/overview> (Azure Cloud shell allows you to options of Bash and powershell.)

Enable-AZVMPSRemoting - <https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-connecting-to-vms-with-azure-psremoting/ba-p/428403>

upvoted 4 times

🗨️ 👤 **Payday123** 1 year, 7 months ago

Enable-AzVMPSRemoting is a part of PSCloudShellUtility module

Description says:

"Enable all aspects of PowerShell remoting on the given target (NSG Rules, Target WinRM/SSH configs"

upvoted 1 times

🗨️ 👤 **NazerRazer** 1 year, 8 months ago

Run from: Azure Cloud Shell

Cmdlet: Enable-PSRemoting -Force

Here's the explanation:

Run from Azure Cloud Shell: You typically run configuration commands like this from an environment that has access to your Azure resources. Azure Cloud Shell is a web-based shell environment that is directly connected to your Azure subscription, making it a suitable place to configure Azure VMs.

Cmdlet: Enable-PSRemoting -Force: This PowerShell cmdlet enables PowerShell remoting on a Windows machine, allowing you to use PowerShell remoting to connect to the VM from another machine (in this case, Computer1). The -Force flag is used to ensure that remoting is enabled even if it's disabled by default.

upvoted 4 times

🗨️ 👤 **Payday123** 1 year, 7 months ago

There is no command Enable-PSRemoting in Cloud Shell. This command is local to Windows and is needed only on non server Windows

upvoted 2 times

🗨️ 👤 **argjend** 1 year, 8 months ago

So I think is

Run from: A powershell session on VM1

Cmdlet: Enable-PsRemoting -Force

Because windows11 have powershell but not azure powershell libraries (wich means you can use enter-ssession and not enter-azvm)

And you can't use the command enable-azvmpsremoting from vm1 (this command is used on cloud shell)

This link may interest you: <https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-connecting-to-vms-with-azure-psremoting/ba-p/428403>

(I am telling you my opinion, don't take my answer as right without having made your considerations please)

upvoted 2 times

🗨️ 👤 **Payday123** 1 year, 7 months ago

PSRemoting is enabled by default on Windows Server. No need to enable it

upvoted 1 times



  **FM221228** 1 year, 9 months ago

Wrong! Since computer 1 runs a default Windows 11, Azure PowerShell is not installed. You must use the Cloud Shell.

upvoted 3 times

## HOTSPOT

-

You have a server named Server1 that runs Windows Server and has the Hyper-V server role installed. Server1 contains a virtual machine named VM1 that runs Windows Server.

You need to install the Hyper-V server role on VM1.

Which PowerShell command should you run first? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Set-VM VM1 Set-VMFirmware VM1 Set-VMHost Server1 Set-VMProcessor VM1 Set-VMSecurity VM1	-EnableEnhancedSessionMode -EnableHostResourceProtection -ExposeVirtualizationExtensions -CompatibilityForOlderOperatingSystemsEnabled	\$true
---	---	--------

## Correct Answer:

## Answer Area

Set-VM VM1 Set-VMFirmware VM1 <b>Set-VMHost Server1</b> Set-VMProcessor VM1 Set-VMSecurity VM1	<b>-EnableEnhancedSessionMode</b> -EnableHostResourceProtection -ExposeVirtualizationExtensions -CompatibilityForOlderOperatingSystemsEnabled	\$true
--	--	--------

**windowsmodulesinstallerworker** Highly Voted 1 year, 9 months ago  
 Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions \$true  
 upvoted 35 times

**Ksk08** 8 months ago  
 Set-VMProcessor VM1 -ExposeVirtualizationExtensions \$true  
 upvoted 1 times

**e489b39** 3 weeks, 3 days ago  
 what's wrong with you man keep using AI only and keep posting stringer posts ?  
 upvoted 1 times

**boapaulo** Highly Voted 1 year, 6 months ago  
 Admin, the correct answer is the one given below, please change it in the screenshot of the answer.  
 - Set-VMProcessor VM1  
 -ExposeVirtualizationExtensions \$true  
 upvoted 6 times

**sardonique** 10 months, 2 weeks ago  
 Admin please do not correct. If all the answers are perfect this will lower the value of the exam and will provoke Microsoft to react. People make at least the effort to search the knowledge base and look at the comments  
 upvoted 2 times

**Ksk08** Most Recent 8 months, 1 week ago  
 Set-VMProcessor VM1 -ExposeVirtualizationExtensions \$true  
 upvoted 1 times

**NazerRazer** 1 year, 8 months ago  
 Configure Nested Virtualization  
 Step 1: While the virtual machine is in the OFF state, run the following command on the

physical Hyper-V host, in this case on SRV1. This enables nested virtualization for the virtual machine.

Step 2: Set-VMProcessor - VMName <VMName> -ExposeVirtualizationExtensions \$true

In our case: Set-VMProcessor -VMName VM1 -ExposeVirtualizationExtensions \$true

Step 3: Start the virtual machine.

Install Hyper-V within the virtual machine, just like you would for a physical server.

Enable the Hyper-V role through Settings

Step 4: Right click on the Windows button and select 'Apps and Features'.

Step 5: Select Programs and Features on the right under related settings.

Step 6: Select Turn Windows Features on or off.

Step 7: Select Hyper-V and click OK.

upvoted 5 times

  **RickySmith** 1 year, 6 months ago

<https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/enable-nested-virtualization>

upvoted 2 times

HOTSPOT

-

You have a Windows Server 2022 container host named Host1 and a container registry that contains the container images shown in the following table.

Name	Container base image OS version
Image1	Windows Server 2022
Image2	Windows Server 2019

You need to run the containers on Host1.

Which isolation mode can you use for each image? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Image1:  ▼  
Hyper-V isolation only  
Process isolation only  
Hyper-V isolation or process isolation

Image2:  ▼  
Hyper-V isolation only  
Process isolation only  
Hyper-V isolation or process isolation

**Answer Area**

Correct Answer:

Image1:  ▼  
Hyper-V isolation only  
Process isolation only  
Hyper-V isolation or process isolation

Image2:  ▼  
Hyper-V isolation only  
Process isolation only  
Hyper-V isolation or process isolation

**Payday123** Highly Voted 1 year, 7 months ago

Correct answer

Process isolation can run only on the same version of Windows

Hyper-V isolation can run the same version or older

<https://learn.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/version-compatibility?tabs=windows-server-2022%2Cwindows-11#windows-server-host-os-compatibility>

upvoted 10 times

**Ksk08** Most Recent 8 months ago

Correct

For Image1 (Windows Server 2022): Hyper-V isolation or process isolation

For Image2 (Windows Server 2019): Hyper-V isolation only

upvoted 2 times



  **RickySmith** 1 year, 6 months ago

Image 1 - Hyper-V isolation or process isolation

Image 2 - Hyper-V isolation only.

upvoted 3 times

  **Payday123** 1 year, 7 months ago

A new question

upvoted 3 times

## SIMULATION

-

You need to run a container that uses the `mcr.microsoft.com/windows/servercore/iis` image on SRV1. Port 80 on the container must be published to port 5001 on SRV1 and the container must run in the background.

To complete this task, sign in to the required computer or computers.