

Your company has serval departments. Each department has a number of virtual machines (VMs).
The company has an Azure subscription that contains a resource group named RG1.
All VMs are located in RG1.
You want to associate each VM with its respective department.
What should you do?

- A. Create Azure Management Groups for each department.
- B. Create a resource group for each department.
- C. Assign tags to the virtual machines.
- D. Modify the settings of the virtual machines.

Correct Answer: C

Community vote distribution

C (98%)

- green_arrow**

Highly Voted

7 months, 2 weeks ago

C is correct, the tags ASSOCIATE the vms to each deparment, then for example it can be charged to each department.

upvoted 77 times
- keyame**

2 weeks, 3 days ago

C is valid answer see full discussion: <https://lc.cx/QYWFgj>

upvoted 1 times
- verifiedtomic**

Highly Voted

3 years, 5 months ago

Selected Answer: C

Since all VMs are in the same resource group, only way to distinguish between them is by adding department tags

upvoted 8 times
- rah_rule100**

Most Recent

1 day, 18 hours ago

Selected Answer: C

C is the correct answer

upvoted 1 times
- joanjw**

2 days, 17 hours ago

Selected Answer: C

Finally, I've obtained my AZ-104 certification! Studying was challenging for six months, but Examtopics made it much easier. Their site provided the most bulk of the exam questions, and they regularly updated their question bank. The forums were really helpful in helping me understand difficult ideas and get more in-depth information. The entire certification procedure seems less daunting thanks to Examtopics Pro.

upvoted 1 times
- AKoselnik**

1 week, 2 days ago

Selected Answer: C

Tags for grouping resources in a bill in the fastest way to do that. Moreover all resources need to be kept in the same resource group. So C is correct.

upvoted 1 times
- gopi1405**

1 week, 2 days ago

Selected Answer: C

tags are best way to associate grouping departments in an organization which is also used for cost analysis

upvoted 1 times
- Emmanuel25512**

1 week, 2 days ago

Selected Answer: C

Avec des balises par département, il est possible de donner l'accès uniquement en fonction du profil

upvoted 1 times
- Makaziwe**

2 weeks, 4 days ago

Selected Answer: C

Tangs allows you to categorized resources like VMs without creating additional resources groups or management groupd

upvoted 1 times

  **Makaziwe** 2 weeks, 4 days ago

Selected Answer: C

C is correct, the tags ASSOCIATE the vms to each deparment

upvoted 1 times

  **andted98** 1 month ago

Selected Answer: C

C is the correct answer because by assigning tags, you can easily separate the VMs based on the department name.

upvoted 1 times

  **babinaprad** 1 month ago

Selected Answer: C

Hello, why is there 601 questions in the AZ-104 topic here in exam topics? I feel it is hard to read for exam. Please suggest

upvoted 1 times

  **MZ1980** 1 month, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

  **674c578** 1 month, 1 week ago

Selected Answer: C

Passed the exam 2 days ago.

847 score and only studied in here aside from few learnings in Azure official study materials that I didn't even complete.

80% of the questionnaires are in here.

My case study was a little different from the established case studies in here but if you learn from the 61 pages you should be good.



Answer in this Q is correct.

I would say the contributor access for me is value for money as I will receive a bonus by passing this exam d^_^b

But yes, the access is expensive as of today.

Goodluck!



upvoted 2 times

  **Ahitagni** 1 month, 2 weeks ago

Selected Answer: C

Assign tag to each of VMs

upvoted 1 times

  **Nepton** 1 month, 3 weeks ago

Selected Answer: C

C is the Correct answer.



upvoted 1 times

  **CheekuPR** 2 months ago

Selected Answer: C

C is correct because TAGGING is the right way

upvoted 1 times

  **HazeTech** 2 months, 3 weeks ago

Selected Answer: C

Is the correct answer

upvoted 1 times

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

Your company has an Azure Active Directory (Azure AD) subscription.

You want to implement an Azure AD conditional access policy.

The policy must be configured to require members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when they connect to Azure AD from untrusted locations.

Solution: You access the multi-factor authentication page to alter the user settings.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (100%)

  **green_arrow** Highly Voted 3 years, 10 months ago

B is correct,
1- the best way to enforce MFA is by Conditional Access
2- the device has to be identified by azure AD as A AD joined Device.
3- the trusted ip must be configured.
upvoted 155 times

  **jackdryan** 2 years, 2 months ago

B is correct.
You access the Azure portal to alter the grant control of the Azure AD conditional access policy.
upvoted 11 times

  **BeauChateau** Highly Voted 1 year, 12 months ago

Selected Answer: B

No, the solution does not meet the goal. To implement the required conditional access policy, the following steps should be taken:

Create a new Conditional Access policy in Azure AD portal.
Set the policy to require Multi-Factor Authentication and Azure AD device registration.
In the policy's "Users and Groups" section, specify the Global Administrators group as the target.
In the policy's "Conditions" section, specify the locations that are considered untrusted.
Save the policy.
Simply accessing the multi-factor authentication page and altering user settings does not provide a comprehensive solution to meet the stated goal.
upvoted 59 times

  **joanjw** Most Recent 2 days, 17 hours ago



Selected Answer: B

I have finally achieved my AZ-104 certification! Although it required six months of studying, Examtopics Pro facilitated everything. It felt as if I had a study guide in my pocket, considering that around 90% of the exam questions originated from their site. The question bank is excellent, and the forums aided my comprehension of concepts I initially found challenging.
upvoted 1 times

  **kjbalamurugan** 3 days, 17 hours ago

Selected Answer: B

Policy should be configured at group level not at user level
upvoted 1 times

  **Emmanuel25512** 1 week, 2 days ago

Selected Answer: B

Il faut configurer l'accès conditionnel en ajoutant MFA
upvoted 1 times

  **Makaziwe** 2 weeks, 4 days ago

Selected Answer: B

Condition access policies aren't configured on the multi-factor authentication MFA page, to achieve the desired results you'd need to create the conditional access policy in Azure AD specifying access, conditions, access controls.
upvoted 1 times

  **juancarlosdlar** 1 month, 1 week ago



Selected Answer: B

You can understand the answer here: <https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa?toc=%2Fentra%2Fidentity%2Fconditional-access%2Ftoc.json&bc=%2Fentra%2Fidentity%2Fconditional-access%2Fbreadcrumb%2Ftoc.json>
upvoted 1 times

  **Vinny** 2 months, 3 weeks ago



Selected Answer: B

B should be right one
upvoted 1 times

  **CameronReal** 3 months, 2 weeks ago

Selected Answer: B

In my opinion the correct option is (B)
To configure MFA the correct way is through Conditional Access Policies.
Prepare smartly with Certsleader and ace your exam.
upvoted 1 times

  **Raki1049** 4 months ago

Selected Answer: B

No, the solution does not meet the goal.



To achieve the desired outcome, you need to configure a conditional access policy that specifically targets the Global Administrators group and sets the required conditions, such as Multi-Factor Authentication (MFA) and the use of an Azure AD-joined device when accessing from untrusted locations. Altering the session control alone is not sufficient to enforce these specific requirements.

You would need to:



1. Create a new conditional access policy in the Azure portal.
2. Target the Global Administrators group.
3. Set the conditions to require MFA and an Azure AD-joined device.
4. Specify the locations considered untrusted.

Would you like more detailed steps on how to configure this policy?

upvoted 1 times

  **kiwwwyis** 6 months, 2 weeks ago

B. No
is the answer because
to enable the MFA depending on the condition can only be enabled from the conditional access option.
Not from MFA option
upvoted 2 times

  **IsaacRayan** 6 months, 3 weeks ago

La bonne réponse c'est la A
upvoted 1 times

  **examprepboy** 7 months, 2 weeks ago

Selected Answer: B

You set MFA by conditional access and use the grant option
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct
upvoted 1 times



  **[Removed]** 6 months ago

You access the Azure portal to alter the grant control of the Azure AD conditional access policy.
upvoted 2 times

  **tsummey** 10 months, 3 weeks ago

Selected Answer: B

This isn't a user setting; you need to create a conditional access policy:
Under Assignments select the Global Admin Group
Under Conditions set the location to any location and exclude all trusted locations
Under Access Controls, grant access and check the options for require MFA and require the device to be marked as compliant.
upvoted 3 times

  **tashakori** 1 year, 1 month ago

No is right
upvoted 1 times

  **Saurabh_Bhargav** 1 year, 2 months ago

B. No
is the answer because
to enable the MFA depending on the condition can only be enabled from the conditional access option.
Not from MFA option
upvoted 1 times

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

Your company has an Azure Active Directory (Azure AD) subscription.

You want to implement an Azure AD conditional access policy.

The policy must be configured to require members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when they connect to Azure AD from untrusted locations.

Solution: You access the Azure portal to alter the session control of the Azure AD conditional access policy.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (89%)

11%

edengoforit

Highly Voted

3 years, 3 months ago

Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator. Browse to Azure Active Directory > Security > Conditional Access. Select New policy. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies. Under Assignments, select Users and groups Under Include, select All users Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts. Select Done. Under Cloud apps or actions > Include, select All cloud apps. Under Exclude, select any applications that don't require multi-factor authentication. Under Access controls > Grant, select Grant access, Require multi-factor authentication, and select Select. Confirm your settings and set Enable policy to Report-only. Select Create to create to enable your policy.

upvoted 19 times

Minaru

Highly Voted

7 months, 2 weeks ago

Correct answer is B.

The solution mentioned does not fully meet the goal of requiring members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when they connect from untrusted locations. While accessing the Azure portal to alter the session control is a step in the right direction, it's essential to configure the specific conditions and controls in the Azure AD conditional access policy to enforce these requirements.

To achieve the goal, you need to create or modify an Azure AD conditional access policy and specify the conditions that require Multi-Factor Authentication and Azure AD-joined devices for members of the Global Administrators group when they access Azure AD from untrusted locations. Simply accessing the Azure portal to alter session control is not sufficient to fully implement this policy.

upvoted 9 times

Makaziwe

Most Recent

2 weeks, 4 days ago

Selected Answer: B

The solutions doesn't meet the goals because altering session control does not directly address the requirements

upvoted 1 times

[Removed]

8 months ago

Selected Answer: B

B is correct

grant control, not session control

upvoted 2 times

tsummey

10 months, 3 weeks ago

Selected Answer: B

Under Assignments select the Global Admin Group Under Conditions set the location to any location and exclude all trusted locations Under Access Controls, grant access and check the options for require MFA and require the device to be marked as compliant.

upvoted 3 times

3ba6d0b

11 months ago

Selected Answer: B

questions 3 and 4 are identical.
upvoted 1 times

  **RealmTarget** 5 months ago



No. One is asking about grant controls and one is session controls.
Grant controls are correct. Because you want to grant access in these situations.
<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant>
<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-session>
upvoted 1 times

  **76d5e04** 11 months, 1 week ago

Hello All
I see lot of recommendtions to check "Mlantonis" answers.Please let me know how to find it in this huge blog
upvoted 1 times


  **MCLC2021** 1 year, 1 month ago

Correc Answer B (NO).
Within a Conditional Access policy:
Access Control GRANT: an administrator can use access controls to grant or block access to resources.
Access Control SESSION: an administrator can make use of session controls to enable limited experiences within specific cloud applications.
upvoted 3 times

  **_gio_** 1 year, 3 months ago



Selected Answer: B

answer is B
upvoted 1 times

  **DBFront** 1 year, 6 months ago

Selected Answer: B

B is correct, needs to be grant control
upvoted 1 times

  **ShyamNallu_100813** 1 year, 9 months ago

Selected Answer: A

ANS :A
upvoted 3 times

  **SivaPannier** 1 year, 8 months ago

I think the Answer is A only. I could see session control option in the Conditional Access Policy configuration page. Grant control should not be for session control. see the link below...

upvoted 1 times

  **SivaPannier** 1 year, 8 months ago

Sorry I am wrong in the earlier comment. The correct answer is B only, for the given requirement there is no need to configure anything in the session control page of conditional access policy. Hence this action will not fulfill the project requirement.
upvoted 3 times

  **james2033** 1 year, 9 months ago

Selected Answer: B

Focus at text "alter the session", it make B is correct choice.
upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago

option B is correct
upvoted 1 times

  **Madbo** 2 years ago

Solution B is not correct because it suggests creating a new resource group for each department. While this approach could be used to organize resources, it does not allow for direct association between the virtual machines and their respective departments. Assigning tags to the virtual machines is a better solution for this requirement.
upvoted 1 times

  **emptyH** 2 years ago

Selected Answer: B

Answer is B. Require MFA is a checkbox listed within the GRANT control portion of the conditional access policy.
upvoted 3 times

  **TunaSD** 2 years, 1 month ago

No, the solution does not meet the goal. Altering the session control of the Azure AD conditional access policy alone will not achieve the desired requirements. You need to configure a conditional access policy that requires Multi-Factor Authentication (MFA) and an Azure AD-joined device for members of the Global Administrators group when connecting from untrusted locations.
upvoted 1 times

  **SindhuM** 2 years, 1 month ago

A - is correct
upvoted 1 times

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

Your company has an Azure Active Directory (Azure AD) subscription.

You want to implement an Azure AD conditional access policy.

The policy must be configured to require members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when they connect to Azure AD from untrusted locations.

Solution: You access the Azure portal to alter the grant control of the Azure AD conditional access policy.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Community vote distribution

A (90%)

10%

- Micah7

Highly Voted

3 years, 8 months ago

Answer is A. There is another copy of this question that mentions going to the MFA page in Azure Portal as the solution = incorrect. On that page you cant make a Conditional Access Policy.
I did this in lab step by step:
- The Answer "A" is correct
- Instead of the MFA page mentioned above, you have to go the route of Conditional Access Policy-->Grant Control mentioned here for this question. Under Grant Control you are given the option of setting MFA and requiring AD joined devices in the exact same window.
Answer is correct.
upvoted 72 times
- jackdryan

2 years, 2 months ago

A is correct.
upvoted 5 times
- MCLC2021

Highly Voted

1 year, 1 month ago

Correc Answer A (YES).
Within a Conditional Access policy:
Access Control GRANT: an administrator can use access controls to grant or block access to resources.
Access Control SESSION: an administrator can make use of session controls to enable limited experiences within specific cloud applications.

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-session>

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant>
upvoted 7 times
- Makaziwe

Most Recent

2 weeks, 4 days ago

Selected Answer: A

Altering the grant control of Azure AD condition policy allows you to: require MFA, require the devices to be compliant for Azure AD joint
upvoted 1 times

[Removed]

2 months, 2 weeks ago

Selected Answer: B

this is the same as q 2,3,4 the correct answer is B
upvoted 1 times

[Removed]

8 months ago

Selected Answer: A

A is correct
upvoted 1 times

Nico1973

9 months, 4 weeks ago

B. No
Explanation:
The provided solution does not meet the goal of requiring members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when connecting from untrusted locations. To achieve this, you need to configure the conditions and controls of the Azure AD conditional access policy, not just alter the grant control. By modifying the grant control, you are changing who the policy applies to, not the specific requirements for access.
upvoted 2 times

🗨️ 👤 **3c5adce** 11 months, 4 weeks ago

Yes, the solution meets the goal. By configuring the Azure AD conditional access policy to require members of the Global Administrators group to use Multi-Factor Authentication (MFA) and an Azure AD-joined device when they connect from untrusted locations, you are effectively adding an additional layer of security to protect sensitive resources and data. This ensures that even if credentials are compromised, unauthorized access is prevented by requiring an additional verification step (MFA) and ensuring the device is trusted (Azure AD-joined).

upvoted 1 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago

No is correct

upvoted 1 times

🗨️ 👤 **Samiron512** 1 year, 2 months ago

Selected Answer: B

correct answer is B. No

upvoted 1 times

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

A. Yes

upvoted 1 times

🗨️ 👤 **kkinna** 1 year, 3 months ago

Selected Answer: B

because under grand control we can only set requiring MFA and require AD joined devices but not location. setting location requirements is located under conditions control panel

upvoted 1 times

🗨️ 👤 **_gio_** 1 year, 3 months ago

Selected Answer: A

answer is A

upvoted 1 times

🗨️ 👤 **Minaru** 1 year, 6 months ago

The correct answer is: A

if you are accessing the Azure portal to alter the grant control of the Azure AD conditional access policy, and you are configuring it to require members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when connecting from untrusted locations, then the solution does indeed meet the goal.

upvoted 2 times

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

Selected Answer: A

Grant control is required for this action!

upvoted 2 times

🗨️ 👤 **james2033** 1 year, 9 months ago

Selected Answer: A

Question's keyword "Azure portal to alter the grant control of the Azure AD conditional access policy", choose A. Azure portal can done this task.

upvoted 3 times

🗨️ 👤 **liketopass** 1 year, 9 months ago

I would say 'partly' as there are 2 requirements :

1. use MFA
2. From untrusted location

And this one only specifies one of them:

To use MFA you indeed use the grant control part, but you would also need to configure the conditions to specify to exclude 'trusted locations' (effectively specifying untrusted locations)

So actually it is maybe a NO as the solution does not meet the goal

upvoted 1 times

🗨️ 👤 **ShyamNallu_100813** 1 year, 9 months ago

B Is correct

upvoted 1 times

You are planning to deploy an Ubuntu Server virtual machine to your company's Azure subscription. You are required to implement a custom deployment that includes adding a particular trusted root certification authority (CA). Which of the following should you use to create the virtual machine?

- A. The New-AzureRmVm cmdlet.
- B. The New-AzVM cmdlet.
- C. The Create-AzVM cmdlet.
- D. The az vm create command.

Correct Answer: D

Community vote distribution

D (98%)

- elishlomo

Highly Voted

3 years, 3 months ago

Selected Answer: D

The az vm create command. you need to create an Ubuntu Linux VM using a cloud-init script for configuration. For example, az vm create -g MyResourceGroup -n MyVm --image debian --custom-data
upvoted 63 times
- NaoVaz

Highly Voted

2 years, 7 months ago

Selected Answer: D

In my opinion the correct option is D) "The az vm create command".

"New-AzureRmVm" is the legacy way to create Vms using Powershell (<https://docs.microsoft.com/en-us/powershell/module/azurerm.compute/new-azurermvm?view=azurerm-6.13.0>).
"New-AzVM" Is the current way to create VMs using Powershell (<https://docs.microsoft.com/en-us/powershell/module/az.compute/new-azvm?view=azps-8.3.0>).

Using Powershell cmdlets I think that it is not currently supported to create a VM passing custom data, like a cloud-init file to accomplish the requested trust for a Custom CA.

"Create-AzVM" Does not seem to exist.

Using AZ cli or ARM Templates we can accomplish this: <https://docs.microsoft.com/en-us/azure/virtual-machines/custom-data>
upvoted 21 times
- AhmeDMoha

Most Recent

1 week, 5 days ago

Selected Answer: B

This is from AI ,

The correct answer is: B. The New-AzVM cmdlet.

 Here's the breakdown:
You're deploying an Ubuntu Server VM in Azure with a custom configuration (like adding a trusted root CA). That points to using PowerShell (not CLI), and more importantly, the current PowerShell module.

 Why not the others?
A. New-AzureRmVm
 Outdated. The AzureRM module is deprecated and replaced by Az. Avoid using this unless you want to time-travel back to 2018.

C. Create-AzVM
 Doesn't exist. Not a real cmdlet. You might be thinking of New-AzVM, which is the valid one.

D. az vm create
 Technically valid, but that's Azure CLI, not PowerShell. If you're going for scripting in Bash or Cloud Shell, sure. But you mentioned custom deployment—PowerShell gives you more control for that, especially for complex provisioning scripts.
upvoted 1 times
- Makaziwe

2 weeks, 4 days ago

Selected Answer: A

You can configure the existing usage of model from "per authentication" to per enable user" vi the Azure portal
upvoted 1 times
- Makaziwe

2 weeks, 4 days ago

Selected Answer: D

This option enable you to run scripts during employment to configure the VM including the adding trusted CAs
upvoted 1 times

  **Makaziwe** 2 weeks, 4 days ago



Selected Answer: D

The az vm create command. you need to create an Ubuntu Linux VM using a cloud-init script for configuration.
upvoted 1 times

  **OsamaQwsmi** 1 month, 2 weeks ago



Selected Answer: D

Create the virtual machine
To create a VM in this resource group, use the vm create command.
upvoted 1 times

  **bacana** 1 month, 3 weeks ago

Selected Answer: D

Others option don't have may options like use sshkey or imprt certificate from vault.
upvoted 1 times

  **compiler_765001** 2 months ago

Selected Answer: D

In my opinion the correct option is D) "The az vm create command".
upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

This command is part of the Azure CLI, and it allows for more extensive customization options, including the ability to specify custom scripts for post-deployment configuration, such as adding a trusted root certification authority (CA).
upvoted 1 times

  **victorio_27** 2 months, 3 weeks ago

Selected Answer: D

Razón por la cual no se eligen las otras opciones:

- A. New-AzureRmVm: Este cmdlet pertenece al módulo AzureRM, que está obsoleto y reemplazado por Az.
 - B. New-AzVM: Aunque es parte del módulo más reciente Az, es un cmdlet de PowerShell y no es la opción más flexible para configuraciones avanzadas como la personalización de certificados en Linux.
 - C. Create-AzVM: No existe un cmdlet con este nombre en Azure PowerShell.
- upvoted 1 times

  **hellz_rellz** 3 months, 3 weeks ago

Selected Answer: D

If using Azure CLI, the answer is D.
If using Azure PowerShell, the answer would be B, but since the question does not specify PowerShell, D is the most fitting choice.
upvoted 1 times

  **Pnidoni** 5 months ago

Selected Answer: B


correct Answer is B

New-AzVm `
-ResourceGroupName 'myResourceGroup' `
-Name 'myVM' `
-Location 'East US' `
-image Debian11 `
-size Standard_B2s `
-PublicIpAddressName myPubIP `
-OpenPorts 80 `
-GenerateSshKey `
-SshKeyName mySSHKey

<https://learn.microsoft.com/en-us/azure/virtual-machines/linux/quick-create-powershell>
upvoted 2 times

  **JustAnotherDBA** 3 months, 1 week ago

The documentation doesn't mention adding a particular trusted root certification authority (CA)
upvoted 2 times

  **smeag** 6 months, 2 weeks ago

yep D!
upvoted 1 times


  **asuarez** 7 months, 1 week ago

Selected Answer: D

To implement a custom deployment that includes adding a particular trusted root certification authority (CA) when creating an Ubuntu Server virtual machine in Azure, you should use the az vm create command (Option D).

During the VM creation process, the az vm create command allows you to specify custom scripts and configurations, such as adding a trusted root CA. This flexibility makes it suitable for custom deployments.



upvoted 2 times

  **Darkfire** 7 months, 1 week ago

Selected Answer: D

Defenitly D

upvoted 1 times

  **Davidsv** 8 months, 1 week ago

Selected Answer: D

```
az vm create \  
--resource-group myResourceGroupAutomate \  
--name myAutomatedVM \  
--image Ubuntu2204 \  
--admin-username azureuser \  
--generate-ssh-keys \  
--custom-data cloud-init.txt
```

This is what we get in this link in answer solution
<https://learn.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-automate-vm-deployment>
upvoted 3 times

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

Your company makes use of Multi-Factor Authentication for when users are not in the office. The Per Authentication option has been configured as the usage model.

After the acquisition of a smaller business and the addition of the new staff to Azure Active Directory (Azure AD) obtains a different company and adding the new employees to Azure Active Directory (Azure AD), you are informed that these employees should also make use of Multi-Factor Authentication.

To achieve this, the Per Enabled User setting must be set for the usage model.

Solution: You reconfigure the existing usage model via the Azure portal.

Does the solution meet the goal?



- A. Yes
- B. No


Correct Answer: B

Community vote distribution

B (93%)

7%



-  **NaoVaz**

Highly Voted 



 2 years, 7 months ago


Selected Answer: B

As described in the official documentation "You cannot change the usage model (per enabled user or per authentication) after an MFA provider is created."

upvoted 13 times
-  **noahsark** 5 months, 4 weeks ago

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



upvoted 1 times
-  **Stephane_37**


Highly Voted 

 2 years, 6 months ago

this should an old question, ..as : Effective September 1st, 2018 new auth providers may no longer be created.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-authprovider>



upvoted 9 times
-  **Makaziwe**

Most Recent 

 2 weeks, 4 days ago



Selected Answer: B

Configuring the existing usage of model "per authentication" of per Enable user via the Azure portal will achieve the goal

upvoted 1 times
-  **lumax007** 1 month, 2 weeks ago

Selected Answer: B

You can't change the usage model (per enabled user or per authentication) after an MFA provider is created.



upvoted 1 times
-  **giannisae** 1 month, 4 weeks ago

Selected Answer: B

You can't change the usage model (per enabled user or per authentication) after an MFA provider is created.



If you purchased enough licenses to cover all users that are enabled for MFA, you can delete the MFA provider altogether.

If your MFA provider isn't linked to a Microsoft Entra tenant, or you link the new MFA provider to a different Microsoft Entra tenant, user settings and configuration options aren't transferred. Also, existing Microsoft Entra multifactor authentication Servers need to be reactivated using activation credentials generated through the MFA Provider.

upvoted 2 times
-  **harout7** 2 months, 1 week ago

Selected Answer: A

The Azure portal allows administrators to modify MFA usage models, including switching from Per Authentication to Per Enabled User. The Per Enabled User model enforces MFA for users who are explicitly enabled, which meets the requirement.

upvoted 1 times
-  **arfan0595** 5 months, 4 weeks ago

nak wak ghane ni

upvoted 1 times

🗨️ 👤 **[Removed]** 7 months, 3 weeks ago

Selected Answer: B

B is correct

a new usage model must be created.

upvoted 2 times

🗨️ 👤 **[Removed]** 8 months ago

Selected Answer: B

B is correct

the usage model can't be modified after MFA is created, a new usage model must be created.

upvoted 1 times

🗨️ 👤 **BanthonyB** 9 months, 3 weeks ago

Yes, the solution meets the goal.

Reconfiguring the existing usage model via the Azure portal to switch from the Per Authentication option to the Per Enabled User option will allow you to enable Multi-Factor Authentication (MFA) for the new employees. This change ensures that MFA is applied to specific users rather than per authentication attempt, aligning with the requirement to include the new staff in the MFA setup.

upvoted 3 times

🗨️ 👤 **Nico1973** 9 months, 4 weeks ago

Answer: A. Yes

The solution provided meets the goal of setting the Per Enabled User option for the new employees to use Multi-Factor Authentication in Azure Active Directory. By reconfiguring the existing usage model via the Azure portal, you can ensure that the new employees are required to use Multi-Factor Authentication as intended.

upvoted 2 times

🗨️ 👤 **tashakori** 1 year, 1 month ago

No is right

upvoted 1 times

🗨️ 👤 **Winnie_the_pooh** 1 year, 1 month ago

Depreciated

As of July 1, 2019, Microsoft will no longer offer multifactor authentication server for new deployments and trial tenants. New customers who would like to require multifactor authentication from their users should use cloud-based multifactor authentication.

upvoted 3 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago

Correct

upvoted 1 times

🗨️ 👤 **_gio_** 1 year, 3 months ago

Selected Answer: B

No because you can't change usage model after MFA provider is created

upvoted 2 times

🗨️ 👤 **AlfredPennyworth** 1 year, 4 months ago

The most suitable and direct solution for changing the MFA usage model for Azure AD is to reconfigure the existing usage model via the Azure portal. This approach is user-friendly and does not require the complexities of setting up a new MFA provider or using Azure CLI for a task that is more efficiently handled through the portal.

upvoted 1 times

🗨️ 👤 **yatharthhhh_xd** 1 year, 5 months ago

The correct solution is to create a new conditional access policy that applies to the new employees. This policy should be configured to require MFA for the new employees when they sign in to Azure AD from any location.

upvoted 3 times

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

Your company's Azure solution makes use of Multi-Factor Authentication for when users are not in the office. The Per Authentication option has been configured as the usage model.

After the acquisition of a smaller business and the addition of the new staff to Azure Active Directory (Azure AD) obtains a different company and adding the new employees to Azure Active Directory (Azure AD), you are informed that these employees should also make use of Multi-Factor Authentication.

To achieve this, the Per Enabled User setting must be set for the usage model.

Solution: You reconfigure the existing usage model via the Azure CLI.

Does the solution meet the goal?



- A. Yes
- B. No


Correct Answer: B

Community vote distribution



B (83%)



A (17%)


-   **rigonet**

Highly Voted 

 3 years, 7 months ago



ANSWER: B - No
You cannot change the usage model after creating the provider.
upvoted 24 times
-   **jackdryan** 2 years, 2 months ago

B is correct.
You create a new Multi-Factor Authentication provider with a backup from the existing Multi-Factor Authentication provider data. You cannot change the usage model (per enabled user or per authentication) after an MFA provider is created.
upvoted 3 times
-   **Rab4622**



Most Recent 

 1 day, 21 hours ago



Selected Answer: B



when users are not in the office: we can't réalize this condition expect via premium entra ID (not via per Authentication neither via per enable
upvoted 1 times
-   **[Removed]** 8 months ago

Selected Answer: B



B is correct
upvoted 1 times
-   **Nico1973** 9 months, 4 weeks ago



Answer:
B. No

Explanation:
The solution provided does not meet the goal of configuring the Per Enabled User setting for the new employees to use Multi-Factor Authentication. To achieve the desired outcome, the Per Enabled User setting should be configured directly for the new employees, not by reconfiguring the existing usage model via the Azure CLI.
upvoted 1 times
-   **tashakori** 1 year, 1 month ago

No is right
upvoted 1 times
-   **_gio_** 1 year, 3 months ago

Selected Answer: B

B agree with rigonet
upvoted 1 times
-   **leo1q91** 1 year, 3 months ago

B is correct
upvoted 1 times
-   **Metavess** 1 year, 7 months ago

A usage model can not be changed once a Multi Factor Authentication has been created.

upvoted 1 times

  **TheCulture** 1 year, 9 months ago

Selected Answer: B

Aaaaaah! Same question, same answer! :^)

"You can't change the usage model (per enabled user or per authentication) after an MFA provider is created."
from <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-authprovider>

upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago

Option B is correct

upvoted 2 times

  **Andre369** 1 year, 11 months ago

Selected Answer: A

Yes, the provided solution meets the goal of configuring the usage model for Multi-Factor Authentication (MFA) for the new employees added to Azure Active Directory (Azure AD) after the acquisition.

Using the Azure CLI, you can reconfigure the existing usage model from "Per Authentication" to "Per Enabled User" to enforce MFA for all new employees in Azure AD. This ensures that MFA is required for each user individually based on their account configuration, regardless of their location or authentication attempts.

upvoted 2 times

  **Madbo** 2 years ago



the solution does not meet the goal because the question states that the "Per Enabled User" setting must be set for the usage model, but the solution mentioned only reconfiguring the existing usage model via the Azure CLI. It does not specify how to change the usage model to "Per Enabled User," which requires additional steps such as setting the user-based policy in Azure AD conditional access. Therefore, the correct answer is B: No, the solution does not meet the goal.

upvoted 3 times

  **lokii9980** 2 years, 1 month ago

Yes, the solution meets the goal of configuring Multi-Factor Authentication for the new employees added to Azure Active Directory (Azure AD). By reconfiguring the existing usage model via the Azure CLI and setting the Per Enabled User setting, the new employees will be required to use Multi-Factor Authentication. This ensures that the new employees' accounts are secured and protected by an extra layer of security beyond just a password.

upvoted 1 times

  **allyQ** 2 years, 2 months ago

Does anyone proof-read these scenarios? ...

upvoted 1 times

  **Rufusinski** 2 years, 3 months ago

Selected Answer: B

B is correct.

upvoted 1 times

  **Sunnyb** 2 years, 5 months ago

B is correct

upvoted 1 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

As described in the official documentation (<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-authprovider>):
"You cannot change the usage model (per enabled user or per authentication) after an MFA provider is created."

upvoted 2 times

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

Your company's Azure solution makes use of Multi-Factor Authentication for when users are not in the office. The Per Authentication option has been configured as the usage model.

After the acquisition of a smaller business and the addition of the new staff to Azure Active Directory (Azure AD) obtains a different company and adding the new employees to Azure Active Directory (Azure AD), you are informed that these employees should also make use of Multi-Factor Authentication.

To achieve this, the Per Enabled User setting must be set for the usage model.

Solution: You create a new Multi-Factor Authentication provider with a backup from the existing Multi-Factor Authentication provider data.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (87%)

13%

- walkaway**

Highly Voted

2 years, 3 months ago

Selected Answer: B

It is a big NO now in 2023. If you still see this question, never say YES.

upvoted 15 times
- FurnishedFlapjack**

Highly Voted

2 years, 6 months ago

Selected Answer: B

Was A, now after 2018 is B

upvoted 7 times
- victorio_27**

Most Recent

2 months, 3 weeks ago

Selected Answer: B

El modelo de uso de MFA en Azure AD está configurado como "Por autenticación", lo que significa que la autenticación multifactor se aplica según condiciones específicas, como cuando los usuarios acceden desde fuera de la oficina.

El problema a resolver es que los nuevos empleados también deben cumplir con esta regla, por lo que la solución correcta sería actualizar la política de acceso condicional en Azure AD para incluirlos.

Por qué la solución propuesta no cumple el objetivo:

Crear un nuevo proveedor de autenticación multifactor con una copia de seguridad no es necesario ni relevante para este escenario. La configuración existente ya usa MFA basado en acceso condicional, por lo que la forma correcta de incluir a los nuevos empleados es modificando la política de acceso condicional en lugar de crear un nuevo proveedor de MFA.

upvoted 1 times
- 58b2872**

4 months, 1 week ago

Selected Answer: B

you need to change it from per auth to per enabled

upvoted 2 times
- minura**

4 months, 2 weeks ago

Selected Answer: B

Answer B. No

upvoted 1 times
- Mark74**

5 months ago

Selected Answer: B

It's B

upvoted 1 times
- asuares**

7 months, 1 week ago

Selected Answer: B

Creating a new Multi-Factor Authentication provider with a backup from the existing provider data does not change the usage model from Per Authentication to Per Enabled User. You would need to specifically change the Multi-Factor Authentication settings to the Per Enabled User model to meet the requirements.

upvoted 6 times

  **[Removed]** 7 months, 3 weeks ago

Selected Answer: B

it's B

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

it's B

upvoted 1 times

  **tsummey** 10 months, 3 weeks ago

Selected Answer: B

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

Important:
Effective September 1st, 2018 new auth providers may no longer be created. Existing auth providers may continue to be used and updated, but migration is no longer possible. Multifactor authentication will continue to be available as a feature in Microsoft Entra ID P1 or P2 licenses.
upvoted 3 times

  **BrkyUlukn** 11 months, 1 week ago

answer is B NO

Effective September 1st, 2018 new auth providers may no longer be created. Existing auth providers may continue to be used and updated, but migration is no longer possible. Multi-factor authentication will continue to be available as a feature in Azure AD Premium licenses.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-authprovider>

upvoted 1 times

  **abhinav_4567** 11 months, 3 weeks ago

Selected Answer: B

b IS CORRECT

upvoted 3 times

  **varinder82** 1 year ago

Final Answer: A (You can't change the usage model (per enabled user or per authentication) after an MFA provider is created.)

upvoted 1 times

  **JPA210** 6 months ago



Yes , you can. Check the documentation again.

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

Yes is correct

upvoted 1 times

  **_gio_** 1 year, 3 months ago

Selected Answer: B

i think B

upvoted 2 times



  **peterp007** 1 year, 3 months ago

Answer -B (No)

Effective September 1st, 2018 new auth providers may no longer be created. Existing auth providers may continue to be used and updated, but migration is no longer possible. Multifactor authentication will continue to be available as a feature in Microsoft Entra ID P1 or P2 licenses.

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

upvoted 2 times

  **ggogel** 1 year, 5 months ago

Selected Answer: B

A would have been the correct answer, but as of 1st September 2018 MFA Providers are discontinued and can not be created anymore. As of today, the only way to use MFA is if the user has a license assigned that includes the MFA feature.

upvoted 7 times

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

Your company has an Azure Active Directory (Azure AD) tenant named weyland.com that is configured for hybrid coexistence with the on-premises Active Directory domain.

You have a server named DirSync1 that is configured as a DirSync server.

You create a new user account in the on-premise Active Directory. You now need to replicate the user information to Azure AD immediately.

Solution: You run the Start-ADSyncSyncCycle -PolicyType Initial PowerShell cmdlet.

Does the solution meet the goal?

A. Yes



B. No


Correct Answer: B

Community vote distribution



B (72%)



A (28%)



-   **imartinez**



Highly Voted 



 3 years, 9 months ago



Answer is B (No)
Initial will perform a full sync and add the user account created but it will take time,
Delta, will kick off a delta sync and bring only the last change, so it will be "immediately" and will fulfill the requirements.
upvoted 129 times
-   **juniorccs** 3 years, 3 months ago



if the delta will be bring the last changes, so it's okay here, isn't it ? the answer should be then "YES" , correct ? where am I lost here ?
upvoted 5 times
-   **Bere** 3 years, 2 months ago



In the solution of this question they say "-PolicyType Initial".
However you must use "-PolicyType Delta" to get only the change made and sync it immediately.
So the answer is "No".
upvoted 29 times
-   **jackdryan** 2 years, 2 months ago


A is correct.
upvoted 10 times
-   **skydivex** 2 years, 2 months ago

The answer is A (YES), since the question did not mention the initial sync has been already done. A is correct
upvoted 13 times
-   **arunet** 3 years, 2 months ago

B is the answer. <https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-how-to-force-azuread-connect-to-sync/ba-p/887043>
upvoted 9 times
-   **GenjamBhai** 3 years ago

B is ok, delta for immediate sync, initial will take longer
upvoted 6 times
-   **Etan1** 1 year, 10 months ago

You article is correct but the answer is A Run the following command to force a complete sync but note that the length of sync time would be greatly increased.
Start-ADSyncSyncCycle -PolicyType Initial
upvoted 1 times
-   **GoldenDisciple2**

Highly Voted 

 1 year, 9 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-feature-scheduler>

In this article. It says word for word, "It could be that you have an urgent change that must be synchronized immediately, which is why you need to manually run a cycle.

If you need to manually run a sync cycle, then from PowerShell run Start-ADSyncSyncCycle -PolicyType Delta."
Keywords in this learn.microsoft article are immediately and manually.... If you want it to synchronize immediately, then you'll want to manually run

a cycle.... To run a cycle manually, run the -delta command.

Immediate = Manual. Manual = Delta. Therefor Immediate = Delta

Full sync = Time Consuming. Time Consuming = Initial
upvoted 19 times

  **Rab4622** Most Recent 1 day, 20 hours ago

Selected Answer: B

La commande Start-ADSyncSyncCycle -PolicyType Initial est spécifique à Azure AD Connect, et non à DirSync.
upvoted 1 times

  **Rab4622** 1 day, 20 hours ago



Selected Answer: B

Is no because the command is for Azure ad connect not for the obsolete service servsync
upvoted 1 times

  **andted98** 1 month ago

Selected Answer: B

To initiate an immediate sync between the on-premises AD and Azure Active Directory, the policy type needs to be changed from 'Initial' to 'Delta'.
upvoted 1 times

  **jharishi** 1 month, 3 weeks ago

Selected Answer: A

A is correct, as it meets the solution. It doesn't ask the faster solution, just if its meet or not, so it meet.
upvoted 1 times

  **victorio_27** 2 months, 3 weeks ago

Selected Answer: A

I cmdlet Start-ADSyncSyncCycle -PolicyType Initial se usa en entornos con Azure AD Connect (anteriormente DirSync) para iniciar manualmente una sincronización completa de directorios.

Dado que el entorno descrito utiliza Azure AD en modo híbrido con un servidor DirSync (DirSync1), la creación de una nueva cuenta de usuario en Active Directory local no se replicará inmediatamente en Azure AD a menos que se inicie manualmente la sincronización o se espere la sincronización programada (que ocurre cada 30 minutos, por defecto).

Diferencia entre tipos de sincronización en Azure AD Connect:



Delta: Solo sincroniza los cambios recientes. Se ejecuta automáticamente cada 30 minutos.

Initial: Realiza una sincronización completa, útil para nuevos usuarios, cambios de esquema o cuando se configuran nuevas reglas de sincronización.
upvoted 1 times

  **willie439** 3 months, 1 week ago

Selected Answer: A

Answer A is correct.
The question is "Does the solution meet the goal?" it is not the best solution, however it meet the goal.
upvoted 1 times

  **Nathan12345** 3 months, 3 weeks ago

Selected Answer: A

To run Delta cmd, data needs to be synced already.
Anyway Initial cmd will not impact immediately however for new sync below cmd is req
Start-ADSyncSyncCycle -PolicyType Initial
upvoted 1 times

  **guha_saheb** 4 months ago

Selected Answer: B

immediately key word changes the answer to NO
so the corret answer in this question in B
upvoted 1 times

  **guha_saheb** 4 months ago

Selected Answer: A

it will take time but the solution is met
upvoted 1 times

  **SolimanAlali** 4 months ago

Selected Answer: A

The Start-ADSyncSyncCycle PowerShell cmdlet is used to trigger a synchronization cycle between the on-premises Active Directory and Azure Active Directory.



-PolicyType Initial: This parameter forces a full synchronization of all objects from the on-premises Active Directory to Azure AD. It includes all changes and ensures that the newly created user is replicated to Azure AD.

Since the goal is to replicate the new user information to Azure AD immediately, running this cmdlet with the -PolicyType Initial parameter meets the requirement.

We can use Start-ADSyncSyncCycle:


- PolicyType Delta: Use this for incremental syncs, which only synchronize the changes since the last sync. It is faster and sufficient in most cases.
- PolicyType Initial: Use this for a full sync. It processes all objects and is typically used when there are significant changes, such as schema updates or large-scale object additions.

upvoted 1 times

  **mm102938** 5 months, 2 weeks ago


according to <https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-feature-scheduler>
"Running a full sync cycle can be very time consuming" you need to use delta instead of initial

upvoted 1 times

  **Capzn** 5 months, 2 weeks ago

Answer should be A here. Initial initiates a full sync cycle while Delta sync's the changes made since the last sync

upvoted 1 times

  **Ariel235788** 6 months, 2 weeks ago



Running the PowerShell cmdlet Start-ADSyncSyncCycle -PolicyType Initial will trigger a full synchronization cycle between your on-premises Active Directory and Azure Active Directory. This ensures that any new user accounts or changes made on-premises, like the one you created, are replicated to Azure AD immediately.

The "Initial" policy type triggers a full sync, which is appropriate in this case to ensure that the newly created user account is synchronized.

The correct answer is:

A. Yes



upvoted 2 times

  **0378d43** 6 months, 3 weeks ago

Selected Answer: A

The cmdlet would sync it

upvoted 1 times

  **LaReis** 6 months, 3 weeks ago

Segundo o Copilot: A. Sim. Executar o cmdlet Start-ADSyncSyncCycle -PolicyType Initial no PowerShell iniciará uma sincronização imediata entre o Active Directory local e o Azure AD, replicando as informações do usuário.

upvoted 2 times

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

Your company has an Azure Active Directory (Azure AD) tenant named weyland.com that is configured for hybrid coexistence with the on-premises Active Directory domain.

You have a server named DirSync1 that is configured as a DirSync server.

You create a new user account in the on-premise Active Directory. You now need to replicate the user information to Azure AD immediately.

Solution: You use Active Directory Sites and Services to force replication of the Global Catalog on a domain controller.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (100%)

  **j5y**



Highly Voted

 3 years, 10 months ago

Ans: NO



On a server with Azure AD Connect installed, navigate to the Start menu and select AD Connect, then Synchronization Service.

- 1. Go to CONNECTORS tab.
 - 2. Select RUN on the ACTIONS pane.
- upvoted 88 times

  **dendenp** 8 months, 2 weeks ago



you always run powershell cmdlet
Start-ADSyncSyncCycle -PolicyType Delta - works just as good- but even faster

upvoted 2 times

  **Saurabh_Bhargav** 1 year, 2 months ago



Thanks for the answer. I will check from the Microsoft Entra ID connect options

upvoted 1 times

  **haazybanj** 3 years ago



Where is the connectors tab located?
I can't find it here

upvoted 2 times

  **haazybanj** 3 years ago

It's under the Synchronization service manager

upvoted 1 times

  **NaoVaz**



Highly Voted

 2 years, 7 months ago

Selected Answer: B

Like described already by other people the best way is either a Synchronization being executed through the "Azure AD Connect", in the Portal or using the command "Start-ADSyncSyncCycle -PolicyType Delta".

upvoted 22 times

  **andted98**



Most Recent

 1 month ago

Selected Answer: B

The 'Active Directory Sites and Services' will only force the replication to all on-premises sites which do replicate the newly created user account, but not in the correct environment (Azure Active Directory).



upvoted 1 times

  **lumax007** 1 month, 2 weeks ago

Selected Answer: B

It is delta

upvoted 1 times

  **asuares** 7 months, 1 week ago

Selected Answer: B

Using Active Directory Sites and Services to force replication of the Global Catalog on a domain controller will only ensure that the new user information is replicated across the on-premises Active Directory environment. It does not trigger synchronization to Azure AD. To replicate the user information to Azure AD immediately, you must run the Start-ADSyncSyncCycle PowerShell cmdlet.

upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

  **Nico1973** 9 months, 4 weeks ago

Answer: B. No

Explanation:

The proposed solution of using Active Directory Sites and Services to force replication of the Global Catalog on a domain controller does not meet the goal of replicating the new user account information to Azure AD immediately. Azure AD Connect is the tool typically used to synchronize user information between on-premises Active Directory and Azure AD. To achieve immediate replication, you would need to trigger a manual synchronization from the Azure AD Connect server rather than relying on Active Directory Sites and Services.

upvoted 2 times

  **004b54b** 10 months, 3 weeks ago

Selected Answer: B

As explained by ef094b65596c14:



B. No, the solution does not meet the goal. Using Active Directory Sites and Services to force replication of the Global Catalog on a domain controller will not directly replicate the user information to Azure AD. The appropriate action would be to use Azure AD Connect to manually trigger a delta synchronization cycle.

upvoted 1 times

  **tashakori** 1 year, 1 month ago

No is right

upvoted 1 times

  **_gio_** 1 year, 3 months ago

Selected Answer: B

i think b

upvoted 1 times

  **VV11_SS22** 1 year, 8 months ago

NO , ON connector servers manually run a sync cycle, then from PowerShell run Start-ADSyncSyncCycle -PolicyType Delta." , DELTA will replicate only changes not full so will be quick

upvoted 1 times

  **james2033** 1 year, 9 months ago

Selected Answer: B

(1) Active Directory Sites & Services inside Windows Server 2022:

(2) Define "Global Catalog": <https://learn.microsoft.com/en-us/windows/win32/ad/global-catalog>

Azure AD Connect: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/reference-connect-dirsync-deprecated>

Cannot use (1) to force replicate (2). Use Azure AD connect by Command "Start-ADSyncSyncCycle -PolicyType Delta" (See <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-feature-scheduler#full-sync-cycle>) Or via Azure portal web GUI.

upvoted 2 times

  **Andre369** 1 year, 11 months ago

Selected Answer: B

Using Active Directory Sites and Services to force replication of the Global Catalog on a domain controller does not directly impact the synchronization process between the on-premises Active Directory and Azure AD.

To replicate the new user information to Azure AD immediately, you should use Azure AD Connect, the synchronization tool for integrating on-premises Active Directory with Azure AD. Azure AD Connect is responsible for synchronizing changes between the on-premises environment and Azure AD.



upvoted 4 times

  **Madbo** 2 years ago

B the correct one

The solution mentioned in the scenario, which is using Active Directory Sites and Services to force replication of the Global Catalog on a domain controller, will replicate the user information to other domain controllers in the same site, but it will not replicate the user information to Azure AD immediately. To replicate the user information to Azure AD immediately, you need to manually start a synchronization cycle on the DirSync server or wait for the next scheduled synchronization cycle to occur. Therefore, the solution does not meet the goal of replicating the user information to Azure AD immediately.


upvoted 3 times

  **je_it** 2 years, 1 month ago

B. No

To replicate the new user account information to Azure AD immediately, you should initiate a delta synchronization from the DirSync server (DirSync1) to Azure AD.

upvoted 1 times

  **DaJarHead** 2 years, 2 months ago

Active Directory Sites and Services will update other domain controllers, or you can restore the AD, but you can't replicate to Azure AD with it

upvoted 5 times

  **Rufusinski** 2 years, 3 months ago

Selected Answer: B

B is correct.

upvoted 1 times

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

Your company has an Azure Active Directory (Azure AD) tenant named weyland.com that is configured for hybrid coexistence with the on-premises Active Directory domain.

You have a server named DirSync1 that is configured as a DirSync server.

You create a new user account in the on-premise Active Directory. You now need to replicate the user information to Azure AD immediately.

Solution: You restart the NetLogon service on a domain controller.

Does the solution meet the goal?



A. Yes

B. No

Correct Answer: B



Community vote distribution



B (100%)



-   **Bere** Highly Voted 3 years, 5 months ago



As described here:
If you need to manually run a sync cycle, then from PowerShell run Start-ADSyncSyncCycle -PolicyType Delta.



To initiate a full sync cycle, run Start-ADSyncSyncCycle -PolicyType Initial from a PowerShell prompt.

Running a full sync cycle can be very time consuming, so if you need to replicate the user information to Azure AD immediately then run Start-ADSyncSyncCycle -PolicyType Delta.
Answer is B. No
upvoted 117 times
-   **sumit_das** 3 years, 1 month ago



very good explanation.
upvoted 4 times
-   **juniorccs** 3 years, 3 months ago

very important explanation
upvoted 4 times
-   **jackdryan** 2 years, 2 months ago



B is correct.
You run the Start-ADSyncSyncCycle -PolicyType Initial PowerShell cmdlet.
upvoted 4 times
-   **18c2076** 1 year, 1 month ago

For any immediate sync actions from AADConnect you do NOT run the Policy Type Initial. YOU RUN POLICY TYPE DELTA!!!!!!!!!!
upvoted 3 times
-   **Steve1983** Highly Voted 3 years, 10 months ago



NO

Please dont restart 'Netlogon' ever, in test or production... Rather reboot the whole DC, wich wont help for starting a sync i guess. If it does, its kinda a retarded way to force a sync to start.
upvoted 34 times
-   **andted98** Most Recent 1 month ago

Selected Answer: B

The NetLogon service is capable of handling authentication users in the domain. For the scope of this question, the policy type needs to be changed to 'Delta'.
upvoted 1 times
-   **[Removed]** 8 months ago

Selected Answer: B



B is correct
upvoted 1 times
-   **Shkb** 8 months, 3 weeks ago

Answer: No
To replicate the new user information from your on-premises Active Directory to Azure Active Directory (Azure AD) immediately, you should run the following PowerShell command on the DirSync1 server:



powershell:
Start-ADSyncSyncCycle -PolicyType Delta
Here's what it does:

Start-ADSyncSyncCycle: This command starts a synchronization cycle.
-PolicyType Delta: This option triggers a delta sync, which is a quick sync that only replicates changes made since the last sync (such as the creation of the new user account).
This command will ensure that the new user information is replicated to Azure AD without waiting for the next scheduled sync.

upvoted 1 times

  **nearF** 9 months, 3 weeks ago

No is the correct answer
upvoted 1 times

  **Nico1973** 9 months, 4 weeks ago



Answer: No
Explanation:
Restarting the NetLogon service on a domain controller will not immediately replicate the new user account information to Azure AD. The DirSync server is responsible for synchronizing user information between the on-premises Active Directory domain and Azure AD. To replicate the new user information to Azure AD immediately, you should manually run a synchronization cycle on the DirSync server or force a synchronization using PowerShell commands.
upvoted 1 times

  **tashakori** 1 year, 1 month ago

No is right
upvoted 2 times

  **Saurabh_Bhargav** 1 year, 2 months ago

B
To run the manual sync cycle you can use command
Start-ADSyncSyncCycle -PolicyType Delta
To run full initial Sync
Start-ADSyncSyncCycle -PolicyType Initial
upvoted 1 times

  **_gio_** 1 year, 3 months ago

Selected Answer: B
I think no
upvoted 1 times

  **VirenderPannu** 1 year, 4 months ago

Delta synchronization is for routine updates, processing only changes since the last sync, while Initialize synchronization is more resource-intensive and is used for initial setup or major changes.
upvoted 2 times

  **thang2902** 1 year, 7 months ago

B is correct
upvoted 1 times

  **Push_Harder** 1 year, 7 months ago

AD to AAD Directory Synchronization is done through Azure AD Connect.



Netlogon is a Local Security Authority service that runs in the background. It handles domain user login authentication. It maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.
upvoted 1 times

  **james2033** 1 year, 9 months ago

Selected Answer: B
Cannot use NetLogon service for replicate user information to Azure AD (even not immediately).
upvoted 3 times

  **james2033** 1 year, 9 months ago

Selected Answer: B
[Restarting NetLogon service] is not related to [Active Directory syncing].
upvoted 1 times

  **iUCorbe** 1 year, 10 months ago

Selected Answer: B
run Start-ADSyncSyncCycle -PolicyType Delta
upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago

Option B

upvoted 2 times

Your company has a Microsoft Azure subscription.

The company has datacenters in Los Angeles and New York.

You are configuring the two datacenters as geo-clustered sites for site resiliency.

You need to recommend an Azure storage redundancy option.

You have the following data storage requirements:

- ☞ Data must be stored on multiple nodes.
- ☞ Data must be stored on nodes in separate geographic locations.
- ☞ Data can be read from the secondary location as well as from the primary location.

Which of the following Azure stored redundancy options should you recommend?



- A. Geo-redundant storage
- B. Read-only geo-redundant storage
- C. Zone-redundant storage
- D. Locally redundant storage


Correct Answer: B

Community vote distribution

B (84%)

Other

-  **Steve1983**

Highly Voted 

 3 years, 10 months ago

B



(A: "data will be available to be read-only if Microsoft initiates a failure", so its not RO if its not failed-over)

Geo-redundant storage (GRS)

As I explained above it helps us in replicating our data to another region which is far away hundreds of miles away from the primary region. It provides at least 99.99999999999999% (16 9's) durability of objects over a given year. GRS replicates our data to another region, but data will be available to be read-only if Microsoft initiates a failure from primary to the secondary region.



Read-access geo-redundant storage (RA-GRS)

It is based on the GRS, but it also provides an option to read from the secondary region, regardless of whether Microsoft initiates a failover from the primary to the secondary region.



upvoted 93 times
-  **pheztux** 6 months, 2 weeks ago

For those in doubt, here is an exact statement from MS: With an account configured for GRS or GZRS, data in the secondary region isn't directly accessible to users or applications when an outage occurs in the primary region, unless a failover occurs.



If your applications require high availability, then you can configure your storage account for read access to the secondary region. When you enable read access to the secondary region, then your data is always available to be read from the secondary, including in a situation where the primary region becomes unavailable. Read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS) configurations permit read access to the secondary region.


upvoted 5 times
-  **pheztux** 6 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#read-access-to-data-in-the-secondary-region>

upvoted 1 times
-  **jackdryan** 2 years, 2 months ago

B is correct.

upvoted 4 times
-  **Saravana12g**



Highly Voted 


 3 years, 7 months ago

Answer B.

Read-access geo-redundant storage (RA-GRS)

It is based on the GRS, but it also provides an option to read from the secondary region, regardless of whether Microsoft initiates a failover from the primary to the secondary region.



upvoted 21 times
-  **nicobio**

Most Recent 

 3 weeks, 4 days ago

Selected Answer: B

Because it can be stored on a geographically remote node and read from a secondary location

upvoted 1 times
-  **nicolase** 1 month ago

Selected Answer: B

Correct

upvoted 1 times

  **mathyvarnan** 2 months ago

Selected Answer: A

GPt Says

The correct Azure storage redundancy option that meets the requirements is:

A. Geo-redundant storage (GRS)

Explanation:

Geo-redundant storage (GRS) stores data across two geographic locations (regions), which aligns with your requirement to store data in separate geographic locations.

upvoted 1 times

  **BUDSENA** 2 months, 1 week ago



Selected Answer: A

There is no read-only geo-redundant storage. It's called Read Access, it's a trick question.

A is the correct answer.

B should be correct if it stated the correct name.



upvoted 2 times

  **henry_chou** 3 months, 4 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

  **Mark74** 5 months ago

Selected Answer: B

B is correct (RA-GRS)

upvoted 1 times

  **Jig77** 5 months, 3 weeks ago

Correct answer should be 'B'. GRS (Geo-Redundant Storage): Replicates data to a secondary region (typically hundreds of miles away). If the primary region fails, the data can be restored from the secondary region.

RA-GRS (Read-Access Geo-Redundant Storage): Works like GRS, but with the additional capability that data can be read from the secondary region.

This is useful for scenarios where you may want to access your data even if the primary region is down.

upvoted 1 times

  **yusuf_eb** 6 months ago

Selected Answer: B

In Azure terminology, Read-Access Geo-Redundant Storage (RA-GRS) is sometimes referred to as "Read-Only Geo-Redundant Storage" because:

Secondary Region Access is Read-Only: In RA-GRS, data replicated to the secondary region is accessible but only in read-only mode. This means users cannot modify the data in the secondary location—they can only read it. Write operations are still limited to the primary location.

Distinction from Full Read-Write Access: The term "read-only" emphasizes that while you can access data in the secondary region, it's not a fully writable, independent copy. Changes must still originate in the primary location, and then they're asynchronously replicated to the secondary.

Summary:

So, "read-only" simply clarifies that while the secondary location provides access for reading, it's not intended for active data modification, thus helping maintain data integrity across regions.

Correct Answer: B. Read-Only Geo-Redundant Storage (RA-GRS)


upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B


B is correct

upvoted 1 times

  **[Removed]** 8 months, 4 weeks ago

Read carefully, there is no such thing as Read Only - check out <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy>

upvoted 1 times

  **Nico1973** 9 months, 4 weeks ago

Based on the provided data storage requirements, the recommended Azure storage redundancy option would be:

- A. Geo-redundant storage

Explanation: Geo-redundant storage meets all the specified requirements:

Data is stored on multiple nodes.

Data is stored on nodes in separate geographic locations (Los Angeles and New York in this case).

Data can be read from the secondary location (New York) as well as from the primary location (Los Angeles).

upvoted 1 times

  **004b54b** 10 months, 3 weeks ago

Selected Answer: B

RO-GRS

upvoted 1 times

  **tsummey** 10 months, 3 weeks ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/storage/common/geo-redundant-design>

upvoted 1 times

  **76d5e04** 11 months, 1 week ago

The answer is RA-GRS but in answer option it is said Read-only Geo Redundant Storage, which is not exists. Please confirm if the answer wording is correct, if it is then none of the answer matches the question

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

B. Read-only geo-redundant storage

This option best meets the requirements because it stores data in a geographically distant location and allows for read access from the secondary location as well as the primary.

upvoted 1 times

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

Establish if the solution satisfies the requirements.

Your company has an azure subscription that includes a storage account, a resource group, a blob container and a file share.

A colleague named Jon Ross makes use of a solitary Azure Resource Manager (ARM) template to deploy a virtual machine and an additional Azure Storage account.

You want to review the ARM template that was used by Jon Ross.

Solution: You access the Virtual Machine blade.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (97%)

- Madbo

Highly Voted

2 years ago

No, accessing the Virtual Machine blade does not provide access to the ARM template used by Jon Ross to deploy the virtual machine and an additional Azure Storage account. The Virtual Machine blade only displays information about the virtual machine itself and its related resources, but not the ARM template used to deploy it.

To review the ARM template used by Jon Ross, you need to access the deployment history of the resource group where the virtual machine and additional storage account were deployed. This will show all deployments made to the resource group, including the ARM template used for the deployment.

upvoted 27 times
- d0bermannn

Highly Voted

3 years, 10 months ago

it is so easy =B. No))

upvoted 10 times
- victorio_27

Most Recent

2 months, 3 weeks ago

Selected Answer: B

es la B ya que cuando tu creas un ARM template de una VM solo puedes crear dentro todo con respecto a la VM mas no con le storgae account

upvoted 1 times
- dnt91

4 months, 3 weeks ago

Selected Answer: A

you can access the template through the VM blade. Go to Automation > Export Template. Azure will generate a template representing the current VM Configuration.

upvoted 1 times
- Saaaii666

3 months, 4 weeks ago

Export template shows only VM related ARM JSON.

upvoted 1 times
- [Removed]

7 months, 3 weeks ago

Selected Answer: B

B is correct

Resource Group blade

upvoted 1 times
- [Removed]

8 months ago

Selected Answer: B

B is correct

upvoted 1 times
- jacksparrowtabali

1 year, 1 month ago

All templates in a RG are stored in Deployments within the the resource group level



upvoted 5 times
- Saurabh_Bhargav

1 year, 2 months ago

B. No

Because i need to access the RG Blade for ARM template of VM and Storage

upvoted 1 times

  **_gio_** 1 year, 3 months ago

Selected Answer: B

i think no B

upvoted 1 times

  **Tilakarasu** 1 year, 4 months ago

RG level it correct, as it gives complete template information used to deploy (Here, VM+SA)
VM level give only VM level template info.

upvoted 1 times

  **naveedpk00** 1 year, 6 months ago

B IS CORRECT

upvoted 1 times

  **fiahbone** 1 year, 7 months ago

Selected Answer: B



Not shown here. Need to go to recourse group and the Deployments tab.

upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago



B is correct

upvoted 2 times

  **Peeking** 1 year, 10 months ago

A template can be exported from both Resource or Resource Group. I think a VM is a resource as well.

upvoted 1 times

  **Diedo** 1 year, 10 months ago

But there are 2 different resources here. The Storage Account resource would be missing.

upvoted 4 times

  **petersoliman** 2 years ago

Selected Answer: B

B is the Answer



You review the ARM template from the Azure Resource Group Deployment, Deployments Tab.

upvoted 3 times

  **TokpaCamara** 2 years, 1 month ago

Answer B. You should use Ressource Group blade to export one to all resources inside the resource group.

upvoted 2 times

  **je_it** 2 years, 1 month ago

B.

To review the ARM template, you need to access the deployment history of the resource group where the virtual machine and additional storage account were deployed. You can access the deployment history by navigating to the “Deployments” blade of the resource group in the Azure portal.

upvoted 3 times

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

Establish if the solution satisfies the requirements.

Your company has an azure subscription that includes a storage account, a resource group, a blob container and a file share.

A colleague named Jon Ross makes use of a solitary Azure Resource Manager (ARM) template to deploy a virtual machine and an additional Azure Storage account.

You want to review the ARM template that was used by Jon Ross.

Solution: You access the Resource Group blade.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Community vote distribution



A (68%)B (32%)

  **green_arrow** Highly Voted 3 years, 10 months ago

A is correct
upvoted 23 times

  **jackdryan** 2 years, 2 months ago

A is correct
upvoted 4 times

  **enklau** 10 months, 3 weeks ago

A is correct
upvoted 2 times

  **AA000EE** 4 months, 1 week ago

A is correct
upvoted 1 times

  **eternaldiarrhea** 1 month, 3 weeks ago

A is correct
upvoted 1 times

  **Akosih** 1 month ago

A is correct
upvoted 1 times

  **Madbo** Highly Voted 2 years ago

Yes, accessing the Resource Group blade can meet the goal of reviewing the ARM template used by Jon Ross to deploy the virtual machine and additional Azure Storage account.

In the Resource Group blade, you can select the resource group where the virtual machine and additional storage account were deployed, and then click on the "Deployments" tab. This will display a list of all deployments made to the resource group, including the ARM template used for the deployment.

Therefore, the solution of accessing the Resource Group blade meets the goal of reviewing the ARM template used by Jon Ross. The answer is A. Yes.

upvoted 13 times

  **ahmadsaquib** Most Recent 23 hours, 17 minutes ago

Selected Answer: B

To see the actual ARM template, you should:
Go to the Resource Group in the Azure Portal.
Navigate to Deployments (under the "Settings" section).
Select the specific deployment (e.g., the one initiated by Jon Ross) There, you can view the Template used for that deployment.

Correct Solution:
Access the Deployments section of the Resource Group to review the ARM template.
Thus, simply accessing the Resource Group blade alone does not meet the goal.
upvoted 1 times

  **himanshu007007** 2 months ago

Selected Answer: B

No, accessing the Resource Group blade alone will not allow you to review the ARM template that was used for deployment.

Correct Approach:

To view the ARM template used for a deployment, you should:

Go to Azure Portal

Navigate to Resource Group → Find the Deployed Resource (e.g., the VM or Storage Account created by Jon Ross).

Click on "Deployments" (inside the Resource Group).

Select the specific deployment you want to review.

Click "Template" to view the ARM template used.

Why Not the Resource Group Blade Alone?

The Resource Group blade only shows deployed resources and their properties.

It does not provide the actual ARM template used for deployment unless you check the Deployments section.

upvoted 1 times

  **Sam_Diddio** 2 months, 1 week ago

Selected Answer: B



If you only go to the Resource Group blade but don't navigate to the "Deployments" section, they won't be able to see the actual ARM template used. The Resource Group blade by default shows the resources overview, but not the deployments or templates directly.

upvoted 1 times

  **Sam_Diddio** 2 months, 1 week ago

However after reviewing the documentation and watching exam preparation videos, I suppose we need to answer A during the exam.

upvoted 2 times

  **UCS_CP** 2 months, 2 weeks ago

Selected Answer: B

Accessing the Resource Group blade in the Azure portal will allow you to see the resources within the resource group, but it will not provide you with the ARM template used for deployment. To review the ARM template, you should access the deployment history for the resource group and view the template used in the deployment

upvoted 1 times

  **ea4b48e** 2 months, 3 weeks ago

Selected Answer: B

Answer: B. No

To review the ARM template used by Jon Ross, you should navigate to the "Deployments" section of the specific Resource Group where the deployment was executed. By accessing the Resource Group blade alone, you would not directly access the ARM template. You need to specifically look at the deployments within that Resource Group. So, this solution does not meet the goal.

upvoted 3 times

  **Sholasleek** 6 months ago

To review the ARM template, you would typically need to access the deployment history within the resource group and then view the template used for a specific deployment.

So, the correct answer is B. No.



upvoted 5 times

  **[Removed]** 8 months ago

Selected Answer: A

A is correct

upvoted 1 times

  **Onang** 9 months, 2 weeks ago


A is the right answer

upvoted 1 times

  **nnamacha** 1 year ago

B could be wrong if there were changes that were manually made to the resource after the deployment. Resource Group creates a snapshot as at that time

upvoted 4 times

  **_gio_** 1 year, 3 months ago

Selected Answer: A

i think yes

upvoted 1 times

  **fiahbone** 1 year, 7 months ago

Selected Answer: A

Yes, there you'll find Deployments

upvoted 1 times

  **dhivyamohanbabu** 1 year, 10 months ago

A is correct

upvoted 1 times

  **Kt4Azure** 2 years, 1 month ago

Selected Answer: A

This is Correct. Resource Group >> Deployments

upvoted 1 times

  **jackdryan** 2 years, 2 months ago

A is correct.

upvoted 1 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: A

You should use the Resource Group blade

upvoted 2 times

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

Establish if the solution satisfies the requirements.

Your company has an azure subscription that includes a storage account, a resource group, a blob container and a file share.

A colleague named Jon Ross makes use of a solitary Azure Resource Manager (ARM) template to deploy a virtual machine and an additional Azure Storage account.

You want to review the ARM template that was used by Jon Ross.

Solution: You access the Container blade.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (100%)

d0bermannn

Highly Voted

3 years, 10 months ago

B. No, as all of us know)

upvoted 20 times

jackdryan

2 years, 2 months ago

B is correct.

You access the Resource Group blade.

upvoted 5 times

Madbo

Highly Voted

2 years ago

No, accessing the Container blade does not provide access to the ARM template used by Jon Ross to deploy the virtual machine and an additional Azure Storage account. The Container blade displays information about the blob container within the storage account, but it does not provide access to the deployment history or ARM templates.

To review the ARM template used by Jon Ross, you need to access the deployment history of the resource group where the virtual machine and additional storage account were deployed. This will show all deployments made to the resource group, including the ARM template used for the deployment.

upvoted 14 times

victorio_27

Most Recent

2 months, 3 weeks ago

Selected Answer: B

la hoja del contenedor no te proporciona para ver la VM

upvoted 1 times

[Removed]

8 months ago

Selected Answer: B

B is correct

upvoted 1 times

tashakori

1 year, 1 month ago

No is right

upvoted 1 times

gio

1 year, 3 months ago

Selected Answer: B

i think no B

upvoted 1 times

fiahbone

1 year, 7 months ago

Selected Answer: B

You has to go to resource group blade

upvoted 1 times

Olufavour

1 year, 10 months ago

The deployment was not containerised, hence the answer is NO

upvoted 1 times

dhivyamohanbabu

1 year, 10 months ago

B is correct
upvoted 1 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: B

You should use the Resource Group blade
upvoted 2 times

  **Rufusinski** 2 years, 3 months ago



Selected Answer: B

B is correct.
upvoted 1 times

  **edutchieuk** 2 years, 5 months ago


Selected Answer: B

Correct Answer: B
upvoted 1 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

To get a ARM template from deployed resources, one must go to the Resource Group Page and see\export the previously done deployments:
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/export-template-portal#export-template-after-deployment>
upvoted 3 times

  **lexxone** 2 years, 8 months ago

Correct Answer: B
upvoted 1 times

  **EmnCours** 2 years, 8 months ago


Selected Answer: B

Correct Answer: B
upvoted 2 times

  **MAKH83** 3 years, 2 months ago

Selected Answer: B

Answer is B
upvoted 1 times

  **nqthien041292** 3 years, 2 months ago

Selected Answer: B

Vote B
upvoted 2 times

Your company has three virtual machines (VMs) that are included in an availability set.
You try to resize one of the VMs, which returns an allocation failure message.
It is imperative that the VM is resized.
Which of the following actions should you take?

- A. You should only stop one of the VMs.
- B. You should stop two of the VMs.
- C. You should stop all three VMs.
- D. You should remove the necessary VM from the availability set.



Correct Answer: C


Community vote distribution

C (74%)

A (15%)

9%

 **CLagnuts**

Highly Voted 

 3 years, 10 months ago



C. Looks Correct

Stop all the VMs in the availability set. Click Resource groups > your resource group > Resources > your availability set > Virtual Machines > your virtual machine > Stop.

After all the VMs stop, resize the desired VM to a larger size.



Select the resized VM and click Start, and then start each of the stopped VMs.

upvoted 63 times

 **jackdryan** 2 years, 2 months ago

C is correct



upvoted 4 times


 **Nathan12345** 3 months, 3 weeks ago

C is correct

<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/restart-resize-error-troubleshooting#issue-error-when-resizing-an-existing-vm>

upvoted 3 times



 **MrJR**

Highly Voted 

 3 years, 7 months ago



This question is deprecated. I tested and I was able to change the size of a VM, which is in an availability set with two other VMs, without stopping any other VM. With the three VMs up you can resize any of them.

upvoted 38 times

 **vombat186** 1 month, 1 week ago

This has nothing to do deprecation. Its an issue with the underlying cluster that hosts the VMs, it may not have capacity or doesn't support the VM size you want to change to. So just because it worked in your case, does not mean it will always work in the future.



upvoted 1 times

 **CommanderBigMac** 2 years, 2 months ago

All this means is that the change in hardware was supported by whatever the availability set was running on, not that the question is deprecated.



If your VM(s) are deployed using the Resource Manager (ARM) deployment model and you need to change to a size which requires different hardware then you can resize VMs by first stopping your VM, selecting a new VM size and then restarting the VM. If the VM you wish to resize is part of an availability set, then you must stop all VMs in the availability set before changing the size of any VM in the availability set. The reason all VMs in the availability set must be stopped before performing the resize operation to a size that requires different hardware is that all running VMs in the availability set must be using the same physical hardware cluster. Therefore, if a change of physical hardware cluster is required to change the VM size then all VMs must be first stopped and then restarted one-by-one to a different physical hardware clusters.


upvoted 31 times

 **drainuzzo** 3 years, 5 months ago

But the question reported: "You try to resize one of the VMs, which returns an allocation failure message." so you can only stop all the 3 vms

upvoted 27 times

 **tangocqui010**



Most Recent 

 2 weeks, 6 days ago

Selected Answer: A

To attach a data disk from one Azure VM to another with minimal downtime, the first action you should take is to Stop the VM that includes the data disk. This is necessary because you cannot detach a data disk from a running VM. Once the VM is stopped, you can then detach the data disk and attach it to the other VM.

upvoted 1 times

  **Nepton** 1 month, 3 weeks ago

Selected Answer: C

In this case, to resolve the allocation failure when resizing a VM in an availability set, you would need to stop all the VMs in the availability set to ensure that there are no resource conflicts or issues that prevent the VM from being resized.

upvoted 1 times

  **emakid** 2 months ago

Selected Answer: C

Retry the request using a smaller VM size.

If the size of the requested VM cannot be changed:

Stop all the VMs in the availability set.

Click Resource groups > your resource group > Resources > your availability set > Virtual Machines > your virtual machine > Stop.
After all the VMs stop, resize the desired VM to a larger size.

Select the resized VM and click Start, and then start each of the stopped VMs.

Source: <https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/restart-resize-error-troubleshooting#issue-error-when-resizing-an-existing-vm>

upvoted 2 times

  **Sama5100** 4 months, 2 weeks ago

Selected Answer: C

In the event of an allocation failure, we should stop all three VMs in the availability set
<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/restart-resize-error-troubleshooting#issue-error-when-resizing-an-existing-vm>

upvoted 4 times

  **SHAHIN_STA** 4 months, 3 weeks ago

Selected Answer: D

****Answer: D. You should remove the necessary VM from the availability set.****


****Explanation:****

When a VM is part of an ****availability set****, resizing the VM can sometimes fail if there aren't sufficient resources available in the underlying hardware for the requested VM size.

In this case, the correct action would be to ****remove the VM from the availability set****, which allows resizing without being constrained by the availability set's resource allocation. After resizing, you can add the VM back into the availability set.

Simply stopping the VMs (Options A, B, and C) doesn't resolve the allocation failure, as the issue lies with the available resources in the set, not with whether the VMs are running or stopped.

upvoted 2 times

  **58b2872** 4 months, 1 week ago

GPT hhahahahahah

upvoted 1 times

  **RajeshwaranM** 4 months, 2 weeks ago

Can I replicate the issue on my end? I really wanna test this scenario

upvoted 1 times

  **MaDota** 5 months ago

Selected Answer: C

most important part of the question is: ".....which returns an allocation failure message"

In this situation Stopping all the VMs in the availability set helps free up enough resources to allow the resizing operation to succeed

upvoted 1 times

  **FritsB** 5 months, 1 week ago

Selected Answer: A

Just tested it in my lab. I created an availability set, added 3 VM's. Stopped VM1 and resized it and started it again. No issues.

upvoted 5 times

  **58b2872** 4 months, 1 week ago

Because you have enough hardware resources, bro, no allocation failure message...

upvoted 1 times

  **RajeshwaranM** 4 months, 2 weeks ago

Did you get the allocation failure while you increased space for the VM?

upvoted 1 times



  **JPA210** 6 months ago

Selected Answer: A

Check down Mr JR answer.
upvoted 1 times

  **JPA210** 6 months ago

Commanderbignmac and drainuzzo gave a very good reply to him, so I change my vote to C.
upvoted 1 times

  **Ayb_FNZ** 6 months, 1 week ago



Answer is C.

We have to understand the allocation failure error. When we create an availability set, all the mVMs are created within the same data center in specific racks (depends on the fault and update domains). When we resize, ARM looks for enough capacity to allocate 3 times the new size. If there is no enough compute capacity, it send s back an error. We have to stop all the VMs (aka deallocate) so they can be allocated on another rack where capacity is available for the 3 VMs (aka 3 times the new desired size)
upvoted 4 times

  **[Removed]** 8 months ago

Selected Answer: C

C is correct
upvoted 3 times

  **[Removed]** 8 months, 4 weeks ago

C: should Stop all the VMs in the availability set' as per
<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/restart-resize-error-troubleshooting>
upvoted 4 times

  **3c5adce** 11 months, 4 weeks ago

C. You should stop all three VMs.

Stopping all VMs in the availability set can help with the reallocation of resources, making it possible to resize the VM by potentially moving it to a different hardware cluster where the desired VM size is available.
upvoted 1 times

  **18c2076** 1 year, 1 month ago

C is correct.

Key context here is the allocation failure

“When you try to start a stopped Azure Virtual Machine (VM), or resize an existing Azure VM, the common error you encounter is an allocation failure. This error results when the cluster or region either does not have resources available or cannot support the requested VM size”
<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/restart-resize-error-troubleshooting>
upvoted 1 times

  **abhikeshu** 1 year, 2 months ago

Selected Answer: D

Option 3 suggests stopping all three VMs. While stopping all VMs might temporarily free up resources within the availability set, it is not the most targeted or efficient solution to address the allocation failure during VM resizing. Additionally, stopping all VMs would disrupt the availability of services running on those VMs, which may not be acceptable in a production environment.

Removing only the necessary VM from the availability set, as suggested in option D, allows for a more surgical approach. It addresses the allocation failure specifically for the VM that needs resizing while minimizing disruption to other VMs in the availability set. Once the necessary VM is resized, it can be added back to the availability set to restore its high availability and redundancy features. This approach is more targeted and focused on resolving the specific issue at hand without unnecessary disruption to other resources.
upvoted 2 times

  **TheFivePips** 9 months, 1 week ago

I was wondering this too. Chat GPT said this: If you want to add the VM back into the availability set after resizing, this is not directly supported. You would need to delete the VM (keeping its disks) and recreate it within the availability set, which involves downtime and additional configuration.
upvoted 1 times

  **TheFivePips** 9 months, 1 week ago

Further explanation: Virtual machines (VMs) must be created within an availability set from the beginning; you cannot add an existing VM to an availability set. This is because the placement of VMs within an availability set is determined at the time of their creation to ensure they are distributed across multiple fault and update domains to provide high availability.
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

C is correct
upvoted 1 times

You have an Azure virtual machine (VM) that has a single data disk. You have been tasked with attaching this data disk to another Azure VM. You need to make sure that your strategy allows for the virtual machines to be offline for the least amount of time possible. Which of the following is the action you should take FIRST?

- A. Stop the VM that includes the data disk.
- B. Stop the VM that the data disk must be attached to.
- C. Detach the data disk.
- D. Delete the VM that includes the data disk.

Correct Answer: C

Community vote distribution

C (80%)A (19%)

- jecawi9630**

Highly Voted

3 years, 10 months ago

Wrong. You can simply detach a data disk from one VM and attach it to the other VM without stopping either of the VMs.

upvoted 252 times
- Sledgehammer**

1 week, 3 days ago

C is correct. I work with data disks on regular bases and it is a blessing that this can be moved over to another VM without having to stop any VM first.

upvoted 1 times
- Dankho**

6 months, 2 weeks ago

Right, not wrong!

upvoted 2 times
- jackdryan**

2 years, 2 months ago

C is correct

upvoted 5 times
- jjnelo**

3 years, 9 months ago

Correct. Just tested in lab.

upvoted 10 times
- FunAJ**

Highly Voted

3 years ago

Selected Answer: A

Stop the VM first so that disk data is not corrupted (if an service is writing data while you detach)

upvoted 23 times
- uwhm2b5fz**

5 months, 1 week ago

detaching the disk is the correct option to satisfy the requirement of least amount of time possible. You can verify no disk activity before doing so so stopping the VM is not the correct answer.

upvoted 4 times
- areyoushawtho**

9 months ago

"allows for the virtual machines to be offline for the least amount of time possible." Detaching means no offline time, weather its better to or now

upvoted 2 times
- Sholasleek**

6 months ago

It also says which action should you take first? FUnAJ is correct, stopping the VM to avoid disk errors.

upvoted 1 times
- ty064**

7 months ago

It says least amount of time possible, it doesn't say least amount of time ever. So least amount of time with best results

upvoted 3 times
- karrey**

2 years, 1 month ago

Makes sense but not needed according to MSF

upvoted 1 times
- klasbeatz**

2 years, 8 months ago

This makes the most sense but apparently stopping the VM isn't needed according to Microsoft documentation

upvoted 14 times

  **Kirby87** Most Recent 2 weeks, 5 days ago

Selected Answer: A

ere's the correct sequence:

- ☒ Stop (deallocate) the VM the data disk is currently attached to (Option A).
- ☒ Then, detach the disk (Option C).
- ☒ Attach the disk to the other VM.
- ☒ Start the VMs as needed.

So while Option C is a required step, it can't be the first step — you have to stop the VM first.

upvoted 1 times

  **andted98** 1 month ago

Selected Answer: C

The question didn't specify whether the data disk is used for OS so since it can be an external attachable data disk, it can be detached without the need to shutdown the VM.

upvoted 1 times

  **azuredbaadmin** 3 months, 1 week ago

Selected Answer: A

To ensure that the virtual machines are offline for the least amount of time possible, the first action you should take is to stop the VM that includes the data disk. This will allow you to safely detach the data disk and then attach it to the other Azure VM.

Here are the steps you should follow:



Stop the VM that includes the data disk: This ensures that the data disk can be safely detached without any data corruption.

Detach the data disk: Once the VM is stopped, you can detach the data disk from the VM.

Attach the data disk to the other VM: After detaching, you can attach the data disk to the target VM.

Start both VMs: Finally, start both VMs to bring them back online.

upvoted 1 times

  **AnilParadhe** 3 months, 4 weeks ago

Selected Answer: A

A. Stop the VM that includes the data disk.

Azure does not allow detaching a data disk from a running VM. You must first stop the VM to detach the disk safely.

upvoted 2 times

  **RajeshwaranM** 4 months, 2 weeks ago

Selected Answer: C

C is the correct option. I tried to detach the data disk from VM1 to VM2 without shutting down either of them. The only thing you need to consider is that while you detach the data disk, you need to ensure that the data disk is not being used by any service or operation.



upvoted 4 times

  **Jig77** 5 months, 3 weeks ago

De-attach the data disk from the current VM:

To attach a data disk from one Azure VM to another, you must first detach the disk from the current VM. The disk must not be in use by the original VM when it is being attached to a different VM. This process can be done without shutting down the VM itself, minimizing downtime.

upvoted 1 times

  **LaReis** 6 months, 3 weeks ago

Segundo o Copilot: Você

Você tem uma máquina virtual (VM) do Azure que tem um único disco de dados. Você foi encarregado de anexar esse disco de dados a outra VM do Azure.

Você precisa ter certeza de que sua estratégia permite que as máquinas virtuais fiquem offline pelo menor tempo possível.



Qual das seguintes é a ação que você deve tomar PRIMEIRO?

- A. Pare a VM que inclui o disco de dados.
- B. Pare a VM à qual o disco de dados deve ser conectado.
- C. Retire o disco de dados.
- D. Exclua a VM que inclui o disco de dados.

Copilot

A. Pare a VM que inclui o disco de dados. Primeiro, pare a VM que atualmente possui o disco de dados para desconectá-lo com segurança. Isso minimizará o tempo de inatividade das VMs.

upvoted 1 times

  **asuares** 7 months, 1 week ago

Selected Answer: A

To ensure the virtual machines are offline for the least amount of time possible, the first action you should take is to stop the VM that includes the data disk (Option A). This step is necessary to safely detach the data disk without risking data corruption1.

upvoted 1 times

🗨️ 👤 **Kalaiarasu** 7 months, 1 week ago

Answer is A since the strategy allows for the virtual machines to be offline for the least amount of time possible
upvoted 1 times

🗨️ 👤 **kejo2** 7 months, 1 week ago

Just tested this in my lab. C is the correct answer: you will need to detach the disk before you can add it to another vm
upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago

Selected Answer: C

it's C
upvoted 1 times

🗨️ 👤 **Davidsv** 8 months, 1 week ago

Selected Answer: C

I made a experiment: 2 VM's in one region in 2 zones (zone 1 and zone 2). And i can say thats you dont need to turn off virtual machine at all!
Create a disk in 1 VM, attach. Now you can see that you can attach Disk on VM when its on. Deattach and you gonna see that's you dont need to turn off VM to do it. Make snapshot of disk, after that do a new disk that gonna take data from snapshot and make it in 2 zone (or in zone 1 if you deattach from VM in zone 2). After creating go to VM2 disk and attach a new disk. You can do it without turning off VM2. And thats a miracle!
Disk2 has been attached! So answer C is complitely correct. If you don't trust my try it by yourself and you will see
upvoted 4 times

🗨️ 👤 **[Removed]** 8 months, 4 weeks ago

answer is 'C' :

When you no longer need a data disk that's attached to a virtual machine, you can easily detach it. This removes the disk from the virtual machine, but doesn't remove it from storage.
upvoted 1 times

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

Selected Answer: C

I dont like this question. It is possible to hot swap the disk, but it is not a best practice. Best answer is still C
upvoted 4 times

🗨️ 👤 **Mixxy1010** 9 months, 2 weeks ago

if its not the Primary disk you should be able to detach the disk without stopping the VM - Voting C
upvoted 1 times

Your company has an Azure subscription.

You need to deploy a number of Azure virtual machines (VMs) using Azure Resource Manager (ARM) templates. You have been informed that the VMs will be included in a single availability set.

You are required to make sure that the ARM template you configure allows for as many VMs as possible to remain accessible in the event of fabric failure or maintenance.

Which of the following is the value that you should configure for the platformFaultDomainCount property?

- A. 10
- B. 30
- C. Min Value
- D. Max Value

Correct Answer: D

Community vote distribution

D (100%)

ppp131176

Highly Voted

3 years, 10 months ago

D is correct. 2 or 3 is max for a region so answer should be Max.
upvoted 30 times

jackdryan

2 years, 2 months ago

D is correct.
upvoted 1 times

maqibali

Highly Voted

2 years, 1 month ago

Selected Answer: D

The platformFaultDomainCount property specifies the number of fault domains to be used by the availability set. A fault domain is a group of underlying hardware resources in a data center that share a common power source and network switch, but are physically separated from each other. By distributing virtual machines across fault domains, you can ensure that no single point of failure can take down all of the virtual machines at once.

In Azure, the maximum value for platformFaultDomainCount is 3. This means that an availability set can have up to 3 fault domains. The minimum value for platformFaultDomainCount is 1.

To make sure that the ARM template allows for as many VMs as possible to remain accessible in the event of fabric failure or maintenance, you should set the platformFaultDomainCount property to its maximum value of 3.

So the correct answer is:

D. Max Value
upvoted 28 times

othiagopadua

Most Recent

3 weeks, 1 day ago

Selected Answer: D

O Azure espalha suas VMs automaticamente entre os domínios disponíveis.
O objetivo é usar o valor máximo possível de domínios de falha, para garantir alta disponibilidade, dessa forma ganhamos operabilidade, a D é a melhor opção
upvoted 1 times

ADIT12345

3 months ago

Selected Answer: D

D correct
upvoted 1 times

Bikth

3 months, 1 week ago

Selected Answer: D

The platformFaultDomainCount property in an Azure Availability Set specifies the number of fault domains for the virtual machines. Fault domains are essentially physical groupings of resources that provide isolation from hardware failures, power outages, or network issues.

Azure allows for a maximum of 3 fault domains in most regions (and up to 2 fault domains in some regions like classic cloud regions). Configuring the maximum value ensures that VMs are distributed across the greatest number of fault domains possible, maximizing their availability during fabric failures or maintenance events.



Key Notes:

Min Value: Would reduce fault tolerance, as all VMs could end up in a single fault domain.
Max Value: Ensures the highest fault tolerance by spreading VMs across all available fault domains.
10 and 30: These values are not valid, as the maximum fault domain count is 3 in Azure (or 2 in specific regions).
upvoted 1 times

  **Mark74** 5 months ago

Selected Answer: D

Max value
upvoted 1 times

  **monisshk** 5 months, 3 weeks ago



Selected Answer: D

To ensure that as many VMs as possible remain accessible in the event of fabric failure or maintenance, you should configure the platformFaultDomainCount property to the maximum value. Therefore, the correct answer is:

D. Max Value

This setting helps distribute the VMs across multiple fault domains, reducing the risk of simultaneous failures.



upvoted 2 times

  **LaReis** 6 months, 3 weeks ago

C. Valor mínimo. Ao configurar a propriedade platformFaultDomainCount, escolher o valor mínimo maximiza a resiliência das VMs em um conjunto de disponibilidade. Isso minimiza a quantidade de VMs impactadas em caso de falha de malha ou manutenção.

Segundo o Copilot: C. Valor mínimo. Ao configurar a propriedade platformFaultDomainCount, escolher o valor mínimo maximiza a resiliência das VMs em um conjunto de disponibilidade. Isso minimiza a quantidade de VMs impactadas em caso de falha de malha ou manutenção.

upvoted 1 times

  **LaReis** 6 months, 3 weeks ago

Segundo o Copilot: C. Valor mínimo. Ao configurar a propriedade platformFaultDomainCount, escolher o valor mínimo maximiza a resiliência das VMs em um conjunto de disponibilidade. Isso minimiza a quantidade de VMs impactadas em caso de falha de malha ou manutenção.

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: D

D is correct
upvoted 1 times

  **jairoaquinterov** 1 year ago

Selected Answer: D

Each virtual machine in your availability set is assigned an update domain and a fault domain by the underlying Azure platform. Each availability set can be configured with up to 3 fault domains and 20 update domains.


However 20 is not in options, the correct answer is D

upvoted 4 times

  **jairoaquinterov** 1 year ago

Is tree sorry. 3 fault domains. 3 is not in answers then option is D

upvoted 1 times



  **MCLC2021** 1 year, 1 month ago

CORRECT ANSWER D (Max Value)

You can set the property properties.platformFaultDomainCount to 1, 2, or 3 (default of 1 if not specified).

<https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-manage-fault-domains>

upvoted 2 times

  **pc1707** 1 year, 2 months ago



Selected Answer: D

@mattpaul why are you creating a new examtopics.com and that too a paid version? please join us here provide your feedback for free.

upvoted 3 times

  **Amir1909** 1 year, 2 months ago

D is correct
upvoted 1 times

  **_gio_** 1 year, 2 months ago

Selected Answer: D

i think D
upvoted 1 times

  **jhothanan** 1 year, 2 months ago

Selected Answer: D

D es correcto

upvoted 2 times

  **Saurabh_Bhargav** 1 year, 2 months ago

D is correct , Max fault domain is 3 so that option is not available so i will go with max
upvoted 1 times

Your company has an Azure subscription.

You need to deploy a number of Azure virtual machines (VMs) using Azure Resource Manager (ARM) templates. You have been informed that the VMs will be included in a single availability set.

You are required to make sure that the ARM template you configure allows for as many VMs as possible to remain accessible in the event of fabric failure or maintenance.

Which of the following is the value that you should configure for the platformUpdateDomainCount property?

- A. 10
- B. 20
- C. 30
- D. 40

Correct Answer: B

Community vote distribution

B (98%)

tubby04

Highly Voted

3 years, 7 months ago

Correct answer is B. 20

'Each virtual machine in your availability set is assigned an update domain and a fault domain by the underlying Azure platform. Each availability set can be configured with up to three fault domains and twenty update domains.'

<https://docs.microsoft.com/en-us/azure/virtual-machines/availability-set-overview>

upvoted 114 times

jackdryan

2 years, 2 months ago

B is correct

upvoted 2 times

Pradh

Highly Voted

3 years, 6 months ago

Admin of this Website ... Please Update the answer to "B" .

its giving negative impact on people who think of buying Contributor Access seeing such mistakes .

upvoted 76 times

creeped

3 years, 1 month ago

this is the way the site is suppose to run because if this site give all the correct answers then MS will shut it down. that is why you need to read the discussions and analyze the answer by yourself.

upvoted 18 times

Mentalfloss

2 years, 7 months ago

Really? Is that how sites like this exist? I had assumed just being out of the country was enough. Wutever. This is my first time back in 18 months and the new comment voting system is DA BOMB! lol

upvoted 6 times

ki01

1 year, 4 months ago

i started thinking the same, if they had only current questions and 100% correct answers MS might sue them. and if they are out of country MS could petition backbone companies to block/remove the site. that's why you see some websites changing domains almost monthly like .to .is. net. .cc and etc. cloudflare received complains about 35k domains in 2021 and actioned a significant amount of them. so the old times of needing to nuke the website itself are gone.

upvoted 1 times

othiagopadua

Most Recent

3 weeks, 1 day ago

Selected Answer: B

20 Correto. É o maior valor configurável atualmente. são 20 Update Domains.

upvoted 1 times

himanshu007007

2 months ago

Selected Answer: A

In an Azure Availability Set, update domains (UDs) help ensure that virtual machines (VMs) remain accessible during planned maintenance.

The platformUpdateDomainCount property defines the number of update domains within an availability set.

Update domains help distribute VMs so that Azure does not restart all VMs at once during maintenance. The maximum number of update domains supported in Azure is 20, but the default is 5, and the recommended value is 10 for most cases.

upvoted 1 times



  **sivv** 3 months, 1 week ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview#how-do-availability-sets-work>

The underlying Azure platform assigns an update domain and a fault domain to each virtual machine in your availability set. Each availability set can have up to 3 fault domains and 20 update domains. You can't change these configurations after you create the availability set.

upvoted 1 times

  **sholguin** 3 months, 1 week ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview>

How do availability sets work?

The underlying Azure platform assigns an update domain and a fault domain to each virtual machine in your availability set. Each availability set can have up to 3 fault domains and 20 update domains. You can't change these configurations after you create the availability set.

upvoted 1 times

  **Jaiiee** 5 months ago

Selected Answer: B

How do availability sets work?

The underlying Azure platform assigns an update domain and a fault domain to each virtual machine in your availability set. Each availability set can have up to 3 fault domains and 20 update domains. You can't change these configurations after you create the availability set.

upvoted 1 times

  **Mark74** 5 months ago

Selected Answer: B

B , 20

upvoted 1 times

  **sreyanchoudhury** 5 months, 1 week ago

Selected Answer: B

It should be set to the max possible value, which is 20 for an availability set.

upvoted 1 times

  **Jig77** 5 months, 3 weeks ago

Answer is A. To maximize VM availability during maintenance and minimize downtime in the event of fabric failure, you should configure the platformUpdateDomainCount property to 10 (Option A). This will distribute your VMs across 10 update domains, ensuring that as many VMs as possible remain unaffected during planned maintenance and providing optimal availability.

upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct



upvoted 1 times

  **[Removed]** 8 months, 4 weeks ago

Answer is B, it specifically mentions the domain max count;

"Each virtual machine in your availability set is assigned an update domain and a fault domain by the underlying Azure platform. Each availability set can be configured with up to 3 fault domains and 20 update domains. These configurations can't be changed once the availability set has been created. source- <https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview>

upvoted 3 times

  **Deepu_s** 11 months, 2 weeks ago

Selected Answer: B

Each availability set can be configured with up to three fault domains and twenty update domains

upvoted 2 times

  **MCLC2021** 1 year, 1 month ago

CORRECT ANSWER B (20)

Each availability set can be configured with up to 3 fault domains and 20 update domains.


<https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview>

upvoted 1 times

  **tashakori** 1 year, 1 month ago

B is correct

upvoted 1 times

  **_gio_** 1 year, 2 months ago

Selected Answer: B

max number of update domains is 20

upvoted 1 times

  **Saurabh_Bhargav** 1 year, 2 months ago

B. 20

Because the maximum value that i can have from the update domain is 20.

upvoted 1 times

DRAG DROP -

You have downloaded an Azure Resource Manager (ARM) template to deploy numerous virtual machines (VMs). The ARM template is based on a current VM, but must be adapted to reference an administrative password.

You need to make sure that the password cannot be stored in plain text.

You are preparing to create the necessary components to achieve your goal.

Which of the following should you create to achieve your goal? Answer by dragging the correct option from the list to the answer area.

Select and Place:

Options

Answer

- An Azure Key Vault
- An Azure Storage account
- Azure Active Directory (AD) Identity Protection
- An access policy
- An Azure policy
- A backup policy

Options

Answer

Correct Answer:

An Azure Key Vault

An Azure Storage account

Azure Active Directory (AD)
Identity Protection

An access policy




An Azure policy



A backup policy



An Azure Key Vault




An access policy




You can use a template that allows you to deploy a simple Windows VM by retrieving the password that is stored in a Key Vault. Therefore, the password is never put in plain text in the template parameter file.



  **pakman** Highly Voted  3 years, 7 months ago
Key vault + access policy
upvoted 84 times



  **jackill** 1 year, 9 months ago
I agree : key vault + access policy
But please note that now the access policy is considered a legacy way to provide access to the key vault. Now you can use RBAC.
upvoted 41 times



  **jackdryan** 2 years, 2 months ago
This is correct.
upvoted 5 times

  **Mazinger** Highly Voted  7 months, 2 weeks ago
The two components you should create to achieve your goal are:
1. An Azure Key Vault: you can store the administrative password in an Azure Key Vault, which provides secure storage and management of cryptographic keys, certificates, and secrets. Storing the password in a Key Vault ensures that it is not stored in plain text and provides an additional layer of security to protect the password.
2. An access policy: You should create an access policy to control access to the Key Vault secrets. An access policy specifies who can perform operations on the secrets stored in the Key Vault. You can grant permissions to users, applications, and services to access the Key Vault and its secrets, and you can specify the level of access that they have. By creating an access policy, you can control who has access to the administrative password and ensure that it is used only by authorized entities.
Therefore, to achieve your goal, you should create an Azure Key Vault to store the administrative password, and an access policy to control access to the Key Vault secrets.
upvoted 29 times

  **[Removed]** Most Recent  7 months, 3 weeks ago
CORRECT
upvoted 1 times

  **CheMetto** 9 months, 1 week ago
Be carefull, Accesspolicy is legacy, now we have RBAC. If they replace it with RBAC, you know this is the correct answer
upvoted 6 times

  **tashakori** 1 year, 1 month ago
Given answer is right
upvoted 1 times

  **_gio_** 1 year, 2 months ago

Key vault + access policy

upvoted 1 times

  **Aldair66** 1 year, 3 months ago



I think is B

upvoted 1 times

  **D1nk8887** 1 year, 4 months ago

The question says "You need to make sure that the password cannot be stored in plain text," not how do you set it up so it's not stored in plain text.

upvoted 3 times

  **Yuraq** 1 year, 6 months ago

Key Vault and Access Policy

Securely Deploy Azure VM With Local Admin Password from Azure Key Vault and not in ARM Template.

upvoted 5 times

  **fiahbone** 1 year, 7 months ago

Azure key vault to store the password and Access policy to make it accessible.

<https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts>

upvoted 6 times

  **havoc2k7** 1 year, 7 months ago

i love it when i find simplest exact answers

upvoted 3 times

  **SeregonAzDev** 1 year, 9 months ago

The question states "option", not "options". Based on the text I assume there is only one correct answer. In this case I would go with the Key Vault

upvoted 4 times

  **kamalpur** 1 year, 9 months ago



This question is explained in below youtube video.

upvoted 7 times

  **xRiot007** 1 year, 11 months ago

If you need to store stuff securely, you should use an Azure Key Vault and store it as key-value, where the key is a string and the value can be anything. To access the keyvault data you need an Access Policy taht defines who has access to the vault.

upvoted 7 times

  **LCR** 1 year, 11 months ago

This whole answers/grid situation is confusing.

upvoted 3 times

  **Madbo** 2 years ago

The two components that should be created to achieve the goal of storing an administrative password securely are:

An Azure Key Vault, which can securely store and manage cryptographic keys, certificates, and passwords. The password can be stored as a secret in the Key Vault and then accessed by the ARM template using a reference to the Key Vault.

An access policy, which is used to define who has permissions to access and manage the Key Vault. This is important to ensure that only authorized users can access the password stored in the Key Vault.

upvoted 13 times

  **GohanF2** 2 years, 1 month ago

answer is correct, plus this question appears in the MS free Assessment exam in MS page for this course.

upvoted 3 times

  **Chandra415** 2 years, 3 months ago

Key Vault & Access Policy

upvoted 3 times

Your company has an Azure Active Directory (Azure AD) tenant that is configured for hybrid coexistence with the on-premises Active Directory domain.

The on-premise virtual environment consists of virtual machines (VMs) running on Windows Server 2012 R2 Hyper-V host servers.

You have created some PowerShell scripts to automate the configuration of newly created VMs. You plan to create several new VMs.

You need a solution that ensures the scripts are run on the new VMs.

Which of the following is the best solution?

- A. Configure a SetupComplete.cmd batch file in the %windir%\setup\scripts directory.
- B. Configure a Group Policy Object (GPO) to run the scripts as logon scripts.
- C. Configure a Group Policy Object (GPO) to run the scripts as startup scripts.
- D. Place the scripts in a new virtual hard disk (VHD).

Correct Answer: A

Community vote distribution

A (53%)C (47%)

  **j5y**



Highly Voted

 7 months, 2 weeks ago

Ans: A


After Windows is installed but before the logon screen appears, Windows Setup searches for the SetupComplete.cmd file in the %WINDIR%\Setup\Scripts\ directory

upvoted 83 times

  **jackdryan** 2 years, 2 months ago

A is correct.

upvoted 4 times

  **NaoVaz**

Highly Voted

 2 years, 7 months ago



Selected Answer: A

GPOs aren't a thing in Azure AD.

Just putting a Script inside the VHD doesn't make it run on boot.



Configuring a "SetupComplete.cmd" in the "%windir%\setup\scripts" directory is the correct approach:

upvoted 22 times

  **BWLZ** 2 months, 1 week ago

the newly created VMs are on-prem not on Azure AD , you are wrong , answer is C

upvoted 1 times

  **MdHussain**

Most Recent

 4 days, 2 hours ago

Selected Answer: C



Given your scenario, the best solution would be:

C. Configure a Group Policy Object (GPO) to run the scripts as startup scripts.

- Here's why:
- 1.Startup scripts are executed when the machine boots up, ensuring that the configuration scripts run before any user logs in. This is particularly useful for setting up system-level configurations that need to be in place before the VM is fully operational.
 - 2.Logon scripts (option B) run when a user logs in, which might not be ideal for initial VM setup tasks.
 - 3.SetupComplete.cmd (option A) is typically used for tasks that need to be performed after Windows Setup completes, but it might not cover all scenarios for ongoing VM creation and configuration.
 - 4.Placing scripts in a new VHD (option D) is not a standard method for ensuring scripts run automatically on new VMs.

Configuring a GPO for startup scripts provides a reliable and centralized way to manage and automate the execution of your PowerShell scripts across multiple VMs.

upvoted 1 times

  **AKoselnik** 1 week ago

Selected Answer: A

For me the answer is A. The machine to login to the domain needs to be register in the domain that the GPO will be working. For me Put the script in the location will start them automatically. Independence on login to the domain or not.



upvoted 1 times

  **ryof** 1 month, 1 week ago

Selected Answer: A

The best solution in this scenario would be A: Configure a SetupComplete.cmd batch file in the %windir%\setup\scripts directory. This method ensures that your PowerShell scripts are automatically executed after the Windows setup process is complete, making it ideal for automating the configuration of newly created VMs. The SetupComplete.cmd file runs immediately after the Windows installation is finalized and before the system restarts, allowing you to automate tasks like running your scripts without needing manual intervention. Options B and C (Group Policy Objects for logon or startup scripts) might not be ideal in this case, as they depend on user logons or startup events, which can introduce delays or inconsistencies, especially in environments where VMs are being rapidly deployed. Option D (placing scripts in a new VHD) is not specifically designed for automating VM configuration; it would involve additional steps for accessing and executing the scripts.

upvoted 1 times

  **entidad** 1 month, 3 weeks ago

Selected Answer: C

Los startup scripts se ejecutan antes de que cualquier usuario inicie sesión, asegurando que la configuración se aplique correctamente a todas las nuevas VMs cuando se inician. Además, este enfoque se administra centralmente desde Active Directory, lo que facilita la aplicación en múltiples máquinas.

upvoted 1 times



  **alinuxguru70** 1 month, 3 weeks ago

Selected Answer: A

You have created some PowerShell scripts to automate the configuration of newly created VMs. You need a solution that ensures the scripts are run on the new VMs.

There is nothing to imply that the script needs to be run on every startup. Therefore there is no reason to use a GPO. SetupComplete.cmd would be the appropriate answer.

upvoted 1 times

  **Ivanvazovv** 1 month, 3 weeks ago

Selected Answer: A

Nowhere in the question is written that the new VMs will be domain joined. So GPO may not be an option at all.

upvoted 1 times

  **Abhisk127** 2 months ago

Selected Answer: C

The best solution is C. Configure a Group Policy Object (GPO) to run the scripts as startup scripts. This ensures that the PowerShell scripts are executed when the VMs start up, automating the configuration process effectively


upvoted 1 times

  **Ponpon3185** 2 months, 1 week ago

Selected Answer: A

I think A because here: <https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-a-custom-script-to-windows-setup?view=windows-11> you could find this: "If the computer joins a domain during installation, the Group Policy that is defined in the domain is not applied to the computer until Setupcomplete.cmd is finished. This is to make sure that the Group Policy configuration activity does not interfere with the script."

upvoted 1 times

  **nnamacha** 2 months, 2 weeks ago

Selected Answer: A


Microsoft Entra ID does not support traditional Group Policy Objects (GPOs) like Active Directory Domain Services (AD DS). GPOs are a legacy feature of on-premises Active Directory environments,

upvoted 2 times

  **victorio_27** 2 months, 3 weeks ago

Selected Answer: C

Para asegurarse de que los scripts de PowerShell se ejecuten automáticamente en las nuevas VM y configuren el sistema correctamente, la mejor opción es usar un GPO configurado para ejecutar los scripts como scripts de inicio.

 Opción correcta: C. Configure un objeto de política de grupo (GPO) para ejecutar los scripts como scripts de inicio.

upvoted 1 times

  **chandiochan** 2 months, 3 weeks ago

Selected Answer: C

The SetupComplete.cmd mechanism is executed during Windows Setup after installation completes. This is useful for initial image configuration but is less flexible if you plan to use an already prepared image or if the VMs are deployed in various scenarios over time.

Since your environment is domain-joined (as indicated by the hybrid coexistence with on-premises Active Directory) and you're creating multiple new VMs, using a GPO with startup scripts is a centralized and scalable way to ensure your configuration scripts run automatically on each new VM.

upvoted 2 times



  **lioroz** 2 months, 3 weeks ago

Selected Answer: C

The best solution in this scenario is to configure a Group Policy Object (GPO) to run the scripts as startup scripts. This ensures that the PowerShell scripts are executed when the virtual machines start up, automating the configuration process.

So the correct answer is C. Configure a Group Policy Object (GPO) to run the scripts as startup scripts.

upvoted 1 times

  **Cruzito** 2 months, 3 weeks ago

Selected Answer: C

he best solution is C. Configure a Group Policy Object (GPO) to run the scripts as startup scripts.

Configuring a GPO to run the scripts as startup scripts ensures that the scripts are executed when the VMs start up, which is ideal for automating the configuration of newly created VMs. This method is reliable and integrates well with the existing Active Directory environment.

Option A, configuring a SetupComplete.cmd batch file in the %windir%\setup\scripts directory, is a valid method for running scripts during the setup process of Windows. However, it is typically used for tasks that need to be executed once during the final stages of the Windows setup process, rather than for ongoing configuration tasks.

upvoted 1 times

  **jeff1988** 3 months ago

Selected Answer: C

C. Configure a Group Policy Object (GPO) to run the scripts as startup scripts.

Here's why:



Startup scripts run when the computer starts, before any user logs on. This ensures that the scripts are executed as soon as the VM is powered on and before any user interaction.

Logon scripts (option B) run when a user logs on, which means the scripts would only execute after a user logs in, potentially delaying the configuration.

SetupComplete.cmd (option A) is used during the Windows setup process, but it is not as flexible or manageable as GPOs for ongoing VM management.

Placing scripts in a new VHD (option D) is not a standard method for ensuring scripts run automatically on new VMs.

upvoted 1 times

  **zhorj1kuee** 3 months, 3 weeks ago

Selected Answer: A

Rationale:

The SetupComplete.cmd file is executed immediately after the operating system setup is complete, ensuring that the scripts are run on the new virtual machines as part of their initial configuration. This solution is both direct and efficient for automating the configuration of freshly created VMs.

Why not the others?

B: Logon scripts via GPO: These run only when a user logs in. For automating initial configurations on new VMs, this is neither timely nor appropriate.

C: Startup scripts via GPO: While they run during the computer's startup, GPOs require the machine to already be part of the Active Directory domain, which is not guaranteed for new VMs during initial setup.

D: Scripts in a new VHD: While theoretically possible, this approach is cumbersome and lacks the streamlined execution of the SetupComplete.cmd method.

upvoted 2 times

Your company has an Azure Active Directory (Azure AD) tenant that is configured for hybrid coexistence with the on-premises Active Directory domain.

You plan to deploy several new virtual machines (VMs) in Azure. The VMs will have the same operating system and custom software requirements.

You configure a reference VM in the on-premise virtual environment. You then generalize the VM to create an image.

You need to upload the image to Azure to ensure that it is available for selection when you create the new Azure VMs.

Which PowerShell cmdlets should you use?

- A. Add-AzVM
- B. Add-AzVhd
- C. Add-AzImage
- D. Add-AzImageDataDisk

Correct Answer: B

Community vote distribution

B (89%)

11%

- NaoVaz**

Highly Voted

7 months, 2 weeks ago

Selected Answer: B

"New-AzVM" is for creating new VMs, not uploading images.

"Add-AzImage" does not exist. the correct command is "New-AzImage".

"Add-AzImageDataDisk" Adds a data disk to an image object.

"Add-AzVhd" seems to be the correct option, sing the it "Uploads a virtual hard disk from an on-premises machine to Azure (managed disk or blob)." (<https://docs.microsoft.com/en-us/powershell/module/az.compute/add-azvhd?view=azps-8.3.0>)

upvoted 79 times
- margotfrpp**

2 years ago

this command exist " Add-AzImage"

<https://learn.microsoft.com/en-us/powershell/module/az.compute/new-azimage?view=azps-9.6.0>

upvoted 2 times
- Dankho**

6 months, 2 weeks ago

how does a person from 1 year, 6 months ago reply to someone from 4 weeks, 1 day ago. Riddle me that...

upvoted 27 times
- mirajkumar**

4 months ago

Time Travel exits

upvoted 3 times
- jersonmartinez**

2 years ago

It command does not exists. It only exist `New-AzImage`. That's different.

upvoted 13 times
- Chi1987**

Highly Voted

3 years, 7 months ago

Correct answer.

Example for how you do this:

Add-AzVhd -ResourceGroupName \$resourceGroup -Destination \$urlOfUploadedImageVhd `

-LocalFilePath \$localPath

upvoted 52 times
- jackdryan**

2 years, 2 months ago

B is correct.

upvoted 3 times
- lumax007**

Most Recent



1 month, 2 weeks ago

Selected Answer: C

Add-AzImage add/upload image to resource manager

<https://learn.microsoft.com/en-us/powershell/module/az.compute/new-azimage?view=azps-13.3.0>

upvoted 1 times

  **0a92195** 2 months, 1 week ago

Selected Answer: C

C. Add-AzImage

Explanation:

Since you generalized the VM to create an image, you need to upload it to Azure as a managed image.

Add-AzImage is the PowerShell cmdlet used to add a VM image to Azure, making it available for creating new VMs.



Why Not the Other Options?

A. Add-AzVM → This is used to create a VM, not to upload an image.

B. Add-AzVhd → Used for uploading a VHD file, but does not create an image from it.

D. Add-AzImageDataDisk → Used to add a data disk, not a VM image.

upvoted 2 times

  **ea4b48e** 2 months, 3 weeks ago

Selected Answer: C

By using Add-AzImage, you ensure that the image is available for selection when creating new Azure VMs.

upvoted 1 times

  **SolimanAlali** 2 months, 3 weeks ago

Selected Answer: C

To upload a generalized VM image and make it available for deployment in Azure, we need to use Add-AzImage.

This cmdlet allows to register a VM image in Azure Compute Gallery (formerly Shared Image Gallery) or in the subscription's image repository.

After we generalize the reference VM using Sysprep (Windows), we need to follow these steps:

1- Capture the image:

* For Azure VMs, use Save-AzVmImage.

* For on-premises VMs, create a VHD and upload it.

2- Upload the VHD to an Azure Storage account.

3- Create an image using Add-AzImage:

\$imageConfig = New-AzImageConfig -Location "EastUS" -SourceUri "https://yourstorageaccount.blob.core.windows.net/vhds/your-image.vhd" -

OsType Windows

Add-AzImage -Image \$imageConfig -ResourceGroupName "YourResourceGroup"

This ensures that the image is available for VM creation in Azure.

upvoted 1 times

  **Marie12345678900** 3 months ago

Selected Answer: B

It is Add-AzVhd. This is one of the question in the Microsoft Learn mock test

upvoted 2 times

  **SHAHIN_STA** 4 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

  **Thomas_M** 5 months ago

Selected Answer: B

To upload a generalized VM image to Azure and make it available for creating new VMs, you would use a combination of the following PowerShell cmdlets:

Add-AzVhd: This cmdlet uploads the generalized VHD file (your image) to an Azure storage account.

Add-AzImage: This cmdlet creates a managed image from the uploaded VHD file, making it available for creating new Azure VMs.

upvoted 3 times

  **Mark74** 5 months ago

Selected Answer: B

for me B is correct



upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

B is corerct

upvoted 2 times

  **nachito** 9 months, 1 week ago

Selected Answer: B

Based on the reference the best option is B:

Before you upload a Windows virtual machine (VM) from on-premises to Azure, you must prepare the virtual hard disk (VHD or VHDX).

reference

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image>

upvoted 1 times


  **MCLC2021** 1 year, 1 month ago

Selected Answer: B

Uploads a virtual hard disk from an on-premises machine to Azure (managed disk or blob).

<https://learn.microsoft.com/en-us/powershell/module/az.compute/add-azvhd?view=azps-11.5.0>

upvoted 1 times

  **tashakori** 1 year, 1 month ago



B is correct

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

B is correct



upvoted 1 times

  **koenigParas2324** 1 year, 3 months ago

Selected Answer: C

The correct PowerShell cmdlet to use for uploading the generalized VM image to Azure is C. Add-AzImage. This cmdlet is used to create a new image in Azure. After generalizing the VM to create an image, you can use the Add-AzImage cmdlet to upload the image to Azure, ensuring that it is available for selection when creating new Azure VMs

upvoted 2 times

  **RVivek** 1 year, 3 months ago

Selected Answer: B

"Add-AzImage" can create a new image from manageddisk only(-ManagedDiskId parameter is required). That means your VHD image should be uploaded first. Add-AzVHD is used to upload image

upvoted 1 times

DRAG DROP -

Your company has an Azure subscription that includes a number of Azure virtual machines (VMs), which are all part of the same virtual network. Your company also has an on-premises Hyper-V server that hosts a VM, named VM1, which must be replicated to Azure.

Which of the following objects that must be created to achieve this goal? Answer by dragging the correct option from the list to the answer area.

Select and Place:

Options

Answer

Hyper-V site

Storage account

Azure Recovery
Services Vault

Azure Traffic
Manager instance

Replication policy

Endpoint

Options

Answer

Hyper-V site

Storage account

Azure Recovery
Services Vault

Azure Traffic
Manager instance

Replication policy

Endpoint

Hyper-V site

Azure Recovery
Services Vault

Replication policy

Correct Answer:

 **weqr23wrefs** Highly Voted 3 years, 7 months ago

For physical servers

- Storage Account

- Azure Recovery Services Vault

- Replication policy

For Hyper-v server

- Hyper-V site
 - Azure Recovery Services Vault
 - Replication policy
- upvoted 307 times

🗄️ 👤 **regex33** 5 months ago

i think:

- **Azure Recovery Services Vault**: Create this to store recovery points and manage replication.
- **Hyper-V Site**: Register the on-premises Hyper-V server as a Hyper-V site in Azure Site Recovery.
- **Storage Account**: Create a storage account to hold the replicated data.
- **Replication Policy**: Define a replication policy to set the rules for replication, including retention and recovery point details.

upvoted 3 times

🗄️ 👤 **ExamPage** 5 months, 4 weeks ago

You were right

upvoted 1 times

🗄️ 👤 **go4adil** 1 year, 3 months ago

Correct Answer:

- Hyper-V site
- Azure Recovery Services Vault
- Replication policy

upvoted 8 times

🗄️ 👤 **jackdryan** 2 years, 2 months ago

This is correct.

upvoted 1 times

🗄️ 👤 **NarenderSingh** Highly Voted 👍 3 years, 7 months ago

1. Hyper-V site
2. Azure Recovery Services Vault
3. Replication policy

<https://docs.microsoft.com/nl-nl/azure/site-recovery/hyper-v-azure-tutorial>

upvoted 34 times

🗄️ 👤 **BobbyMc3030** 2 years, 2 months ago

<https://learn.microsoft.com/en-US/azure/site-recovery/hyper-v-azure-tutorial#prerequisites> for the english speakers

upvoted 2 times

🗄️ 👤 **digitalcoder** Most Recent 🕒 2 months, 2 weeks ago

To replicate an on-premises Hyper-V VM (VM1) to Azure using Azure Site Recovery, the following objects must be created:

Hyper-V site: This is a logical grouping of one or more Hyper-V hosts or clusters. It helps organize and manage the Hyper-V servers involved in replication.

Azure Recovery Services Vault: This is required to store metadata about the replicated VM and manage the replication process.

Storage account: This is used to store the replicated data from the on-premises VM in Azure.

Replication policy: This defines how replication should occur, including recovery point objectives (RPOs), recovery time objectives (RTOs), and retention settings.

These components are essential for configuring and managing the replication process between your on-premises Hyper-V environment and Azure.

upvoted 2 times

🗄️ 👤 **[Removed]** 6 months ago

CORRECT

upvoted 1 times

🗄️ 👤 **Vinayak30** 6 months, 3 weeks ago

Hyper-V site: This refers to configuring your on-premises Hyper-V environment and linking it to Azure.

Storage account: Used to store the replicated data.

Azure Recovery Services Vault: This is essential for managing the replication, failover, and failback of your on-premises VMs.

Replication policy: This defines the replication settings, such as frequency and retention points.

upvoted 1 times

🗄️ 👤 **bcristella** 7 months, 2 weeks ago

How to set up disaster recovery of on-premises physical Windows and Linux servers to Azure. These are the steps:

Set up Azure and on-premises prerequisites

Create a Recovery Services vault for Site Recovery

Set up the source and target replication environments

Create a replication policy

Enable replication for a server

Link: <https://docs.microsoft.com/en-us/azure/site-recovery/physical-azure-disaster-recovery>



How to set up disaster recovery to Azure for on-premises Hyper-V VMs
There are the steps:
Review Hyper-V requirements, and VMM requirements if your Hyper-V hosts are managed by System Center VMM.
Prepare VMM if applicable.
Verify internet access to Azure locations.
Prepare VMs so that you can access them after failover to Azure.
Link: <https://docs.microsoft.com/en-nz/azure/site-recovery/hyper-v-prepare-on-premises-tutorial>
upvoted 3 times

  **SivaPannier** 7 months, 2 weeks ago

Answer is only "Azure Recovery Services Vault" and "Storage Account".

The question is to do only On-prem VM replication to Azure. They did not mention about Disaster Recovery or Site Recovery. Hence we need to do just the Azure migration configuration. Steps are provided in the links below..

The difference between Azure VM Migration and Azure Site Recovery is clearly explained in the below link for your reference.
upvoted 5 times

  **AD_Dude** 7 months, 2 weeks ago

Answer is only "Azure Recovery Services Vault" and "Storage Account".

This tutorial shows you how to prepare Azure components when you want to replicate on-premises Hyper-V VMs to Azure.

In this tutorial, you learn how to:

Create an Azure Storage account to store images of replicated machines.
Create a Recovery Services vault to store metadata and configuration information for VMs and other replication components.
Set up an Azure network. When Azure VMs are created after failover, the VMs are joined to this network.

upvoted 3 times

  **tsummey** 10 months, 2 weeks ago



Answers:
- Storage Account
- Azure Recovery Service Vault
- Replication Policy
Azure Recovery Services Vault stores the recovery points created over time and provides an interface to manage the backup, replication, and recovery of data.
Replication Polic defines the settings for replication, such as the frequency of replication, recovery point retention, and other parameters.
Storage Accounts is where your VM's disks will be replicated to. It's necessary to have a storage account in Azure to hold the data.
The Hyper-V Site is not a direct object but rather a logical grouping within Azure Site Recovery for your Hyper-V servers. An Azure Traffic Manager instance is not required for the replication process itself; it's more about directing traffic across global Azure regions. Lastly, an Endpoint is generally used in the context of network connections and isn't directly related to the replication of VMs.
upvoted 1 times

  **3c5adce** 12 months ago

Why is no one closing out the steps with an End point?
- Hyper-V site
- Azure Recovery Services Vault
- Replication policy
- End Point
upvoted 2 times

  **tashakori** 1 year, 1 month ago



Given answer is right
upvoted 1 times

  **hebb0777** 1 year, 5 months ago
do i need to put answers in order?



- Azure Recovery Services Vault
- Hyper-V site
- Replication policy
upvoted 4 times

  **areuzure** 1 year, 7 months ago

Gosh dang it, I love it here.
upvoted 3 times

  **dubliss** 1 year, 7 months ago

Hyper V Site
Azure recovery Sercices Vault
Replication policy
upvoted 2 times

  **bacana** 1 year, 8 months ago

Should be
Azure Recovery Services Vault

Hyper-V site
Replication policy
upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago

Hyper-V site
Azure Recovery Services Vault
Replication policy
upvoted 2 times

  **ExamPage** 1 year, 11 months ago

The question is about what needs to be created in Azure. Hyper-V site is only linked as the Source during configurations and not created as a resource during the process. Hence, the resources that gets created and seen on the platform after migration will be

- Azure Recovery Service Vault
- Storage Account : disks
- Replication Policy

upvoted 2 times

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

Your company's Azure subscription includes two Azure networks named VirtualNetworkA and VirtualNetworkB.

VirtualNetworkA includes a VPN gateway that is configured to make use of static routing. Also, a site-to-site VPN connection exists between your company's on- premises network and VirtualNetworkA.

You have configured a point-to-site VPN connection to VirtualNetworkA from a workstation running Windows 10. After configuring virtual network peering between VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network. However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation.

You have to make sure that a connection to VirtualNetworkB can be established from the Windows 10 workstation.

Solution: You choose the Allow gateway transit setting on VirtualNetworkA.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (91%)

9%

- NTT_Sttg09**

Highly Voted

2 years, 8 months ago

"After configuring virtual network peering between VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network." This indicates the Allow/Use gateway transit is set up working. The next step will be restart/reinstall the VPN-Client config at the windows 10 WS.

upvoted 309 times
- jackdryan**

2 years, 2 months ago

B is correct.

upvoted 3 times
- VikasN**

2 years, 1 month ago

Really good explanation

upvoted 3 times
- Quantigo**

Highly Voted

3 years, 7 months ago

Answer B - No

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 55 times
- Rab4622**

Most Recent

1 day, 18 hours ago

Selected Answer: B

Vnet b have to also activate allow gateway transit

upvoted 1 times
- ITnerd123**

2 weeks, 1 day ago

Selected Answer: B

Correct answer is B.

upvoted 1 times
- CallMeJimmy**

1 month, 2 weeks ago

Selected Answer: A

The issue arises because the point-to-site (P2S) VPN connection to VirtualNetworkA does not automatically allow traffic to VirtualNetworkB after virtual network peering is established. By enabling "Allow gateway transit" on VirtualNetworkA, you permit the VPN gateway of VirtualNetworkA to forward traffic to VirtualNetworkB.

upvoted 1 times
- victorio_27**

2 months, 3 weeks ago

Selected Answer: A

El problema ocurre porque la estación de trabajo con Windows 10 se conecta a VirtualNetworkA mediante una VPN de punto a sitio (P2S), pero no puede acceder a VirtualNetworkB, a pesar de que VirtualNetworkA y VirtualNetworkB están emparejadas.

Para permitir el tráfico entre la VPN de punto a sitio y VirtualNetworkB, es necesario habilitar el tránsito de puerta de enlace en VirtualNetworkA.

◆ ¿Qué hace la opción "Permitir tránsito de puerta de enlace"?

Permite que el tráfico fluya a través de la puerta de enlace VPN de VirtualNetworkA hacia redes emparejadas (en este caso, VirtualNetworkB).
Habilita la estación de trabajo con Windows 10 para acceder a VirtualNetworkB a través de la conexión VPN de punto a sitio.

upvoted 1 times

🗨️ 👤 **NaoVaz** 7 months, 2 weeks ago

Selected Answer: B

"If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client."

upvoted 9 times

🗨️ 👤 **[Removed]** 7 months, 3 weeks ago

Selected Answer: B

B is correct

You download and re-install the VPN client configuration package on the Windows 10 workstation.

upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗨️ 👤 **[Removed]** 7 months, 4 weeks ago

You download and re-install the VPN client configuration package on the Windows 10 workstation.

upvoted 1 times

🗨️ 👤 **hemanthbugata** 8 months, 1 week ago

No, is the correct one

upvoted 1 times

🗨️ 👤 **raj29oct** 9 months ago

If mobile user wants to access peered VM2, which is peered with VM1 and mobile have point to site with Vm1, but in order to access VM2, BGP must be used.-

upvoted 1 times

🗨️ 👤 **tsummey** 10 months, 2 weeks ago

Selected Answer: A

The answer is A.

By choosing the Allow gateway transit setting on VirtualNetworkA, you enable the Windows 10 workstation that's connected to VirtualNetworkA via a point-to-site VPN to access VirtualNetworkB. This is because the gateway transit setting allows the peered virtual network (VirtualNetworkB in this case) to use the VPN gateway in VirtualNetworkA for cross-premises connectivity

upvoted 1 times

🗨️ 👤 **tashakori** 1 year, 1 month ago

No is right

upvoted 1 times

🗨️ 👤 **tashakori** 1 year, 1 month ago

No is right

upvoted 1 times

🗨️ 👤 **MrTheoDaProphet** 1 year, 4 months ago

Selected Answer: B

NO! The solution of choosing the "Allow gateway transit" setting on VirtualNetworkA does not address the issue of establishing a connection to VirtualNetworkB from the Windows 10 workstation. Troubleshooting the point-to-site VPN connection configuration and ensuring proper routing and security rules are in place is necessary to resolve the problem. Checking the network configuration on VirtualNetworkB for inbound connections from the point-to-site VPN subnet is also recommended.

upvoted 3 times

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

No, enabling the "Allow gateway transit" setting on VirtualNetworkA does not directly address the issue of connecting to VirtualNetworkB from the Windows 10 workstation.

The "Allow gateway transit" setting in Azure is used when you have multiple virtual networks connected through virtual network peering, and it allows one virtual network to use the VPN gateway in another virtual network. However, it doesn't automatically make resources in VirtualNetworkB accessible from the Windows 10 workstation

upvoted 4 times

🗨️ 👤 **KanglD** 1 year, 8 months ago

"you confirm that you are able to access VirtualNetworkB from the company's on-premises network."

That's mean the network is working



"However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation."

Reference to this Microsoft Learn section

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

"If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client."

upvoted 3 times

  **etrop** 1 year, 2 months ago

Good old windows, it's like the same since the 1990s reinstalling or rebooting or reinstalling a driver are the main troubleshooting techniques since Windows 3.1 lol

upvoted 3 times

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

Your company's Azure subscription includes two Azure networks named VirtualNetworkA and VirtualNetworkB.

VirtualNetworkA includes a VPN gateway that is configured to make use of static routing. Also, a site-to-site VPN connection exists between your company's on- premises network and VirtualNetworkA.

You have configured a point-to-site VPN connection to VirtualNetworkA from a workstation running Windows 10. After configuring virtual network peering between VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network. However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation.

You have to make sure that a connection to VirtualNetworkB can be established from the Windows 10 workstation.

Solution: You choose the Allow gateway transit setting on VirtualNetworkB.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (100%)

- d0bermannn**

Highly Voted

3 years, 10 months ago

After reconfiguring \ creating peering existing point-to-site VPN connections need to be recreated

upvoted 34 times
- Takloy**

3 years, 6 months ago

You're right. almost forgot about this. whenever you made some changes on the azure network, you basically need to download the P2S client again for the client devices.

upvoted 5 times
- jackdryan**

2 years, 2 months ago

B is correct

upvoted 1 times
- Quantigo**

Highly Voted

3 years, 7 months ago

Answer B - No

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Thanks for indicating Yes or NO!

upvoted 31 times
- Ponpon3185**

Most Recent

2 months, 1 week ago

Selected Answer: B

It' seems Traffic forwarded is enable: " After configuring virtual network peering between VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network"...so it seems that the issue is not here.

upvoted 1 times
- Bugati**

5 months, 4 weeks ago

can anyone help me with how much topics are there in exaptopics for az-104 and how many questions are there in each topic

upvoted 1 times
- eduardovzermeno**

7 months ago

Selected Answer: B

The "Allow gateway transit" has to be setting on "VirtualNetworkA". "VirtualNetworkB" needs "Use remote gateways" enabled.

upvoted 2 times
- cosmicT73**

6 months ago

I think since the on-prem network can access network B, then those two gateway settings must be already enabled, so the only thing left is to ensure that the VPN client is downloaded and installed again

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

  **Watcharin_start** 1 year, 2 months ago

"you confirm that you are able to access VirtualNetworkB from the company's on-premises network. However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation." it mean, you have completed setting up with `Allow gateway transit` option in Network-A and used `Use remote gateway` option in Network-B already. You just need to restart/reinstall VPN client on your specified host. If you change option in Network-B to `Allow gateway transit`, it will destroy your routing.

upvoted 1 times

  **dhivyamohanbabu** 1 year, 10 months ago

Option B is correct

upvoted 1 times

  **Madbo** 2 years ago

The solution proposed in this scenario is incorrect. Enabling the "Allow gateway transit" setting on VirtualNetworkB would not help establish a connection to VirtualNetworkB from the Windows 10 workstation.

To enable the connection, the "Use remote gateway" setting should be enabled on the point-to-site VPN configuration for VirtualNetworkA. This would allow the Windows 10 workstation to use the VPN gateway on VirtualNetworkA to access resources on VirtualNetworkB.

Therefore, the correct answer is B. No.

upvoted 6 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

"If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client."

upvoted 4 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

  **edengoforit** 3 years, 3 months ago

Site-to-Site (IPsec/IKE VPN tunnel) configurations are between your on-premises location and Azure. This means that you can connect from any of your computers located on your premises to any virtual machine or role instance within your virtual network, depending on how you choose to configure routing and permissions. It's a great option for an always-available cross-premises connection and is well suited for hybrid configurations.

upvoted 2 times

  **orion1024** 3 years, 7 months ago

After changing topology the azure vpn client must be reinstalled to include the new topology information.

upvoted 2 times

  **mdmdmdmd** 3 years, 7 months ago

If you ****make a change to the topology**** of your network and have ****Windows VPN clients****, the VPN client package for Windows clients must be ****downloaded and installed again****

upvoted 5 times

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

Your company's Azure subscription includes two Azure networks named VirtualNetworkA and VirtualNetworkB. VirtualNetworkA includes a VPN gateway that is configured to make use of static routing. Also, a site-to-site VPN connection exists between your company's on- premises network and VirtualNetworkA.

You have configured a point-to-site VPN connection to VirtualNetworkA from a workstation running Windows 10. After configuring virtual network peering between VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network. However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation.

You have to make sure that a connection to VirtualNetworkB can be established from the Windows 10 workstation.

Solution: You download and re-install the VPN client configuration package on the Windows 10 workstation.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: A

Community vote distribution

A (85%)B (15%)

- NaoVaz**

Highly Voted

7 months, 2 weeks ago

Selected Answer: A

"If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client."

upvoted 40 times
- jackdryan**

2 years, 2 months ago

A is correct

upvoted 4 times
- Benjam**

Highly Voted

2 years ago

I have done this at work many times A is correct.

upvoted 10 times
- Helpnosense**

Most Recent

2 months, 1 week ago

Selected Answer: B

Need to update configuration then redownload and reinstall the VPN client.

upvoted 1 times
- ea4b48e**

2 months, 3 weeks ago

Selected Answer: B

The solution provided of downloading and re-installing the VPN client configuration package on the Windows 10 workstation is not likely to meet the goal.

The issue here likely stems from the fact that when you establish a point-to-site VPN connection to VirtualNetworkA, the client configuration package does not automatically update to include routes to any newly peered virtual networks, in this case, VirtualNetworkB. To resolve this, you would need to update the VPN client configuration package to include the new routes.

Therefore, the correct answer is: B. No

upvoted 3 times
- bhaskarraobaipothu**

4 months, 2 weeks ago

Selected Answer: B

Enable Remote Gateway Usage:

Ensure that the peering between VNet A and VNet B is correctly configured.

Enable Allow Gateway Transit on the peering for VNet A.

Enable Use Remote Gateway on the peering for VNet B.

Configure Routing:

Add the necessary routes to ensure that the Windows 10 workstation can route traffic to VNet B. This can be done by:

Configuring custom routes in Azure Route Tables.

Ensuring that the Windows 10 workstation (or the VPN client) has routes to VNet B. You may need to manually add these routes to the VPN client or configure them in Azure's route tables.



upvoted 2 times

  **Mark74** 5 months ago

Selected Answer: A

A is correct , refresh correct routes

upvoted 1 times

  **tsummey** 7 months, 2 weeks ago

Selected Answer: B

B is correct.

The question implies that the Windows 10 workstation should access both VirtualNetworkA and VirtualNetworkB. The scenario says that VirtualNetworkA and VirtualNetworkB are peered, and the Windows 10 workstation has a site-to-site VPN connection with VirtualNetworkA, so you need to turn on the Allow gateway transit option on VirtualNetworkA. Downloading and re-installing the VPN client configuration package on the Windows 10 workstation won't fix the problem of connecting to VirtualNetworkB from the workstation.

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: A

A is correct

upvoted 1 times

  **pooh0805** 1 year, 7 months ago

Selected Answer: B

Downloading and re-installing the VPN client configuration package on the Windows 10 workstation is unlikely to resolve the issue of not being able to establish a connection to VirtualNetworkB from the Windows 10 workstation. This issue is related to the configuration of the VPN client and routing, and simply re-installing the client configuration package is unlikely to address the underlying problem.

upvoted 1 times

  **abinnnnnnnnnn** 1 year, 8 months ago

No, downloading and re-installing the VPN client configuration package on the Windows 10 workstation is not the right solution to establish a connection to VirtualNetworkB from the Windows 10 workstation1. To establish a connection to VirtualNetworkB from the Windows 10 workstation, you need to enable the Allow gateway transit setting on VirtualNetworkA and the Use remote gateways setting on VirtualNetworkB23. This will allow VirtualNetworkB to use the VPN gateway in VirtualNetworkA for connectivity purposes, and the Windows 10 workstation will be able to establish a connection to VirtualNetworkB through the point-to-site VPN connection to VirtualNetworkA

upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago

Option A is correct

upvoted 1 times

  **Madbo** 2 years ago

The solution in option A as YES (downloading and re-installing the VPN client configuration package on the Windows 10 workstation) may resolve the issue of not being able to establish a connection to VirtualNetworkB from the Windows 10 workstation. This is because when a VPN gateway is configured to use static routing, it may require updating the VPN client package configuration after making changes to the VPN gateway, such as adding a virtual network peering. Therefore, downloading and re-installing the VPN client configuration package on the Windows 10 workstation could potentially fix the issue.

upvoted 1 times

  **lokii9980** 2 years, 1 month ago

B. No, downloading and re-installing the VPN client configuration package on the Windows 10 workstation is unlikely to resolve the issue of not being able to connect to VirtualNetworkB. This is because the issue seems to be related to the virtual network peering between VirtualNetworkA and VirtualNetworkB, and not with the VPN client configuration on the Windows 10 workstation.

A more appropriate solution would be to check the virtual network peering configuration, and ensure that the appropriate routes are in place to allow traffic to flow between VirtualNetworkA and VirtualNetworkB. Additionally, checking the network security groups and the Azure Firewall rules can help ensure that traffic is allowed to flow from the Windows 10 workstation to VirtualNetworkB.

upvoted 4 times

  **habbey** 2 years, 1 month ago

I agree. A is correct based on MSC documentation.



upvoted 1 times

  **Shajeecool** 2 years, 3 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

  **bonobos1979** 2 years, 3 months ago

why “Allow gateway transit” and “Use remote gateways” don't need?

upvoted 2 times

  **ricardona** 2 years, 2 months ago

"After configuring virtual network peering between VirtualNetworkA and VirtualNetworkB, you confirm that you are **able** to access VirtualNetworkB from the company's on-premises network."

upvoted 1 times

  **bdumois** 2 years, 7 months ago

A is correct:
Clients using Windows can access directly peered VNets, but the VPN client must be downloaded again if any changes are made to VNet peering or the network topology.
<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

upvoted 2 times

Your company has virtual machines (VMs) hosted in Microsoft Azure. The VMs are located in a single Azure virtual network named VNet1. The company has users that work remotely. The remote workers require access to the VMs on VNet1. You need to provide access for the remote workers. What should you do?

- A. Configure a Site-to-Site (S2S) VPN.
- B. Configure a VNet-toVNet VPN.
- C. Configure a Point-to-Site (P2S) VPN.
- D. Configure DirectAccess on a Windows Server 2012 server VM.
- E. Configure a Multi-Site VPN

Correct Answer: C

Community vote distribution

C (100%)

- StudyNerd123

Highly Voted

3 years, 7 months ago

Answer C:
upvoted 54 times
- jackdryan

2 years, 2 months ago

C is correct
upvoted 3 times
- Iglars

Highly Voted

3 years, 8 months ago

Correct, S2S would be better if you know that the remote workers work from one location, but we don't know that. They could be working from different locations(like home) that's why P2S is better.
upvoted 32 times
- xRiot007

2 years, 1 month ago

P2S is the correct answer. Remote work can be done from anywhere at anytime. If you condition your remote workers to work from one location, that is not remote work anymore, that is an office branch.
upvoted 18 times
- nonia

Most Recent

4 months, 3 weeks ago

Selected Answer: C

Point-to-Site (P2S) VPN is the most appropriate option in this scenario because it allows remote users to securely connect from their individual devices (e.g., laptops, tablets) to an Azure virtual network (VNet1). This is typically used when users need to access Azure resources like VMs remotely over the internet.
upvoted 3 times
- [Removed]

8 months ago

Selected Answer: C

C is correct
upvoted 1 times
- tashakori

1 year, 1 month ago

C is right
upvoted 1 times
- TheUnit720

1 year, 9 months ago

Answer C is correct
This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference.
upvoted 2 times
- maheshwariravi

1 year, 9 months ago

Correct answer is C:-P2S
upvoted 1 times
- [Removed]

1 year, 10 months ago

Selected Answer: C

c
upvoted 1 times

🗨️ 👤 **dhivyamohanbabu** 1 year, 10 months ago

Option C is correct
upvoted 1 times

🗨️ 👤 **LPaul** 1 year, 10 months ago

SITE to Site = Vpn to Vpn , Point to Site = remote (Device)to Vpn
upvoted 6 times

🗨️ 👤 **BowSec** 2 years ago

Selected Answer: C

C. Configure a Point-to-Site (P2S) VPN.

To provide access for remote workers to virtual machines (VMs) hosted in Microsoft Azure, you can use a Point-to-Site (P2S) VPN connection. This type of connection enables individual remote clients to securely connect to an Azure virtual network (VNet) over the Internet.

A Site-to-Site (S2S) VPN connection is used to connect two or more on-premises networks to an Azure virtual network (VNet), while a VNet-to-VNet VPN connection is used to connect two or more Azure virtual networks (VNets) together.

upvoted 7 times

🗨️ 👤 **Madbo** 2 years ago

C the correct one. A P2S VPN is a secure connection between a remote computer and a virtual network. It enables remote workers to securely connect to the virtual network over the Internet. With P2S VPN, the remote worker can connect to VNet1 from their client computer, and then access the VMs in VNet1.

upvoted 2 times

🗨️ 👤 **npsteph** 2 years, 1 month ago

Réponse C
upvoted 1 times

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

The appropriate solution to provide remote workers access to VMs on VNet1 is to configure a Point-to-Site (P2S) VPN.

A P2S VPN allows individual remote computers to connect securely to an Azure virtual network. This solution is ideal for remote workers because it does not require the workers to have an on-premises VPN device, and it allows the workers to access the virtual network resources from anywhere with an internet connection.

Site-to-Site (S2S) VPNs and VNet-to-VNet VPNs are used to connect two or more networks together. DirectAccess is a deprecated technology that is not recommended for new deployments. Multi-Site VPN is used to connect multiple on-premises sites to a single Azure virtual network.

upvoted 7 times

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

Selected Answer: C

Answer C:
upvoted 1 times

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

Selected Answer: C

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

upvoted 3 times

🗨️ 👤 **rolo5555** 2 years, 5 months ago

Answer C:
"This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference"
upvoted 1 times

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

Your company has a Microsoft SQL Server Always On availability group configured on their Azure virtual machines (VMs). You need to configure an Azure internal load balancer as a listener for the availability group.

Solution: You create an HTTP health probe on port 1433.



Does the solution meet the goal?


- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (100%)

-   **Madbo**



Highly Voted 


 7 months, 2 weeks ago

No, the solution does not meet the goal.

Port 1433 is used by SQL Server for SQL Server Database Engine connections, not HTTP connections. Therefore, creating an HTTP health probe on port 1433 will not work.

To configure an Azure internal load balancer as a listener for the availability group, you need to create a TCP health probe on port 1433, which is the default port for SQL Server.

So, the correct solution would be to create a TCP health probe on port 1433, not an HTTP health probe. Therefore, the answer is B (No).
upvoted 49 times
-   **pverma20**



Highly Voted 


 7 months, 2 weeks ago

No, the solution does not meet the goal.

Port 1433 is used by SQL Server for SQL Server Database Engine connections, not HTTP connections. Therefore, creating an HTTP health probe on port 1433 will not work.

To configure an Azure internal load balancer as a listener for the availability group, you need to create a TCP health probe on port 1433, which is the default port for SQL Server.

So, the correct solution would be to create a TCP health probe on port 1433, not an HTTP health probe. Therefore, the answer is B (No).
upvoted 25 times
-   **othiagopadua**

Most Recent 

 3 weeks, 1 day ago



Selected Answer: B

Porta 1433
É usada pelo protocolo TDS (Tabular Data Stream), que é o protocolo de comunicação do:

Microsoft SQL Server

Banco de dados SQL Azure



Ela não é uma porta HTTP e nunca foi rs
upvoted 1 times

  **MrTheoDaProphet** 7 months, 2 weeks ago

Selected Answer: B

No, creating an HTTP health probe on port 1433 does not meet the goal of configuring an Azure internal load balancer as a listener for the SQL Server Always On availability group.

In order to configure an Azure internal load balancer as a listener for the availability group, you need to create a TCP health probe on port 1433. SQL Server uses TCP to communicate on port 1433, so a TCP health probe is the appropriate choice to ensure the availability and health of the SQL Server instances in the availability group.
upvoted 17 times

  **[Removed]** 7 months, 2 weeks ago

Selected Answer: B

B is correct

You enable Floating IP.
upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago

Selected Answer: B

B is corerct
upvoted 1 times

🗨️ 👤 **[Removed]** 7 months, 4 weeks ago

You enable Floating IP.
upvoted 1 times

🗨️ 👤 **Nico1973** 9 months, 4 weeks ago

Answer B. No
Explanation
An HTTP health probe on port 1433 would not be appropriate for an SQL Server Always On availability group listener. It is essential to use a TCP health probe on port 59999 to monitor the availability group listener properly.
upvoted 2 times

🗨️ 👤 **james2033** 1 year, 6 months ago

Selected Answer: B

Port 1433 for database connections pool, not for HTTP protocol in health check.
upvoted 5 times

🗨️ 👤 **KangID** 1 year, 8 months ago

"If enabled, the default instance of the SQL Server Database Engine listens on TCP port 1433."

<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver16>
upvoted 1 times

🗨️ 👤 **maheshwariravi** 1 year, 9 months ago

No is correct answer,as Port 1433 for TCP is needed to connect to the SQL database instance
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 10 months ago

Selected Answer: B

Port 1433 for TCP is needed to connect to the SQL database instance
<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver16>
upvoted 1 times

🗨️ 👤 **dhivyamohanbabu** 1 year, 10 months ago

Option B is correct
upvoted 2 times

🗨️ 👤 **lokii9980** 2 years, 1 month ago

B. No.

The solution mentioned in the scenario is not correct. Creating an HTTP health probe on port 1433 will not work because SQL Server does not use HTTP as a protocol. The HTTP health probe will not be able to determine if the SQL Server instance is running or not.

To configure an Azure internal load balancer as a listener for the availability group, you need to create a TCP health probe on port 1433. SQL Server uses TCP as a protocol, and a TCP health probe will be able to determine if the SQL Server instance is running or not.

Therefore, the correct solution is to create a TCP health probe on port 1433.
upvoted 4 times

🗨️ 👤 **dilipsun** 2 years, 1 month ago

CHATGPT lols
upvoted 6 times

🗨️ 👤 **liza1234** 2 years, 1 month ago

yes.
port 1433 health probe should monitor the status of microsoft sql server.
if this port is healthy, it means the app running on the server, the connection to db, as well as the VM itself are all healthy.
In fact this is the best practice whenever possible since it can monitor at the app/db level not just the VM level.
upvoted 1 times

🗨️ 👤 **harisavt47** 2 years, 1 month ago

Yes but per article below it should be TCP protocol not HTTP

upvoted 1 times

🗨️ 👤 **GBAU** 2 years, 2 months ago

Selected Answer: B


"An availability group listener is a virtual network name that clients connect to for database access. On Azure Virtual Machines in a single subnet, a load balancer holds the IP address for the listener."

To configure an Azure internal load balancer as a listener for the availability group you need to configure an "availability group listener" not a HTTP health probe

upvoted 13 times

  **jackdryan** 2 years, 2 months ago

B is correct
upvoted 1 times

  **micro9000** 2 years, 3 months ago

Eliminate the need for an Azure Load Balancer for your Always On availability (AG) group by creating your SQL Server VMs in multiple subnets within the same Azure virtual network.
upvoted 1 times

  **Mugamed** 2 years, 3 months ago

1433 is a sql port, http is 80, so NO.
upvoted 5 times

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

Your company has a Microsoft SQL Server Always On availability group configured on their Azure virtual machines (VMs). You need to configure an Azure internal load balancer as a listener for the availability group.

Solution: You set Session persistence to Client IP.

Does the solution meet the goal?



- A. Yes
- B. No


Correct Answer: B

Community vote distribution

B (62%)

A (38%)



-   **J511**

Highly Voted 



 3 years, 5 months ago

Answer is B. "None"



FYI: Session persistence ensures that a client will remain connected to the same server throughout a session or period of time. Because load balancing may, by default, send users to unique servers each time they connect, this can mean that complicated or repeated requests are slowed down.

upvoted 48 times
-   **awssecuritynewbie** 3 years, 2 months ago



that defeats the purpose of a load balancer that is allowing traffic to various different SQL servers.


upvoted 7 times
-   **jackdryan** 2 years, 2 months ago

you need to configure an "availability group listener" not a HTTP health probe

upvoted 2 times
-   **jackdryan** 2 years, 2 months ago

B is correct

upvoted 1 times
-   **Timock**

Highly Voted 

 7 months, 2 weeks ago



The load balancing rules configure how the load balancer routes traffic to the SQL Server instances. For this load balancer, you enable direct server return because only one of the two SQL Server instances owns the availability group listener resource at a time.


Therefore Floating IP (direct server return) is Enabled.

TCP 1433 is the standard SQL port. The availability group listener health probe port has to be different from the cluster core IP address health probe port.

The ports on a health probe are TCP59999 and TCP58888.

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/availability-group-load-balancer-portal-configure>



upvoted 14 times
-   **Jay_D_Lincoln**

Most Recent 

 3 months, 1 week ago

Selected Answer: B



It amazes me 40% vote on session persistence!! Really?

upvoted 1 times
-   **minura** 4 months, 2 weeks ago



Selected Answer: B

Answer is B. No

Session persistence ensures that a client will remain connected to the same server throughout a session or period of time.

upvoted 2 times
-   **RajeshwaranM** 4 months, 2 weeks ago

You are correct

upvoted 1 times
-   **7bc6163** 5 months, 2 weeks ago

Selected Answer: A

To configure an Azure internal load balancer (ILB) as a listener for a SQL Server Always On availability group, Session persistence must be set to Client IP. This ensures that the traffic from a specific client is directed consistently to the same backend server during the session. It is a critical requirement for SQL Server Always On listener configurations in Azure, as it helps maintain consistent connectivity for applications interacting with the SQL Server.

upvoted 2 times

  **Chuong0810** 7 months, 2 weeks ago

Selected Answer: A

A is correct



upvoted 1 times

  **SHAHIN_STA** 4 months, 3 weeks ago

Client IP causes traffic to be directed to a specific server based on the client's IP address, even if that server becomes unavailable.

This disrupts SQL Server's automatic Failover process and can cause issues with database accessibility.

upvoted 1 times

  **Madbo** 7 months, 2 weeks ago

The solution meets the goal.

When you configure an Azure internal load balancer as a listener for a Microsoft SQL Server Always On availability group, you need to ensure that session persistence is configured correctly. Session persistence ensures that a client's connections are maintained with the same server during the session. In this case, setting the session persistence to Client IP is a valid solution as it ensures that a client's connection is maintained with the same server for the duration of the session based on the client's IP address.

Therefore, the solution of setting session persistence to Client IP meets the goal. The answer is A (Yes).

upvoted 2 times

  **Flo42** 7 months, 2 weeks ago



asked to chatGPT, and the answer is:

No, the solution does not meet the goal.

For an Azure internal load balancer to properly work as a listener for an SQL Server Always On availability group, you need to set Session persistence to Client IP and protocol, not just Client IP.

Setting the session persistence to "Client IP and protocol" ensures that the load balancer can route the traffic correctly based on both the client's IP address and the protocol, which is essential for the proper functioning of SQL Server Always On availability groups.

upvoted 2 times

  **lokii9980** 7 months, 2 weeks ago

A. Yes.

The solution mentioned in the scenario is correct. Setting session persistence to Client IP will ensure that all connections from a given client IP address are routed to the same SQL Server instance. This is important for ensuring that the client's session state is maintained, as SQL Server Always On availability groups do not provide session state sharing across multiple replicas.

By using the Client IP session persistence mode, the Azure internal load balancer will route all client connections from a specific IP address to the same SQL Server instance. This ensures that the client's session state is maintained and provides a seamless failover experience.

Therefore, the solution meets the goal of configuring an Azure internal load balancer as a listener for the SQL Server Always On availability group.

upvoted 1 times

  **Just_Nick** 2 years ago

Read it again carefully, to setup on Client IP, this is wrong! To configure Availability Group you should do it all in the server side not on Client Side.

upvoted 2 times

  **dilipsun** 2 years, 1 month ago

Again ChatGpt

upvoted 4 times

  **[Removed]** 8 months ago

Selected Answer: B

B is corerct

upvoted 1 times

  **longwhiteclouds** 9 months, 1 week ago

For configuring an Azure internal load balancer (ILB) as a listener for a SQL Server Always On availability group, setting the session persistence to "Client IP" is correct. This setting ensures that client connections from the same IP address are consistently routed to the same backend server. This is important for SQL Server Always On availability groups to ensure that the traffic is directed to the correct primary replica.

Answer: A

upvoted 1 times

  **Charumathi** 11 months ago

Selected Answer: A

Yes, session persistence can be configured in an internal load balancer (ILB) used as a listener for an Availability Group in Azure. This is useful in scenarios where you have a high-availability setup for SQL Server Always On Availability Groups and need to ensure that client connections are consistently routed to the same backend node for session consistency.

<https://learn.microsoft.com/en-us/azure/load-balancer/distribution-mode-concepts#session-persistence>
upvoted 3 times

  **skywalker** 1 year ago

Selected Answer: A

Paste the question to CoPilot. and you will know.
upvoted 1 times

  **tashakori** 1 year, 1 month ago

No is right
upvoted 1 times

  **pooh0805** 1 year, 7 months ago

Selected Answer: A

Setting session persistence to "Client IP" on the Azure internal load balancer is a valid solution for configuring an Azure internal load balancer as a listener for a Microsoft SQL Server Always On availability group. This configuration ensures that client connections from the same source IP address are consistently directed to the same SQL Server instance within the availability group.
upvoted 1 times

  **havoc2k7** 1 year, 7 months ago

Ans. is NO, the key word is 'availability group' means we need redundancy of servers, servers must talk with each other which uses health probe not session persistence, this is use for communication between client and server. Correct me if im wrong.
upvoted 2 times

  **System2214** 1 year, 7 months ago

Selected Answer: B

B es correcto.
upvoted 2 times

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

Your company has a Microsoft SQL Server Always On availability group configured on their Azure virtual machines (VMs). You need to configure an Azure internal load balancer as a listener for the availability group.

Solution: You enable Floating IP.

Does the solution meet the goal?

- A. Yes
- B. No


Correct Answer: A

Community vote distribution

A (85%)

B (15%)

-   **Bloodwar**

Highly Voted 



 3 years, 9 months ago

The load balancing rules configure how the load balancer routes traffic to the SQL Server instances. For this load balancer, you enable direct server return because only one of the two SQL Server instances owns the availability group listener resource at a time.



> > Floating IP (direct server return) Enabled

upvoted 72 times
-   **ricardona** 2 years, 2 months ago



Yes, enabling Floating IP on the Azure internal load balancer as a listener for the availability group can meet the goal. By enabling Floating IP, the load balancer will use a floating IP address as the source IP address for outbound flows from the backend pool. This will ensure that the IP address used by the backend pool remains the same even if a VM is restarted or replaced, which is important for maintaining the listener for the availability group.


upvoted 31 times
-   **happpieee** 6 months, 2 weeks ago

Yes floating IP is a configuration supported by Azure LB:

upvoted 2 times
-   **jackdryan** 2 years, 2 months ago

A is correct

upvoted 2 times
-   **edengoforit**

Highly Voted 

 3 years, 3 months ago

If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition.

When Floating IP is enabled, Azure changes the IP address mapping to the Frontend IP address of the Load Balancer frontend instead of backend instance's IP.

Without Floating IP, Azure exposes the VM instances' IP. Enabling Floating IP changes the IP address mapping to the Frontend IP of the load Balancer to allow for additional flexibility.

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip>


upvoted 12 times
-   **TheOwl**

Most Recent 

 1 week, 6 days ago



Selected Answer: A

Answer is A

upvoted 1 times
-   **58b2872** 4 months, 1 week ago


Selected Answer: A

Since enabling Floating IP is required for the ILB to act as a listener for SQL Server Always On availability groups, the solution meets the goal.

upvoted 1 times
-   **Z_MU** 4 months, 1 week ago



Selected Answer: A

<https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/availability-group-load-balancer-portal-configure?view=azuresql#step-4-set-the-load-balancing-rules>

upvoted 1 times
-   **Mark74** 5 months ago

Selected Answer: A

A is correct
upvoted 1 times

  **ralphmas** 7 months, 2 weeks ago

The solution provided, enabling Floating IP, does not meet the goal of configuring an Azure internal load balancer as a listener for the availability group.

Enabling Floating IP is not the correct configuration option for an Azure internal load balancer listener for SQL Server Always On availability groups. Floating IP is only used for outbound traffic from the virtual machine, and not for inbound traffic from the Azure internal load balancer.



To configure an Azure internal load balancer as a listener for the availability group, you need to create an internal load balancer and configure the listener for the availability group. You will then add the IP address of the internal load balancer as the listener IP address for the availability group.

Therefore, the correct answer is B. No.
upvoted 3 times

  **[Removed]** 8 months ago

Selected Answer: A

A is corerct
upvoted 1 times

  **Nico1973** 9 months, 4 weeks ago

Answer: B. No

Explanation: Enabling Floating IP is not the correct solution for configuring an Azure internal load balancer as a listener for the availability group. In Azure, for an internal load balancer to act as a listener for the availability group, you should configure the load balancer with a Standard SKU and a Basic SKU public IP address. The internal load balancer should be associated with the back-end pool of the availability group nodes.

Therefore, enabling Floating IP does not meet the goal of configuring an Azure internal load balancer as a listener for the availability group.
upvoted 1 times

  **tsummey** 10 months, 2 weeks ago

Selected Answer: A

In the context of SQL Server Always On AG, the Floating IP is crucial because it provides a consistent endpoint for the AG listener. To support failover Handling, Azure VNets do not support broadcasting, so the Floating IP and the internal load balancer's probe setup help determine which node is the primary replica and direct application traffic to it without the need for broadcasting.

upvoted 2 times

  **tashakori** 1 year, 1 month ago

Yes is right
upvoted 1 times

  **eddzequiel** 1 year, 2 months ago

worksThe load balancing rules configure how the load balancer routes traffic to the SQL Server instances. For this load balancer, you enable direct server return because only one of the two SQL Server instances owns the availability group listener resource at a time.

upvoted 1 times

  **harendradhiman** 1 year, 4 months ago



Selected Answer: A

Azure Load Balancer Floating IP configuration explanation:
<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip>

upvoted 2 times



  **bgbgvfvf** 1 year, 4 months ago

A correct
upvoted 1 times

  **TedM2** 1 year, 6 months ago

Selected Answer: A

A
upvoted 1 times

  **JWS80** 1 year, 9 months ago

Selected Answer: B

No, the solution does not meet the goal. Enabling Floating IP is not a required step when configuring an Azure internal load balancer as a listener for a SQL Server Always On availability group. There are several steps involved in configuring an Azure internal load balancer for a SQL Server Always On availability group, including creating the load balancer, configuring the backend pool, creating a probe, and setting the load balancing rules. Enabling Floating IP is not one of these steps.

upvoted 5 times

  **kamalpur** 1 year, 9 months ago

The floating IP concept is explained in below video
upvoted 7 times

Your company has two on-premises servers named SRV01 and SRV02. Developers have created an application that runs on SRV01. The application calls a service on SRV02 by IP address.

You plan to migrate the application on Azure virtual machines (VMs). You have configured two VMs on a single subnet in an Azure virtual network. You need to configure the two VMs with static internal IP addresses.

What should you do?

- A. Run the New-AzureRMVMConfig PowerShell cmdlet.
- B. Run the Set-AzureSubnet PowerShell cmdlet.
- C. Modify the VM properties in the Azure Management Portal.
- D. Modify the IP properties in Windows Network and Sharing Center.
- E. Run the Set-AzureStaticVNetIP PowerShell cmdlet.

Correct Answer: C

Community vote distribution

C (53%) E (47%)

blackmetalx

Highly Voted

7 months, 2 weeks ago

Set-AzureStaticVNetIP is for Classic VMs and will be retired on September 1, 2023.

For new VM it can be don in the portal or using Powershell:
<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/reset-network-interface>

#Add/Change static IP. This process will change MAC address
\$vnet = Get-AzVirtualNetwork -Name \$VNET -ResourceGroupName \$ResourceGroup

\$subnet = Get-AzVirtualNetworkSubnetConfig -Name \$subnet -VirtualNetwork \$vnet

\$nic = Get-AzNetworkInterface -Name \$NetInter -ResourceGroupName \$ResourceGroup

#Remove the PublicIpAddress parameter if the VM does not have a public IP.
\$nic | Set-AzNetworkInterfaceIpConfig -Name ipconfig1 -PrivateIpAddress \$PrivateIP -Subnet \$subnet -PublicIpAddress \$publicIP -Primary

\$nic | Set-AzNetworkInterface
upvoted 28 times

Quantigo

Highly Voted

3 years, 7 months ago

Correct Answer E:
Run the Set-AzureStaticVNetIP PowerShell cmdlet.

upvoted 21 times

rah_rule100

Most Recent

1 day, 18 hours ago

Selected Answer: E

E is the correct answer

upvoted 1 times

saadraaz

2 weeks, 2 days ago

Selected Answer: C

Set-AzureStaticVNetIP is from the Azure Service Management (ASM or "Classic") model, and it has been deprecated in favor of the Azure Resource Manager (ARM) model — which is what most deployments use today.

upvoted 1 times

Ekramy_Elnaggar

3 weeks, 2 days ago

Selected Answer: C

Set-AzureStaticVNetIP (Classic VMs only – Deprecated)

upvoted 1 times

GohanF2

1 month, 1 week ago

Selected Answer: C

I will vote for C as well. We the command for Option E is already deprecated. I dont think so that they will be evaluating on old content.
<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-networks-static-private-ip?tabs=azureportal>

upvoted 1 times

HartMS

2 months, 3 weeks ago

Selected Answer: C

In VM settings, we need to go to Networking to make the required changes. C is the correct answer.

Set-AzureStaticVnetIP is not a valid option, as that cmdlet was part of the classic model, which is now deprecated.

The correct cmdlet is Set-AzNetworkInterface.


upvoted 2 times

  **Nathan12345** 2 months, 3 weeks ago

Selected Answer: C

Take help from copilot or chatgpt


upvoted 1 times

  **Bikth** 3 months, 1 week ago

Selected Answer: E

To configure Azure virtual machines (VMs) with static internal IP addresses, the best approach is to use the Set-AzureStaticVNetIP PowerShell cmdlet. This allows you to assign a static private IP address to the VM within the Azure virtual network (VNet).



upvoted 1 times

  **Odc4dd8** 3 months, 2 weeks ago

Selected Answer: C

To configure static internal IP addresses for Azure VMs, you need to set the IP address configuration directly in the Azure portal or using Azure PowerShell/CLI.

upvoted 1 times

  **superrvirgo** 3 months, 2 weeks ago

Selected Answer: C

There is no Set-AzureStaticVNetIP anymore.

But if there was, I would say that the correct answer should be C & E

upvoted 2 times

  **mpaen10928** 3 months, 2 weeks ago

Selected Answer: C

C is the closest answer, but the change is done within Settings, not Properties. <https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-networks-static-private-ip?tabs=azureportal>

In the following steps, you change the private IP address static for the VM created previously:

In the portal, search for and select Virtual machines.

In Virtual machines, select myVM from the list.

On the myVM page, under Settings, select Networking.

upvoted 1 times

  **lockmas101** 3 months, 3 weeks ago

Selected Answer: E

Answer is E. You cannot edit the properties in the VM Overview --> Properties. The command might be old but this is probably an old question

upvoted 3 times

  **TodRose** 4 months ago

Selected Answer: E

E. Run the Set-AzureStaticVNetIP PowerShell cmdlet.

Explanation:

To configure a static internal IP address for Azure VMs in the same virtual network, you need to use the Set-AzureStaticVNetIP PowerShell cmdlet. This cmdlet allows you to assign a specific private IP address to a virtual machine's network interface within a subnet.

upvoted 2 times

  **58b2872** 4 months, 1 week ago

Selected Answer: E

Option C modifies general VM properties but cannot manage the static IP configuration for the NIC.

Option E is designed specifically for static IP assignment, which is exactly addresses the NIC level.

upvoted 2 times

  **58b2872** 4 months, 1 week ago

Selected Answer: E

The Set-AzureStaticVNetIP cmdlet is specifically used to assign a static internal IP address to an Azure VM in a virtual network.

Modifying VM properties in the Azure Management Portal (Option C) does not allow you to directly set a static internal IP address. Static IP addresses for Azure VMs must be configured at the network interface level, and this is best done via PowerShell.

upvoted 1 times

  **bhaskarraobaipothu** 4 months, 2 weeks ago

Selected Answer: E

C. partially correct but not the best answer for the given context.

E.E. Run the Set-AzureStaticVNetIP PowerShell cmdlet.

It allows you to assign a static IP address to a VM within an Azure Virtual Network

upvoted 1 times

Your company has an Azure Active Directory (Azure AD) subscription.

You need to deploy five virtual machines (VMs) to your company's virtual network subnet.

The VMs will each have both a public and private IP address. Inbound and outbound security rules for all of these virtual machines must be identical.

Which of the following is the least amount of network interfaces needed for this configuration?

- A. 5
- B. 10
- C. 20
- D. 40

Correct Answer: A

Community vote distribution

A (92%)

8%

- samshir**

Highly Voted

3 years, 7 months ago

5 VM so 5 NIC Cards .we have public and private ip address set to them .however they needs same inbound and outbound rule so create NSG and attach to NIC and this req can be fulfilled 5 NIC hence 5 is right ans

upvoted 88 times
- jackdryan**

2 years, 2 months ago

A is correct

upvoted 6 times
- CloudyTech**

Highly Voted

3 years, 10 months ago

5 is correct

upvoted 26 times
- andted98**

Most Recent

4 weeks, 1 day ago

Selected Answer: A

An NIC Card can have one public & multiple private IP addresses. In this case study, 5 VMs are to be deployed, hence 5 NICs are required.

upvoted 1 times
- Odc4dd8**

3 months, 2 weeks ago

Selected Answer: A

Each virtual machine (VM) in Azure can have multiple network interfaces (NICs), but in this scenario, you only need one NIC per VM

upvoted 1 times
- Mark74**

5 months ago

Selected Answer: A

A is correct, you can add public and private IP to the same Network card

upvoted 2 times
- minura**

5 months, 2 weeks ago

Selected Answer: A

5 VMs - 5 Network Interface Cards (NIC)

upvoted 2 times
- dilopezat**

5 months, 2 weeks ago

Selected Answer: A

To deploy five VMs with both public and private IP addresses, you would need at least five network interfaces (one for each VM). Each VM requires a network interface to connect to the virtual network, and since each VM will have both a public and a private IP address, you would typically assign one network interface per VM.


upvoted 1 times
- KangID**

7 months, 2 weeks ago

5 Azure Virtual Machine.
That's means at least 5 NICs on it.

Ref.
Constraints of Azure VM
A VM must have at least one network interface attached to it

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm>
upvoted 2 times

  **pooh0805** 7 months, 2 weeks ago

Selected Answer: B

The least amount of network interfaces needed for this configuration is:

B. 10

Here's why:

You have five virtual machines (VMs), each with both a public and private IP address. To achieve this configuration, you need one network interface (NIC) for each VM. Each NIC has both a private IP address (associated with the virtual network subnet) and a public IP address (if you want to assign one).

So, for the five VMs, you would need 5 NICs. Since each NIC has both a private and public IP address, you have a total of 5 NICs * 2 IP addresses per NIC = 10 IP addresses.

Therefore, the least amount of network interfaces needed for this configuration is 10.

upvoted 3 times

  **Riz504** 5 months ago

Question is "least amount of network interfaces" and not how many IPs so answer is 5 and not 10. i.e. A and not B.

upvoted 1 times

  **18c2076** 1 year, 1 month ago

You understand that you stated the entirely correct answer, and then immediately proceeded to contradict yourself with a stoopid statement that made zero sense right afterward, correct? lol

upvoted 6 times

  **GODUSGREAT** 1 year, 6 months ago

it's 5

upvoted 1 times

  **GODUSGREAT** 1 year, 6 months ago

The least amount of network interfaces needed for this configuration is one network interface per VM.

Each virtual machine (VM) in Azure requires at least one network interface. In this scenario, you need to deploy five VMs, each with both a public and private IP address. To achieve this, you would need to create five network interfaces, one for each VM.

Each network interface can be associated with both a public IP address (for inbound connections) and a private IP address (for internal communication within the virtual network). By configuring the appropriate security rules, you can ensure that the inbound and outbound traffic for all five VMs is identical.

Therefore, the least amount of network interfaces needed for this configuration is one network interface per VM, resulting in a total of five network interfaces.

upvoted 1 times

  **BigStevieMcDave** 7 months, 2 weeks ago

I initially thought this was 10 too, because with physical NICs it would be.

But I did some digging and I think 5 is correct.

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-network-interface-addresses?tabs=nic-address-portal>

"You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article."

upvoted 3 times

  **etrop** 12 months ago

Not really no even with Physical systems you can have multiple IP addresses on one NIC card and you can just tag different VLANS on your NIC traffic, with one being the public VLAN. But honestly nobody would do that nowadays they would just have the public addresses reside on the firewall or outer edge systems.

upvoted 2 times

  **robsoneuclides** 11 months, 1 week ago

Correto

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: A

A is correct

upvoted 1 times


  **demha2024** 9 months, 2 weeks ago

5 is the correct answer

"You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. You

can add a private IPv6 address to one secondary IP configuration (as long as there are no existing secondary IP configurations) for an existing network interface. Each network interface can have one IPv6 private address. You can optionally add a public IPv6 address to an IPv6 network interface configuration. See IPv6 for details about using IPv6 addresses."

upvoted 1 times

  **Nico1973** 9 months, 4 weeks ago

The least amount of network interfaces needed for this configuration is B. 10.
Each virtual machine requires two network interfaces - one for the public IP address and one for the private IP address. Therefore, with five virtual machines, you would need a total of 10 network interfaces to accommodate both types of IP addresses for each VM.

upvoted 2 times

  **tashakori** 1 year, 1 month ago

A is right

upvoted 3 times

  **Tim150** 1 year, 9 months ago

Selected Answer: A

very easy

upvoted 1 times

  **Aquintero** 1 year, 9 months ago

A. 5 cada VM debe tener minimo una NIC y cada una de estas puede tener varias direcciones Ip

upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago

Correct answer A

upvoted 1 times

Your company has an Azure Active Directory (Azure AD) subscription.

You need to deploy five virtual machines (VMs) to your company's virtual network subnet.

The VMs will each have both a public and private IP address. Inbound and outbound security rules for all of these virtual machines must be identical.

Which of the following is the least amount of security groups needed for this configuration?

- A. 4
- B. 3
- C. 2
- D. 1

Correct Answer: D

Community vote distribution

D (100%)

- Exam_khan**

Highly Voted

 3 years, 9 months ago

all identical security groups so you will only require 1 security group as all the settings are the same

upvoted 54 times
- jackdryan** 2 years, 2 months ago

D is correct

upvoted 3 times
- Biju1**

Highly Voted

 3 years, 10 months ago

correct Answer D

upvoted 23 times
- andted98**

Most Recent

 4 weeks, 1 day ago

Selected Answer: D

All VMs are assigned identical inbound and outbound security groups within the same subnet, so only one NSG is needed.

upvoted 1 times
- minura** 5 months, 2 weeks ago

Selected Answer: D

Correct Answer is D. 1

upvoted 1 times
- Nico1973** 7 months, 2 weeks ago

To achieve the deployment of five virtual machines (VMs) with both public and private IP addresses, sharing identical inbound and outbound security rules, the least amount of security groups needed for this configuration is B. 3.

Here's the breakdown:

One security group for the VMs' public IP addresses.

One security group for the VMs' private IP addresses.

One security group for the identical inbound and outbound security rules that must apply to all five VMs.

upvoted 1 times
- KangID** 7 months, 2 weeks ago

At least one security group is an answer

ref.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

You can deploy resources from several Azure services into an Azure virtual network. For a complete list, see Services that can be deployed into a virtual network. You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine. The same network security group can be associated to as many subnets and network interfaces as you choose.

upvoted 2 times
- [Removed]** 8 months ago



Selected Answer: D

D is corerct

upvoted 1 times
- Saurabh_Bhargav** 1 year, 2 months ago

D.1 is correct

upvoted 1 times

  **Awot** 1 year, 7 months ago

the correct answer is D


upvoted 1 times

  **System2214** 1 year, 7 months ago

Selected Answer: D

Correct

upvoted 1 times

  **Aquintero** 1 year, 9 months ago

Selected Answer: D

un unico grupo de seguridad (NSG) puedes ser asignado a la subnet, de esta manera todas las VM tendran la mismas reglas

upvoted 4 times

  **dhivyamohanbabu** 1 year, 10 months ago

Correct answer D

upvoted 1 times

  **mukesh5184** 1 year, 11 months ago

Shouldn't there be 2 NSGs - 1 each for Inbound and Outbound?

upvoted 1 times

  **18c2076** 1 year, 1 month ago

No. The NSG sets both inbound and outbound in the same group

upvoted 3 times

  **Madbo** 2 years ago

The correct answer is D. You can use a single network security group (NSG) for all five VMs since the inbound and outbound security rules are identical for all of them.

upvoted 5 times

  **bcristella** 2 years, 1 month ago



1 NSG -> 1 Vnet (This is hosting 5 VM's)

upvoted 1 times

  **almikhdade** 2 years, 1 month ago

D. an NSG can be attached to a subnet,

upvoted 2 times

  **ThePro** 2 years, 5 months ago

Selected Answer: D

Same VNet with same inbound/outbound rules so it will be 1 security group only.

upvoted 4 times

  **NandKeshwar** 2 years, 4 months ago

NSG is attached at subnet or network interface and not at Vnet.

upvoted 6 times



Your company's Azure subscription includes Azure virtual machines (VMs) that run Windows Server 2016. One of the VMs is backed up every day using Azure Backup Instant Restore. When the VM becomes infected with data encrypting ransomware, you decide to recover the VM's files. Which of the following is TRUE in this scenario?


- A. You can only recover the files to the infected VM.
- B. You can recover the files to any VM within the company's subscription.
- C. You can only recover the files to a new VM.
- D. You will not be able to recover the files.

Correct Answer: B

Community vote distribution

B (70%)	A (19%)	11%
---------	---------	-----



-   **lazz77**

Highly Voted 



 7 months, 2 weeks ago

According to below, we can restore the files to an alternate VM too



Therefore the answer should be B

upvoted 46 times
-   **TDS_sada** 3 years, 7 months ago

As I understand Here the catch is new VM,any VM, means it can be any non windows OS. So in this scenario the effected os is Windows and only the Answer A related to the windows OS.

upvoted 5 times
-   **garmatey** 2 years, 1 month ago

But the question specifically says the VMs in your company's subscription run Windows. And answer B specifies any VM "within the company's subscription".



upvoted 4 times
-   **rawrkadia** 3 years, 10 months ago

This is a different feature.



<https://docs.microsoft.com/en-us/azure/backup/backup-instant-restore-capability>

Backup instant restore is snapshotting. In order to be 'instant' tier you have to be restoring from a stored snapshot vs from the vault. I do not believe you are correct.



<https://docs.microsoft.com/en-us/azure/backup/about-azure-vm-restore>


upvoted 5 times
-   **rawrkadia** 3 years, 10 months ago

In fact, I don't even know if you **can** recover files from a snapshot. You have to convert the snapshot to a managed disk then attach that to a VM.

upvoted 5 times
-   **aldebaran65** 1 year, 8 months ago

You can restore file level from snapshot. Azure will mount the snapshot as a disk on OS level, and you can copy the files manually.



upvoted 1 times
-   **Gyanexcel**


Highly Voted 

 7 months, 2 weeks ago

Selected Answer: B

Rationale: Option-A and Option-C are incorrect as they respectively exclaim that "Can Only" recover on infected VM or "Can only" recover on new VM. And both are not complete truth with "Can only" specified in the statements. It can be recovered on any VM. Option-D suggests that it cannot be recovered at all, so that's also not correct. Therefore, Option-B is the right answer.



upvoted 15 times
-   **dhavalmodi**

Most Recent 

 1 month, 2 weeks ago

Selected Answer: C

C: Typically, you will recover the data to a new VM in a safe environment to ensure that the new ransomware doesn't affect the restored files or VM

upvoted 2 times
-   **BWLZ** 2 months, 1 week ago

Selected Answer: B

With Azure Backup Instant Restore, you can recover individual files from the snapshot without restoring the entire VM. The File Recovery feature allows you to mount the backup as a virtual drive and copy the required files to any VM within the same Azure subscription.

upvoted 2 times

  **c4ecedc** 3 months ago

Selected Answer: B

The correct answer is B.



upvoted 1 times

  **Jay_D_Lincoln** 3 months, 1 week ago

Selected Answer: B

B is not the ideal action to be taken in this scenario, but it IS the correct answer. C is incorrect because of the same word as A which is "ONLY"



upvoted 2 times

  **minura** 5 months, 2 weeks ago

Selected Answer: B

Simple, the correct answer is B. You can recover the files to any VM within the company's subscription.

upvoted 1 times

  **dilopezat** 5 months, 2 weeks ago

Selected Answer: B

Yes, you can recover files from Azure Backup Instant Restore to any VM within the company's subscription. Azure Backup allows you to restore files and folders from a recovery point to any VM in the same subscription. This flexibility helps in scenarios like ransomware attacks where you need to recover data to a different VM.



upvoted 2 times

  **Xpinguser** 6 months, 3 weeks ago

Selected Answer: C

C. You can only recover the files to a new VM

upvoted 1 times

  **FredFrom** 6 months, 2 weeks ago

C should be the best but is not the ONLY option ! Then answer B is correct.

upvoted 1 times

  **Xpinguser** 6 months, 3 weeks ago

Selected Answer: C

The correct answer is:



C. You can only recover the files to a new VM.

Azure Backup Instant Restore allows you to recover files from a VM backup to a new VM. This is a crucial security measure to prevent re-infection. Recovering files to the infected VM could potentially reintroduce the ransomware.

Here's a breakdown of why the other options are incorrect:

B. You can recover the files to any VM within the company's subscription. This is incorrect because recovering files to another infected VM could also lead to re-infection.



upvoted 2 times

  **0378d43** 6 months, 3 weeks ago

Selected Answer: A

Creating new. VM and then configuring it takes more time compared to restoring in the same VM.



upvoted 1 times

  **Omer87** 7 months, 1 week ago

Selected Answer: C

It should be a new VM as there are certain limitations to where (i.e. OS version) the files could be recovered <https://learn.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm>

upvoted 1 times

  **Timock** 7 months, 2 weeks ago


Answer is B:

In-place restore capability: With instant restore, users also get a capability to perform in-place restore, thus, overwriting the data in the original disk rather than creating a copy of the disk at an alternate location...

*Note: "users ALSO get the capability to perform in-place restores overwriting the data on the original disk." - Meaning that they can still create a copy elsewhere. This intimates that before Instant Restore this really wasn't an option.

Answer A states you can ONLY recover to the infected VM. This is not true and instant restore works for both Linux and Windows machines as of 2017.

upvoted 6 times

  **maqibali** 7 months, 2 weeks ago

Selected Answer: A

A. You can only recover the files to the infected VM.

When using Azure Backup Instant Restore to restore files on a VM, the restore operation overwrites the existing files on the VM with the restored files. In this scenario, the infected VM is backed up every day, so you can use Azure Backup Instant Restore to restore the VM's files to a previous backup point before the ransomware infection occurred.

However, it's important to note that Azure Backup Instant Restore can only restore files to the original VM that was backed up. You cannot restore the files to a different VM or to a new VM. This is because Azure Backup Instant Restore uses a snapshot of the VM's disks to restore the files, and the snapshot is tied to the original VM's disk.

upvoted 3 times



  **Leunis** 7 months, 2 weeks ago

Selected Answer: B

There are two variants of this question.

- Recovering only the files, you can recover them to any other VM within the company.
- Using instant recover to recover the entire VM, this should be done to a new VM.

upvoted 3 times

  **yarwana** 7 months, 2 weeks ago

Selected Answer: A

The correct answer is A. You can only recover the files to the infected VM.

Azure Backup Instant Restore enables you to recover files and folders from a VM backup directly to the same VM. It does not provide an option to restore the files to a different VM.

In the scenario described, since the VM is infected with ransomware, restoring the files to the same VM may not be advisable, as it may reintroduce the malware. However, this is still the only option provided by Azure Backup Instant Restore.

To restore the files to a different VM, you may need to use a different recovery option, such as restoring the backup to a new VM, or using Azure Site Recovery to replicate the VM and recover the data from the replica. However, these options may require additional configuration and may take longer to complete than using Azure Backup Instant Restore.

upvoted 5 times

  **DJHASH786** 7 months, 2 weeks ago

The correct answer in this scenario is:

B. You can recover the files to any VM within the company's subscription.

Explanation:

Azure Backup Instant Restore allows you to recover files and folders from the recovery points of a VM. This feature provides the flexibility to recover files either to the original VM or to any other VM within the same subscription. Therefore, if a VM becomes infected with ransomware, you have the option to recover its files to another VM to avoid any risk of re-infection. This capability ensures that you can restore the necessary data without having to restore it directly to the infected machine, providing a safer recovery option.

upvoted 3 times

Your company's Azure subscription includes Azure virtual machines (VMs) that run Windows Server 2016. One of the VMs is backed up every day using Azure Backup Instant Restore. When the VM becomes infected with data encrypting ransomware, you are required to restore the VM. Which of the following actions should you take?

- A. You should restore the VM after deleting the infected VM.
- B. You should restore the VM to any VM within the company's subscription.
- C. You should restore the VM to a new Azure VM.
- D. You should restore the VM to an on-premise Windows device.

Correct Answer: C

Community vote distribution

C (89%)8%

- shamst**

Highly Voted

3 years, 10 months ago

It should be C

upvoted 48 times
- jackdryan**

2 years, 2 months ago

C is correct

upvoted 3 times
- Zokko**

Highly Voted

7 months, 2 weeks ago

I belive it is the C option

A - If you delete the VM you cannot recover to that vm it must exist

B - You do not know the other VMs

C - Creating a New VM you can recover the VM

D - You can recover from the backup

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms>

upvoted 38 times
- ggogel**

1 year, 5 months ago

"A - If you delete the VM you cannot recover to that vm it must exist"

This is not correct. As described in your link, you cannot use the option "replace existing" after the VM was deleted.

The backup is not linked to the existence of the VM! What kind of backup would this be that gets deleted when the original VM gets deleted?!

In my opinion, A and C would work just fine. I would even argue that A is the saver option. Firstly, we get rid of the ransomware such that it cannot infect any other systems. Secondly, we prevent any overlaps in hostname / IP configuration between the new and old VM.

upvoted 7 times
- J4U**

3 years, 8 months ago

Yes, VM can be restored by replacing the existing disk or in a new VM.

upvoted 10 times
- Odc4dd8**

Most Recent

3 months, 2 weeks ago

Selected Answer: C

When dealing with a VM infected with ransomware, the safest and most effective approach is to restore the VM to a new Azure VM

upvoted 2 times
- 58b2872**

4 months, 1 week ago

Selected Answer: C

Restoring to an on-premises server is possible but involves significant compatibility, complexity, and performance issues, making it impractical for disaster recovery scenarios. Restoring the VM to a new Azure VM (option C) is the most efficient and reliable choice in this situation.

upvoted 1 times
- minura**

5 months, 2 weeks ago

Selected Answer: C

A. You should restore the VM after deleting the infected VM.

B. You should restore the VM to any VM within the company's subscription.



C. You should restore the VM to a new Azure VM.

D. You should restore the VM to an on-premise Windows device.

Correct Answer is C

However, one can argue that answer A is also correct, but deleting the infected VM is not a mandatory step to restore a VM. You can simply restore the VM to a new Azure VM.

upvoted 1 times


  **RVivek** 6 months, 1 week ago

Selected Answer: C

A is wrong because if you delete the VM , replace existing disks or restore disk options cannot be used .
C is the best option.

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms>

upvoted 1 times



  **EmadSal** 7 months, 1 week ago

A is incorrect because you need the source machine to be available while recovering a corrupted VM, visit [<https://learn.microsoft.com/en-us/azure/backup/backup-azure-restore-system-state>] and search for [source machine] you will understand this point.

C is incorrect, you can recover to any VM, no need to create a new one.

B is correct.

upvoted 1 times

  **Timock** 7 months, 2 weeks ago

Answer: Create a new VM

Create a new VM: Quickly creates and gets a basic VM up and running from a restore point.

Restore disk: Restores a VM disk, which can then be used to create a new VM.

Both of these options state creating a new VM and either doing it directly or attaching a restored VM disk. You could use an existing VM as well but that VM is probably already being used for something else. In the other question in this series it states what is TRUE and they are saying you can ONLY recover to specified locations which is not correct. In this answer it states SHOULD. You should use a new VM.

Replace existing: The current VM must exist. If it's been deleted, this option can't be used.

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms>

upvoted 4 times

  **Bere** 7 months, 2 weeks ago

The answer is C.

As described here:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms#choose-a-vm-restore-configuration>

You can Restore Virtual Machine to a new VM or replace disks on existing VM.

A => you don't need to delete the infected VM

B => you cannot restore to any VM (Linux or Windows), but you can restore to a new Windows VM or to the existing Windows VM

C => this option is valid

D => you cannot restore to an on-premise VM

upvoted 1 times

  **30th** 7 months, 2 weeks ago

Selected Answer: C

It is not possible to "restore the vm TO any vm".

- I can restore a vm to a NEW vm

- I can restore a vm REPLACING any other vm

- I can restore FILES to any other vm.

Doesn't matter what I do, it is better to shutdown the infected VM, but not to delete it until the restore process is finished.

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: C

C is correct

upvoted 1 times

  **OpOmOp** 10 months ago

Replace existing: You can restore a disk, and use it to replace a disk on the existing VM.

The current VM must exist. If it's been deleted, this option can't be used.

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms>

upvoted 1 times

  **4557af7** 10 months ago

Selected Answer: C

It should be C

upvoted 1 times



  **Wiz78** 10 months, 1 week ago



be careful at wording, it says you should (so where is recommended not where you can)..so it should be C as is safe way to go

upvoted 1 times



  **justjeroen** 11 months, 2 weeks ago

What is wrong with A?
You delete the compromised VM and restore the VM from backup.
What is the added value for another VM?
upvoted 1 times

  **Raseekara** 10 months, 1 week ago
May be due to SID involvement
upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago
Answer C (You should restore the VM to a new Azure VM) is a better choice. This approach ensures you're working with a completely uncontaminated, fresh environment, thereby significantly reducing the risk of any remnants of the ransomware affecting your new setup.

However, it should be noted that this option should ideally be combined with the deletion of the infected VM (A) to mitigate any risk of spreading the ransomware further. This isn't explicitly mentioned in option C but is a critical step in the recovery process. So, while C is the better answer among the provided options for where to restore the VM, ensure to first delete the infected VM as a preparatory step.
upvoted 5 times

  **01525bd** 1 year, 1 month ago
gpt v4 ansewr:
The best practice in this scenario, to maintain security and prevent the spread of ransomware, would be to delete the infected VM and then restore the clean backup to a new VM. This prevents the ransomware from potentially remaining on the system or affecting other VMs within the same environment.

Therefore, the most appropriate action would be:

A. You should restore the VM after deleting the infected VM.

This answer ensures that the infected VM is completely removed and that the clean, backed-up version is restored, minimizing the risk of the ransomware persisting or spreading.
upvoted 1 times

You administer a solution in Azure that is currently having performance issues.

You need to find the cause of the performance issues pertaining to metrics on the Azure infrastructure.



Which of the following is the tool you should use?


- A. Azure Traffic Analytics
- B. Azure Monitor
- C. Azure Activity Log
- D. Azure Advisor

Correct Answer: B

Community vote distribution



B (100%)


-   **Madbo**

Highly Voted 

 2 years ago

B. Azure Monitor is the tool used to collect and analyze performance metrics and logs in Azure. It provides insights into the performance of Azure resources, applications, and workloads, and helps identify and troubleshoot issues related to availability, performance, and security. Azure Traffic Analytics is used to monitor and analyze network traffic, Azure Activity Log provides insights into activities performed on Azure resources, and Azure Advisor provides recommendations for improving the performance, security, and reliability of Azure resources.



upvoted 34 times
-   **kerker**

Highly Voted 



 3 years, 10 months ago


Yes Correct

<https://docs.microsoft.com/en-us/azure/architecture/framework/scalability/monitor-infrastructure>

upvoted 24 times
-   **jackdryan** 2 years, 2 months ago

B is correct



upvoted 3 times
-   **JL2000**

Most Recent 

 3 weeks, 1 day ago



Selected Answer: B

In today's exam 13-04-2025

upvoted 2 times
-   **Mark74** 5 months ago



Selected Answer: B

B is correct, Azure Monitor

upvoted 1 times
-   **minura** 5 months, 2 weeks ago

Selected Answer: B



Correct asnwer is B

upvoted 1 times
-   **EleChie** 7 months, 2 weeks ago



Answer is correct.

Some information about Azure Traffic Analytics: Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud. With traffic analytics, you can:

- * Visualize network activity across your Azure subscriptions and identify hot spots.
 - * Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks.
 - * Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity.
 - * Pinpoint network misconfigurations leading to failed connections in your network.

upvoted 3 times
-   **EleChie** 3 years, 4 months ago

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

upvoted 1 times
-   **Nico1973** 7 months, 2 weeks ago

Answer: The tool that you should use to find the cause of the performance issues pertaining to metrics on the Azure infrastructure is Azure Monitor.

Explanation:

- Azure Monitor is the correct tool for monitoring and diagnosing the performance issues of your Azure infrastructure. It provides a comprehensive

solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.

- Azure Traffic Analytics is focused on analyzing network traffic and security, not specifically performance issues.
- Azure Activity Log provides insight into operations that were performed on resources in your subscription, but it does not focus on performance metrics.
- Azure Advisor is a service that analyzes your configurations and usage telemetry against a set of best practices and provides recommendations, but it may not directly address performance issues related to metrics.

upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

  **robsoneuclides** 11 months, 1 week ago

Selected Answer: B

Monitor

upvoted 1 times

  **MCLC2021** 11 months, 4 weeks ago

Selected Answer: B



Azure Traffic Analytics: Network insights.
Azure Monitor: Comprehensive monitoring.
Azure Activity Log: Subscription events.
Azure Advisor: Best practice recommendations.

upvoted 1 times

  **tashakori** 1 year, 1 month ago

B is correct

upvoted 1 times

  **walezb** 1 year, 7 months ago

wally_vic8 B Correct

upvoted 1 times

  **stevegod0** 1 year, 7 months ago

B is correct

upvoted 1 times

  **Aquintero** 1 year, 9 months ago

Selected Answer: B

La respuesta es B

upvoted 2 times

  **dhivyamohanbabu** 1 year, 10 months ago

Correct answer B

upvoted 1 times

  **MarMar2022** 2 years, 1 month ago

Selected Answer: B

B is correct

upvoted 2 times

  **Mazinger** 2 years, 2 months ago

Selected Answer: B

You should use Azure Monitor to find the cause of performance issues pertaining to metrics on the Azure infrastructure. Azure Monitor provides comprehensive monitoring of Azure resources and workloads, and collects and analyzes data from multiple sources, such as performance counters, diagnostics logs, and Azure Activity Logs, to identify and diagnose issues.

upvoted 2 times

Your company has an Azure subscription that includes a Recovery Services vault.

You want to use Azure Backup to schedule a backup of your company's virtual machines (VMs) to the Recovery Services vault.


Which of the following VMs can you back up? Choose all that apply.

- A. VMs that run Windows 10.
- B. VMs that run Windows Server 2012 or higher.
- C. VMs that have NOT been shut down.
- D. VMs that run Debian 8.2+.
- E. VMs that have been shut down.

Correct Answer: *ABCDE*

Community vote distribution

ABCDE (58%)	BDE (23%)	Other
-------------	-----------	-------

  **RVivek** Highly Voted 6 months, 1 week ago

Selected Answer: ABCDE

Answer : ABCDE

Azure Backup supports backup of 64-bit Windows server operating system from Windows Server 2008.

Azure Backup supports backup of 64-bit Windows 10 operating system.



Azure Backup supports backup of 64-bit Debian operating system from Debian 7.9+.

Azure Backup supports backup of VM that are shutdown or offline.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas>

upvoted 11 times

  **Chuong0810** Highly Voted 7 months, 1 week ago

Selected Answer: BDE



The answer from Copilot

Azure Backup supports a wide range of operating systems, including various versions of Windows Server and Linux distributions like Debian.

Additionally, backups can be performed on VMs that are either running or shut down.

Azure Backup does not support backing up client operating systems like Windows 10. It is primarily designed for server operating systems and certain Linux distributions.

upvoted 6 times

  **sca88** 6 months ago

Copilot it's very helpfull but don't think that is God. Often it's wrong. Windows 10 is supported

<https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas>

I use copilot too, and it give me the same response that it gave to you. I reported the error and he answer as follow: " You're right, and I apologize for the confusion. According to the Azure Backup support matrix, Azure Backup does support backing up VMs running Windows 10. Here are the correct options:

A. VMs that run Windows 10: Supported.

B. VMs that run Windows Server 2012 or higher: Supported.



D. VMs that run Debian 8.2+: Supported.

E. VMs that have been shut down: Supported, with the backup being crash-consistent.

Both running and shut down VMs can be backed up, so Option C is also technically correct, but it doesn't add new information since both states are supported.



Thank you for pointing that out! If you have any more questions or need further clarification, feel free to ask"

upvoted 9 times

  **Ivanvazovv** 1 month, 3 weeks ago

Copilot invents stuff. Don't use it when you need accuracy.

upvoted 2 times

  **saadraaz** Most Recent 2 weeks, 2 days ago

Selected Answer: ABCDE

It is lot of detail, I went through several latest pages on Microsoft docuentation and you can trust the answer which is: A,B,C,D,E.

So, all are correct.

If someone is interested in details, respond to it and I will provide details and references.

upvoted 1 times

  **Ekramy_Elnaggar** 3 weeks, 2 days ago

Selected Answer: ABCDE

<https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas>
upvoted 1 times

  **TobeReto** 1 month, 2 weeks ago

Selected Answer: BDE

The correct answers are:
B. VMs that run Windows Server 2012 or higher
D. VMs that run Debian 8.2+
E. VMs that have been shut down

Explanation:

Windows Server 2012 or Higher: Azure Backup supports virtual machines running Windows Server 2012 or newer versions. This includes operating systems with official support for Azure Backup services.

Debian 8.2+: Azure Backup supports Linux distributions like Debian 8.2 and above. The OS compatibility must meet Azure Backup's requirements.

Shut Down VMs: Azure Backup can back up virtual machines, even if they are shut down. The backup process uses Azure's snapshot feature, which does not require the VM to be running.

Incorrect Options:

A. VMs that run Windows 10: Azure Backup does not support Windows 10 VMs for backup.

C. VMs that have NOT been shut down: This is a valid condition for backup, but it doesn't exclude shut down VMs. Both running and shut down VMs can be backed up.

upvoted 1 times

  **Ponpon3185** 2 months, 1 week ago

Selected Answer: ABCD

It seems that's ABCDE, but for my personal computer & test i use MARS Agent and when my Laptopt is down, backup make an error....So it's different with VM....(may be)....

upvoted 1 times

  **bpal** 3 months, 2 weeks ago

Selected Answer: BCDE

The question only states "Which of the following VMs can you back up?" so in this case B, C, D, E should be selected but A since that is a client OS.


upvoted 2 times

  **Abhisk127** 3 months, 3 weeks ago

Selected Answer: BCDE



Azure does support or not for Windows 10 backup?

upvoted 1 times

  **794fc80** 5 months, 1 week ago

Actually Win 10 here is not supported as the question does not specify that is 64 bits, as 32 is not supported I would answer BCDE.

upvoted 1 times

  **minura** 5 months, 2 weeks ago

Selected Answer: BDE

OS Support:

Windows Server 2012 or higher: Supported.

Debian 8.2+: Supported as Azure Backup supports a variety of Linux distributions, including Debian 8.2 and later versions.

VM power state is NOT a problem. Azure Backup can back up stopped VMs. The process captures the latest state of the disk(s).

So the answer "VMs that have NOT been shut down" While this is technically possible, it is not relevant to the question since Azure Backup works for both running and stopped VMs. The option focuses on whether "not being shut down" is a prerequisite, which it is not.


upvoted 1 times

  **MJONESAUS17** 5 months, 3 weeks ago

Selected Answer: BD



I fail to understand, how can you backup to something, that has been shutdown? How is that VM gonna respond?

upvoted 1 times

  **MJONESAUS17** 5 months, 3 weeks ago

My bad I failed to understand the question.

upvoted 1 times

  **1e65755** 6 months, 2 weeks ago

Selected Answer: BCDE

windows client OS is not supported.

upvoted 1 times

  **DT95** 6 months, 2 weeks ago

Selected Answer: BDE

Correct answer: BDE

For Azure Backup with a Recovery Services vault, the following VMs can be backed up:

B. VMs that run Windows Server 2012 or higher.

Azure Backup supports Windows Server 2012 and higher (including Windows Server 2016 and 2019). These versions are fully supported for backup to an Azure Recovery Services vault



D. VMs that run Debian 8.2+.

Azure Backup supports several Linux distributions, including Debian 8.2 and above. This ensures that VMs running these versions of Linux can be backed up using Azure Backup

E. VMs that have been shut down.

Azure Backup can back up VMs even if they are shut down, as long as they are in a stopped (deallocated) state. This makes it possible to back up a VM without having it running, which is useful for cost-saving and backup scheduling

upvoted 1 times

  **Dankho** 6 months, 2 weeks ago

Selected Answer: BCDE

Everything except windows 10

upvoted 1 times

  **Vinayak30** 6 months, 3 weeks ago

B. VMs that run Windows Server 2012 or higher:

Azure Backup supports Windows Server 2012 or higher versions for VM backup.

D. VMs that run Debian 8.2+:

Azure Backup supports Linux-based VMs, including Debian 8.2 and higher versions.

E. VMs that have been shut down:

Azure Backup can back up VMs even if they have been shut down, as long as they are not deallocated (stopped but not deleted).

Explanation for the others:

A. VMs that run Windows 10:

Azure Backup does not support the backup of VMs running client operating systems like Windows 10.

C. VMs that have NOT been shut down:

This option is misleading because VMs can be backed up whether they are running or shut down, as long as they are not deallocated.



So the correct answers are B, D, and E.

upvoted 1 times

  **Bogey** 2 months ago

<https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas#operating-system-support-windows>

upvoted 1 times

  **happpieee** 6 months, 2 weeks ago

Windows 10 could be backup with Azure Backup: <https://azure.microsoft.com/en-us/blog/announcing-backup-of-windows-10-machines-using-azure-backup/>

upvoted 1 times

  **eduardovzermeno** 7 months ago

I found this information:

After enabling backup:

The Backup service installs the backup extension whether or not the VM is running.

An initial backup will run in accordance with your backup schedule.

When backups run, note that:


A VM that's running has the greatest chance for capturing an application-consistent recovery point.

However, even if the VM is turned off, it's backed up. Such a VM is known as an offline VM. In this case, the recovery point will be crash-consistent.

Explicit outbound connectivity isn't required to allow backup of Azure VMs.

Maybe it can be helpful.

upvoted 1 times

  **AndyFil** 7 months, 1 week ago

Selected Answer: BCDE

Only server versions of Windows are supported

upvoted 2 times

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-AzureADUser cmdlet for each user.

Does this meet the goal?



- A. Yes
- B. No


Correct Answer: B

Community vote distribution

B (90%)

10%

 **NaoVaz**



Highly Voted 


 2 years, 7 months ago

"New-AzureADUser" is for creating new Azure AD users not inviting Guests.

To invite using Powershell one should use the "New-AzureADMSInvitation" cmdlet.

upvoted 21 times



 **Mev4953**

Highly Voted 

 7 months, 2 weeks ago



#Read external users from CSV file
\$GuestUsers = Import-CSV "C:\Temp\GuestUsers.csv"
\$i = 0;
\$TotalUsers = \$GuestUsers.Count
#Iterate users and send guest invite one by one
Foreach(\$GuestUser in \$GuestUsers)
{
\$GuestUserName = \$GuestUser.'UserName'
\$GuestUserEmail = \$GuestUser.'EmailAddress'

\$i++;
Write-Progress -activity "Processing \$GuestUserName - \$GuestUserEmail" -status "\$i out of \$TotalUsers completed"
Try
{
#Send invite
\$InviteResult = New-AzureADMSInvitation -InvitedUserDisplayName \$GuestUserName -InvitedUserEmailAddress \$GuestUserEmail -
InviteRedirectURL https://myapps.microsoft.com -SendInvitationMessage \$true
Write-Host "Invitation sent to \$GuestUserName (\$GuestUserEmail)" -f Green
}
catch
{
Write-Host "Error occurred for \$GuestUserName (\$GuestUserEmail)" -f Yellow
Write-Host \$_ -f Red
}
}
upvoted 15 times

 **Mev4953** 2 years, 8 months ago



Create with invitation could be better option. You can also create new user with "New-AzureADUser". But i am not sure about yes or not. there is no issue about "invitation". It is about "need to create" guest users. If you have better explanation, I am looking forward to it :)

upvoted 3 times

 **jackdryan** 2 years, 2 months ago



B is correct


upvoted 5 times

 **18c2076** 1 year, 1 month ago

no sht sherlock

upvoted 1 times

 **Ponpon3185**

Most Recent 

 2 months, 1 week ago

Selected Answer: B

It's a Bulk Create so : <https://learn.microsoft.com/en-us/entra/identity/users/users-bulk-add>.
To my mind and if i well understood B is correct

upvoted 1 times

  **selvakarthick** 2 months, 3 weeks ago

Selected Answer: A



AZ 104 stopped asking bulk users addition questions

upvoted 1 times

  **selvakarthick** 2 months, 3 weeks ago

Delete this LOL

upvoted 1 times

  **Vinny** 2 months, 3 weeks ago

Selected Answer: B

New-AzureADMSInvitation



upvoted 2 times

  **PixelG** 3 months ago

Selected Answer: B

Ans:- B. as New-AzureADUser would need parameter for guest account, and this command will create usual new user accounts.


upvoted 1 times

  **minura** 5 months, 2 weeks ago

Selected Answer: B

To invite using Powershell we should use the "New-AzureADMSInvitation" cmdlet.

upvoted 1 times

  **minura** 5 months, 2 weeks ago

The New-AzureADUser cmdlet is used to create new users in Azure AD, but it is not suitable for creating guest user accounts.

upvoted 1 times

  **[Removed]** 7 months, 3 weeks ago

Selected Answer: B

B is correct

You create a PowerShell script that runs the New-AzureADMSInvitation cmdlet for each external user.

upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: B

B is corerct

upvoted 1 times

  **vrn1358** 8 months, 3 weeks ago

This question in not clear. because if the intention of the question is to creating guest users, so we can create guest users with this command: New-AzureADUser and the parmeter:

-UserType. Therefore we can choose Yes for correct answer.

but, if the intension of the question is only the command New-AzureADUser (without specific parameter like -UserType) then the answer should be No.

upvoted 1 times

  **Nico1973** 9 months, 4 weeks ago

Answer: B. No

Explanation: Running the New-AzureADUser cmdlet in PowerShell does not directly create guest user accounts in an Azure AD tenant. The New-AzureADUser cmdlet is typically used to create new user accounts within the organization's Azure AD, not for creating guest user accounts for external users. To achieve the goal of creating guest user accounts for the 500 external users in contoso.com, a different approach or command should be used, such as inviting external users as guests using the appropriate Azure AD cmdlets or methods.

upvoted 1 times

  **7658b84** 11 months, 1 week ago


For EntraID, the powershell command is New-MgInvitation.

upvoted 2 times

  **tashakori** 1 year, 1 month ago

No is right



upvoted 2 times

  **mojo86** 1 year, 1 month ago

A is correct if used with the -UserType "Guest" parameter.

The New-AzureADUser cmdlet is used in Azure Active Directory (Azure AD) to create a new user account. The -UserType "Guest" parameter specifies that the new user should be created as a guest user. Guest users are typically users from outside the Azure AD organization, such as partners or customers, who need access to resources within the organization. Creating a guest user allows you to grant them access to specific resources without requiring them to be a member of your organization's Azure AD directory.

upvoted 4 times

  **30th** 1 year, 2 months ago

Selected Answer: A

I am not sure about B. According to the task the account must be created user "in contoso.com". Invited users won't be a real members of contoso.com domain. Users are invited with their own E-Mails.

upvoted 1 times

  **Saurabh_Bhargav** 1 year, 2 months ago

B is correct

upvoted 1 times

  **photon99** 1 year, 6 months ago

New-AzureADMSInvitation is realted to Azure AD Powershell, why its included in AZ 104?

upvoted 2 times

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: From Azure AD in the Azure portal, you use the Bulk create user operation.

Does this meet the goal?



- A. Yes
- B. No


Correct Answer: B

Community vote distribution

B (93%)

7%

-  **gabyrever**

Highly Voted 



 2 years, 7 months ago

Selected Answer: B



"Bulk Create" is for new Azure AD Users.

For Guests:



 - Use "Bulk invite users" to prepare a comma-separated value (.csv) file with the user information and invitation preferences
 - Upload the .csv file to Azure AD
 - Verify the users were added to the directory


upvoted 51 times
-  **jackdryan** 2 years, 2 months ago

B is correct

upvoted 3 times
-  **meeko86** 2 years, 4 months ago

Agree answer is B



upvoted 3 times
-  **km_2022**


Highly Voted 

 2 years, 3 months ago

Answer is B - Bulk Invite would be the option not Bulk Create

Login to Azure Active Directory Admin Center <https://aad.portal.azure.com> Click on "Users" >> Click on "New Guest User" from the toolbar >> Choose "Invite User" and then click on "I want to invite guest users in bulk" (You can also use "Bulk Invite" under "Bulk Activities" to invite multiple external users.)

upvoted 7 times
-  **TobeReto**



Most Recent 

 1 month, 2 weeks ago

Selected Answer: B



The New-AzureADUser cmdlet is used to create regular users in Azure Active Directory, not guest user accounts. To create guest accounts for external users, you need to use the New-AzureADMSInvitation cmdlet, which is specifically designed for inviting external users as guest accounts in Azure AD.

If you'd like, I can guide you on using the correct cmdlet or scripting process for this task. Let me know!

upvoted 1 times
-  **Flip46** 2 months, 2 weeks ago

Selected Answer: B

The solution you mentioned does not meet the goal. The "Bulk create user" operation in Azure AD is used for creating multiple internal users, not guest users. To create guest user accounts for external users, you should use the "Bulk invite user" feature in Azure AD. This feature allows you to invite multiple external users as guests by uploading a CSV file with their details.

upvoted 1 times
-  **Mark74** 5 months ago

Selected Answer: B

B is correct, remeber guest users

upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago

Selected Answer: B

B is corerct
upvoted 1 times

🗨️ 👤 **Nico1973** 9 months, 4 weeks ago

Answer: B. No
Explanation: The "Bulk create user" operation in Azure AD is not designed for creating guest user accounts for external users. This operation is specifically used for creating user accounts within the Azure AD tenant, not for creating guest accounts. To create guest user accounts for external users, you would typically need to use a different method such as inviting users via the Azure portal, Azure AD PowerShell module, Microsoft Graph API, or Azure AD B2B collaboration features.
upvoted 2 times

🗨️ 👤 **Chesterfield** 10 months, 1 week ago

Selected Answer: B

B, It is "Bulk invite" instead of "Bulk create"
upvoted 1 times

🗨️ 👤 **3c5adce** 11 months, 4 weeks ago

No, this solution does not meet the goal.

The "Bulk create user" operation in Azure AD is typically used for creating new users directly within your Azure AD tenant, not for creating guest user accounts for external users. To bulk invite external users as guests to your Azure AD tenant, you should use the "Bulk invite" operation, which specifically handles guest invitations. This process involves uploading a CSV file with the required information and sending invitations to these external users to join your Azure AD as guests.
upvoted 1 times

🗨️ 👤 **Surs** 1 year, 4 months ago

Sorry, it says bulk create, that is wrong.
Bulk invite works from portal, so in this case, answer is B
upvoted 1 times

🗨️ 👤 **Surs** 1 year, 4 months ago

Answer A:
If you use Microsoft Entra B2B collaboration to work with external partners, you can invite multiple guest users to your organization at the same time.

<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite>
upvoted 1 times

🗨️ 👤 **kamalpur** 1 year, 9 months ago

This question is explained in below video that how can we perform same operation using azure portal and PowerShell commandline.

upvoted 2 times

🗨️ 👤 **dhivyamohanbabu** 1 year, 10 months ago

A is correct
upvoted 1 times

🗨️ 👤 **dhivyamohanbabu** 1 year, 10 months ago

Correct answer A
upvoted 1 times

🗨️ 👤 **rishisoft1** 1 year, 11 months ago

To invite Guest user, need 3 fields , email, Full n name and Invited user type. use type is missing in the question, so Answer I am expecting to be 'B'
upvoted 2 times

🗨️ 👤 **Madbo** 2 years ago

Solution B using the Bulk create user operation from Azure AD in the Azure portal would meet the goal of creating a guest user account in contoso.com for each of the 500 external users.
upvoted 1 times

🗨️ 👤 **bcristella** 2 years, 1 month ago

B is correct, but A it's right too.

If you use Azure Active Directory (Azure AD) B2B collaboration to work with external partners, you can invite multiple guest users to your organization at the same time. In this tutorial, you learn how to use the Azure portal to send bulk invitations to external users. Specifically, you'll follow these steps:
Use Bulk invite users to prepare a comma-separated value (.csv) file with the user information and invitation preferences
Upload the .csv file to Azure AD
Verify the users were added to the directory

Link: <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite?source=recommendation>
upvoted 3 times

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-AzureADMSInvitation cmdlet for each external user.



Does this meet the goal?


- A. Yes
- B. No

Correct Answer: A

Community vote distribution

A (83%)B (17%)

-  **abcduio**



Highly Voted 

 7 months, 2 weeks ago



i use this script almost every day, i think what this question is asking the main command to use for creating guest users. it didn't say that other commands are not necessary, depends how you read it, it could be wrong or right. but i will still choose A for this question.


Below is my script.

foreach (\$email in \$invitations)
{New-AzureADMSInvitation `
-InvitedUserEmailAddress \$email.InvitedUserEmailAddress `
-InvitedUserDisplayName \$email.Name `
-InviteRedirectUrl https://myapps.microsoft.com `
-InvitedUserMessageInfo \$messageInfo `
-SendInvitationMessage \$true
}
}

upvoted 15 times
-  **xRiot007** 1 year, 11 months ago

Spot on. People forget that the redirect URL can simply be passed as a param.

upvoted 6 times
-  **lumax007**

Most Recent 

 1 month, 2 weeks ago



Selected Answer: A

nvite a new external user to your directory
New-AzureADMSInvitation -InvitedUserEmailAddress someexternaluser@externaldomain.com -SendInvitationMessage \$True -InviteRedirectUrl "http://myapps.microsoft.com"

Using the cmdlet in this example, an email is sent to the user who's email address is in the -InvitedUserEmailAddress parameter. When the user accepts the invitation, they are forwarded to the url as specified in the -InviteRedirectUrl parameter

<https://github.com/Azure/azure-docs-powershell-azuread/blob/main/azureadps-2.0-preview/AzureAD/New-AzureADMSInvitation.md>



upvoted 1 times

 **Ponpon3185** 2 months, 1 week ago

Selected Answer: B

I asked this question to an MVP P.Paiola and more easy is Bulk Invite



upvoted 1 times

 **Ponpon3185** 2 months, 1 week ago

Selected Answer: B

Bulk Invite could be a good answer no?

upvoted 1 times

 **Jaafer09** 7 months, 2 weeks ago

es, creating a PowerShell script that runs the New-AzureADMSInvitation cmdlet for each external user would meet the goal of creating a guest user account in contoso.com Azure AD tenant for each of the 500 external users.

Here are the high-level steps:

Install and import the Azure AD PowerShell module.
Connect to your Azure AD tenant using the Connect-AzureAD cmdlet.
Read the CSV file that contains the names and email addresses of the external users.
Loop through the rows in the CSV file, and for each row, run the New-AzureADMSInvitation cmdlet to create a guest user account for the external

user. You can use the -SendInvitationMessage switch to send an invitation email to the external user. Repeat the above steps for each external user in the CSV file. This approach would automate the process of creating guest user accounts in contoso.com Azure AD tenant and allow you to create the accounts in bulk.

upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: A



A is corerct

upvoted 1 times

  **3c5adce** 1 year ago

I used ChatGPT to confirm - the answer is A:
Yes, using the New-AzureADMSInvitation cmdlet in a PowerShell script to invite each external user from the CSV file would meet the goal of creating a guest user account in the contoso.com Azure AD tenant for each external user. This cmdlet is specifically designed for inviting external users to an Azure AD tenant as guests, making it suitable for this scenario.

upvoted 2 times

  **MelKr** 1 year, 1 month ago

Current documentation is using the new Graph Powershell-Command "New-MgInvitation": <https://learn.microsoft.com/en-us/entra/external-id/bulk-invite-powershell>. Everything else still applies. So A would be valid for new command as well. The question may be updated after October 26, 2023.

upvoted 4 times

  **Amir1909** 1 year, 2 months ago

Yes is correct

upvoted 1 times

  **Samuel77** 1 year, 5 months ago

This is correct

upvoted 1 times

  **AMEHAR** 1 year, 8 months ago

Selected Answer: A

New-AzureADMSInvitation is correct command <https://learn.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0> . For the Bulk user
foreach (\$email in \$invitations)
{New-AzureADMSInvitation `
-InvitedUserEmailAddress \$email.InvitedUserEmailAddress `
-InvitedUserDisplayName \$email.Name `
-InviteRedirectUrl https://myapps.microsoft.com `
-InvitedUserMessageInfo \$messageInfo `
-SendInvitationMessage \$true
}

upvoted 1 times

  **GoldenDisciple2** 1 year, 8 months ago

Selected Answer: A

Reading through the comments to see if there is any good discussions. I see in the documentation, when running the New-AzureADMSInvitation that you'll have to put a -InviteRedirectURL parameter in the command so I feel that should be sufficient even though the CSV file doesn't contain the appropriate fields therefor I say it's yes. A

upvoted 1 times

  **james2033** 1 year, 9 months ago

Selected Answer: A

We can use PowerShell for invite a list of users (even use CSV file), see <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/bulk-invite-powershell#send-bulk-invitations> .

upvoted 1 times

  **dhivyamohanbabu** 1 year, 10 months ago

Correct answer A

upvoted 1 times

  **carlosFS** 1 year, 10 months ago

A CORRECTA

CSV FOR POWERSHELL : In Microsoft Excel, create a CSV file with the list of invitee user names and email addresses. Make sure to include the "Name" and "InvitedUserEmailAddress" column headings.

CSV FOR PORTAL:Required values are:

"Email address to invite" - the user who will receive an invitation

"Redirection url" - the URL to which the invited user is forwarded after accepting the invitation. I

upvoted 3 times

  **Vanilla007** 1 year, 11 months ago

I think redirection URL is mandatory if we are doing it via Azure portal. But in this question it is asking to pass a ps command. SO I think the solution meets the requirement and the answer is A

upvoted 2 times

  **cvalladares123** 2 years ago

Answer should be B) No - Check the following document: <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/bulk-invite-powershell> - "Send bulk invitations" -> "The script sends an invitation to the email addresses in the Invitations.csv file" - While the question states that the cmdlet should be used once per user, Microsoft documentation states that it should be done once as the comand releases invitations for addresses in .CSV File

upvoted 2 times

HOTSPOT -

You have an Azure subscription named Subscription1 that contains a resource group named RG1.

In RG1, you create an internal load balancer named LB1 and a public load balancer named LB2.

You need to ensure that an administrator named Admin1 can manage LB1 and LB2. The solution must follow the principle of least privilege.

Which role should you assign to Admin1 for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To add a backend pool to LB1:

	▼
Contributor on LB1	
Network Contributor on LB1	
Network Contributor on RG1	
Owner on LB1	

To add a health probe to LB2:

	▼
Contributor on LB2	
Network Contributor on LB2	
Network Contributor on RG1	
Owner on LB2	

Answer Area

To add a backend pool to LB1:

	▼
Contributor on LB1	
Network Contributor on LB1	
Network Contributor on RG1	
Owner on LB1	

Correct Answer:

To add a health probe to LB2:

	▼
Contributor on LB2	
Network Contributor on LB2	
Network Contributor on RG1	
Owner on LB2	

The Network Contributor role lets you manage networks, but not access them.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

🗨️  **alen995454** Highly Voted 7 months, 2 weeks ago

The given answer is incorrect:

Box 1. Network Contributor on RG1

Box 2. Network Contributor on RG1

upvoted 170 times

🗨️  **SHAHIN_STA** 4 months, 3 weeks ago

Wrong

-----why?

1. To add a backend pool to LB1:

Network Contributor on LB1

Reason: This role allows managing the Load Balancer's network settings. Assigning it only to LB1 follows the Principle of Least Privilege by limiting access.

2. To add a Health Probe to LB2:

Network Contributor on LB2

Reason: This role lets the user create and manage Health Probes. Giving access only to LB2 keeps permissions limited and secure.

upvoted 5 times

  **achu_r_27** 4 months, 2 weeks ago

<https://learn.microsoft.com/en-us/answers/questions/1288486/network-contributor-explains-network-contributor-can't-create-backend-VMs>.
So my ans 1)Contributor on LB1 2) Network contributor on LB2

upvoted 3 times

  **Jaiiee** 4 months, 4 weeks ago

For LB1 (Internal Load Balancer):

Network Contributor

Reason: This role grants full permissions to manage all aspects of networking resources, including internal load balancers.

For LB2 (Public Load Balancer):

Network Contributor

Reason: Similar to LB1, managing a public load balancer requires the Network Contributor role.

Explanation:

The Network Contributor role is the minimum role required to manage load balancers, including configuration changes, backend pool management, and health probes. Assigning it at the resource or resource group level ensures Admin1 can manage these specific resources without excessive permissions to unrelated services.

upvoted 1 times

  **Jaiiee** 4 months, 4 weeks ago

Assigning the Network Contributor role at the RG1 level would allow Admin1 to manage all networking resources in the resource group, not just LB1 and LB2. While this may seem convenient, it violates the principle of least privilege, which dictates that a user should only have permissions for the specific resources they need to manage.

upvoted 2 times

  **Abd99** Highly Voted  7 months, 2 weeks ago

Network Contributor on LB1

Network Contributor on LB2

Network Contributor role on LB1 and LB2 is the correct answer. With this role user can add create a backend address without actually adding the actual IP addresses. Network contributor can also create and modify health probe.

If the user wants to add address to backend pools (eg: IPs from a VNet or entire subnet) then a Network Contributor role is required at the resource group level (or atleast on VNet)

upvoted 53 times

  **XristophD** 2 years, 5 months ago

this answer is not correct, just tested in a lab environment.

Network-Contributor needs to be given on the Resource Group in question, not only the LB - for both actions, adding a Health-Probe and adding a Backend-Pool a validation on the RG-level is triggered.



Not having the Network Contributor role on RG level will produce the following error mesage for adding a Health Probe:

Additional details from the underlying API that might be helpful: The client 'test@<domain.ltd>' with object id '<some-object-id>' does not have authorization to perform action 'Microsoft.Resources/deployments/validate/action' over scope '/subscriptions/<subscriptionId>/resourceGroups/pb-weu-d-testexam/providers/Microsoft.Resources/deployments/HealthProbe-20221125094430' or the scope is invalid.

Adding a backend pool fails to create the deployment at all.

Both actions work with Network Contributor role on the Resource Group level.



upvoted 32 times

  **FNog** 2 years, 2 months ago

Both Load Balancers already exist, though...



Only management rights are requested so, LB1 and LB2.

upvoted 5 times

  **jackill** 1 year, 9 months ago

Actually the Network Contributor role (<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>) has "Microsoft.Resources/deployments/*" among allowed actions, but from the error you reported it appears that the HealthProbe resource is not included in the scope path of the Load Balancer, but it appears to be a resource defined externally from the Load Balancer. Is this the reason of the failure? Is the Backend Pool defined externally too?

upvoted 1 times

  **DrMiyu** 2 years, 10 months ago

From Microsoft Network Contributor = "Lets you manage networks, but not access to them.". RG contributor would give you right on everything in the RG so too much

upvoted 8 times

  **mrmccoy007** Most Recent  1 month, 3 weeks ago

I think what is tripping people up in the first box is whether we are creating or adding an existing backend pool. You need RG1 if you are creating a backend pool but this says adding a backend pool which is a function of the loadbalancer configuration.

upvoted 1 times

  **Mitko_V_Milkov** 2 months, 2 weeks ago



Network Contributor to LB1 and LB2. The statement says that the LBs are already created, and Admin 1 needs these right with least privileges. You are not Admin 1...Admin 1 is another user and giving him "Contributor to the RGs" is too broad.

upvoted 1 times

  **CloudEngJS** 5 months, 1 week ago

Tested and confirmed in a lab, the correct answers are NetworkContributor on RG1



upvoted 1 times

  **jorex535** 5 months, 3 weeks ago

Copilot answer:
"Both solutions are valid, but the preferable one depends on your specific needs and management preferences:

Assigning the Network Contributor role at the resource group level (RG1):
Pros: Simplifies role management by granting Admin1 permissions to manage all network-related resources within the resource group, including both LB1 and LB2.
Cons: Admin1 will have broader access, which might include other network resources in RG1 that they don't need to manage.
Assigning the Network Contributor role directly to LB1 and LB2:
Pros: Follows the principle of least privilege more strictly by limiting Admin1's access to only the specific load balancers they need to manage.
Cons: Requires more granular role assignments, which can be more complex to manage if there are many resources.
If you want to keep things simple and Admin1 needs to manage multiple network resources within RG1, assigning the role at the resource group level is preferable. However, if you want to strictly limit Admin1's access to only the load balancers, assigning the role directly to LB1 and LB2 is the better choice."

upvoted 1 times

  **bacana** 6 months, 1 week ago

Network contributor to LB is the latest permission, but not work in real life. You need be network contributor to RG1

upvoted 1 times

  **zeuge** 6 months, 2 weeks ago



According to the response from Microsoft, which specifies the permissions of the 'Network Contributor' role in the resource group LB, the correct answer, in my opinion, looks like this:
Box 1. Network Contributor on LB1
Box 2. Network Contributor on RG1

upvoted 1 times

  **zeuge** 6 months, 2 weeks ago

Network Contributor on LB can't add a health probe.

upvoted 1 times

  **Dankho** 6 months, 2 weeks ago

I'm glad the discussion basically has every possibility.

upvoted 7 times

  **happpieee** 6 months, 2 weeks ago

Network Contributor on LB1 and LB2 (to either add backend pool or health probe).
Source: <https://learn.microsoft.com/en-us/azure/role-based-access-control/permissions/networking#microsoftnetwork>

upvoted 1 times

  **happpieee** 6 months, 2 weeks ago

Network Contributor for LB1 (add backend pool)
Network Contributor for LB2 (add healthprobe)
Source: <https://learn.microsoft.com/en-us/azure/role-based-access-control/permissions/networking#microsoftnetwork>

upvoted 1 times

  **rikininetysix** 7 months, 2 weeks ago

The correct answer would be -

1. Network Contributor on RG1
2. Network Contributor on LB2

The "Network Contributor" role provides permissions to manage network resources such as virtual networks, subnets, network interfaces, and IP addresses. While it does grant certain permissions related to load balancers, such as managing load balancing rules and probes, it does not provide the necessary permissions to add or modify backend VMs associated with the load balancer.

To add backend VMs to a load balancer, the user would require additional permissions, specifically the "Virtual Machine Contributor" role or higher. So, the Network Contributor on RG1 option would be the only viable option for the first answer.

Link - <https://learn.microsoft.com/en-us/answers/questions/1288486/network-contributor>

upvoted 4 times

  **Alandt** 7 months, 2 weeks ago

Come on guys, how is it possible that these questions are so confusing that the community can't even reach to a consensus for the right answer. So what's the correct answer here?

Network Contributor on RG1
Network Contributor on RG1

Or

Network Contributor on LB1

Network Contributor on LB2

upvoted 3 times

  **nmsshrwt** 1 year, 3 months ago

It is neither Ans is for health probe assign network contributor on RG level for backend pool assign owner on LB if not owner contributor on RG can do it

upvoted 1 times

  **[Removed]** 7 months, 3 weeks ago

WRONG

- Network Contributor on RG1

- Network Contributor on RG1

upvoted 1 times

  **[Removed]** 8 months ago

wrong

1st. Network Contributor on RG1

2nd. Network Contributor on RG1



upvoted 1 times

  **salihGamar** 8 months, 3 weeks ago

Yes, you can assign Admin1 the "Network Contributor" role directly to LB1 and LB2 instead of the entire resource group. This would follow the principle of least privilege more closely by limiting Admin1's permissions specifically to those two load balancers. So the Answer is correct! ..

Network Contributor on LB1 & Network Contributor on LB2 ..

upvoted 3 times

  **divzrajshekar123** 9 months, 1 week ago

Correct answer is :

box 1: 3 - network contributor access on RG1

box2: 3 - network contributor access on RG1

if we give network contributor access on LB level then we wont be able to access the Lb resource. hence network contributor access on resource level is required. I found out this after long lab session. hope its helps.

upvoted 4 times

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com and an Azure Kubernetes Service (AKS) cluster named AKS1.

An administrator reports that she is unable to grant access to AKS1 to the users in contoso.com.

You need to ensure that access to AKS1 can be granted to the contoso.com users.



What should you do first?

- A. From contoso.com, modify the Organization relationships settings.
- B. From contoso.com, create an OAuth 2.0 authorization endpoint.
- C. Recreate AKS1.
- D. From AKS1, create a namespace.

Correct Answer: B

Community vote distribution

B (86%)	8%
---------	----



-   **AlleyC** Highly Voted 2 years, 11 months ago

Selected Answer: B

Answer is correct B

Cluster administrators can configure Kubernetes role-based access control (Kubernetes RBAC) based on a user's identity or directory group membership. Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol



<https://docs.microsoft.com/en-us/azure/aks/managed-aad>

upvoted 76 times
-   **FredFrom** 6 months, 2 weeks ago

it does not address the specific issue described in the question, which is that the administrator is unable to grant access to the AKS cluster to users in contoso.com.



the issue here is not about configuring authentication mechanisms like OAuth 2.0; it's about ensuring that Azure AD integration is in place to allow access control for AKS.

Correct Answer: C. Recreate AKS1



upvoted 4 times
-   **tweedo** 2 years, 9 months ago

This seems to be a correct answer in scope of listed answers, but please mind that AKS now supports direct integration with AAD, the method using OAuth 2.0 is considered legacy:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>



upvoted 34 times
-   **jackdryan** 2 years, 2 months ago

B is correct



upvoted 2 times
-   **18c2076** Highly Voted 1 year, 1 month ago

as of late 2023 / early 2024 Azure Kubernetes Service is NO LONGER part of the exam. This question is defunct. Please review the MS provided documentation regarding the AZ104 exam:

<https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/az-104>

upvoted 26 times
-   **GlixRox** 11 months, 1 week ago



Glad you said this because I had never heard of this during my course.

upvoted 4 times
-   **a2675f7** Most Recent 2 weeks, 6 days ago

Selected Answer: C

You can only enable Azure Active Directory integration when you create your AKS cluster. It can't be added to an existing AKS cluster later. When you want to manage access to AKS using Azure AD identities, AKS must be integrated with Azure AD at the time of creation.

If it's not integrated, you can't use Azure AD users/groups to assign roles (e.g., viewer, contributor) at the Kubernetes level.

upvoted 1 times
-   **dhavalmodi** 1 month, 2 weeks ago

Selected Answer: C

Azure AD integration must be enabled during AKS cluster creation.

upvoted 1 times

  **SolimanAlali** 1 month, 3 weeks ago

Selected Answer: C

Correct Answer: C. Recreate AKS1

AKS must be created with Azure AD integration enabled. This setting cannot be modified after creation.

Azure AD integration for AKS must be enabled during cluster creation and cannot be added later.

If it was not enabled, the only solution is to delete and recreate the AKS cluster with Azure AD authentication.

After that, we can assign roles to Azure AD users to control access.



Why is B Incorrect?

- OAuth 2.0 authorization endpoints are used for application authentication and API access control, not for granting users access to an AKS cluster.

- AKS integrates directly with Azure AD for authentication and role-based access control (RBAC).

- If Azure AD authentication was not enabled during the AKS cluster creation, the only way to fix it is to recreate the cluster with Azure AD integration enabled.

upvoted 1 times

  **James18** 3 months, 3 weeks ago

Selected Answer: B

Answer is correct B

upvoted 2 times

  **Nisita** 4 months, 3 weeks ago

Selected Answer: C

If Azure AD integration was not initially enabled during the creation of AKS1, and the administrator is unable to grant access to contoso.com users, the cluster might lack proper Azure AD integration. However, if the cluster already has Azure AD integration configured, the issue is likely related to proper setup of RBAC or permissions in Azure AD.

In this question, there is no explicit mention of whether Azure AD integration is already configured for the AKS cluster (AKS1). Therefore, we cannot assume it is enabled by default.

Given the ambiguity of the question, the safest assumption is that Azure AD integration is not configured, as it aligns with the reported issue ("unable to grant access"). This scenario is more common and consistent with real-world problems. Without explicit information stating that Azure AD integration is enabled, the correct action is to:

C. Recreate AKS1.

upvoted 1 times

  **SHAHIN_STA** 4 months, 3 weeks ago

Selected Answer: C

according to the official Microsoft Learn page, the Azure Kubernetes Service (AKS) is no longer part of the AZ-104 Azure Administrator certification exam as of late 2023. The current exam objectives focus on managing Azure identities and governance, implementing and managing storage, deploying and managing Azure compute resources, implementing and managing virtual networking, and monitoring and maintaining Azure resources.

For the most up-to-date information and exam preparation resources, you can refer to the official AZ-104 certification page on Microsoft Learn: [Microsoft Certified: Azure Administrator Associate](https://learn.microsoft.com/en-us/credentials/certifications/azure-administrator/).



upvoted 1 times

  **Jaiiee** 4 months, 4 weeks ago

Selected Answer: C

Azure Kubernetes Service (AKS) does not allow enabling Azure Active Directory (Azure AD) integration on an existing cluster that was not originally configured with it. If the AKS cluster (AKS1) was created without Azure AD integration, you cannot simply enable it later. Instead, you must recreate the cluster with Azure AD integration enabled.

upvoted 2 times

  **FredFrom** 6 months, 2 weeks ago

Selected Answer: C

When an administrator is unable to grant access to an AKS cluster for users in an Azure Active Directory (Azure AD) tenant, it typically indicates that the AKS cluster was not configured with Azure AD integration when it was initially created.

Azure AD integration must be enabled when the AKS cluster is created in order to manage access and authentication through Azure AD. If this integration was not enabled during the cluster's creation, users in the Azure AD tenant (in this case, contoso.com) cannot be assigned access. The only way to enable Azure AD integration after creation is to recreate the AKS cluster with the proper configuration.



upvoted 2 times

  **FredFrom** 6 months, 2 weeks ago

C. When an administrator is unable to grant access to an AKS cluster for users in an Azure Active Directory (Azure AD) tenant, it typically indicates that the AKS cluster was not configured with Azure AD integration when it was initially created.

Azure AD integration must be enabled when the AKS cluster is created in order to manage access and authentication through Azure AD. If this integration was not enabled during the cluster's creation, users in the Azure AD tenant (in this case, contoso.com) cannot be assigned access. The only way to enable Azure AD integration after creation is to recreate the AKS cluster with the proper configuration.

upvoted 1 times

  **loganvm** 6 months, 4 weeks ago

Correct Answer is C

To ensure that access to the Azure Kubernetes Service (AKS) cluster can be granted to the users in your Azure Active Directory (Azure AD) tenant (contoso.com), you should first:

C. Recreate AKS1.

This is because, when you create an AKS cluster, you can specify the Azure AD integration settings. If it was not configured correctly to allow access to users from the contoso.com tenant during the initial setup, recreating the cluster with the correct Azure AD integration settings is necessary to resolve the access issue.

Other options do not directly address the need for Azure AD integration with AKS.


upvoted 1 times

  **Chuong0810** 7 months, 1 week ago

Selected Answer: A

You need to integrate Azure AD with AKS. This often requires modifying the organization relationships settings in Azure AD

upvoted 1 times

  **Andre369** 7 months, 2 weeks ago

Selected Answer: A

Option A is the correct choice. By modifying the Organization relationships settings in the Azure AD tenant (contoso.com), you can establish the required connection between the Azure AD tenant and the AKS cluster. This configuration allows users in contoso.com to access and manage AKS resources.

Here's a high-level overview of the steps involved in this process:

Sign in to the Azure portal using an account with appropriate permissions in the contoso.com Azure AD tenant.



Navigate to the Azure AD tenant (contoso.com) settings.

Locate the Organization relationships settings and configure the necessary settings to establish the connection between Azure AD and AKS.

Follow any additional prompts or steps provided during the configuration process.

Once the Organization relationships settings are properly configured, the administrator should be able to grant access to AKS1 for the users in the contoso.com Azure AD tenant.

upvoted 4 times

  **JonHanes** 7 months, 2 weeks ago

This one had me confused between B and C, asking the Bing AI resulted in the following:

The question does leave out some important details that would help determine the most appropriate answer.

For instance, it doesn't specify whether Azure RBAC is enabled on the AKS cluster.

If Azure RBAC is not enabled, then the cluster would need to be recreated with Azure RBAC enabled (Option C).

However, if Azure RBAC is already enabled and the cluster is integrated with Azure AD, then creating an OAuth 2.0 authorization endpoint could be a valid first step (Option B).

The question also doesn't specify whether the users are part of the same Azure AD tenant as the AKS cluster or if they are external users.

If they are external users, additional steps might be needed to grant them access to the AKS cluster.


upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

  **Witbaas13** 8 months, 3 weeks ago

A.

This is because Azure Active Directory needs to be properly configured to grant access to AKS1. Modifying the organization relationships settings can help resolve issues related to user access.

upvoted 2 times

You have a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to grant three users named User1, User2, and User3 access to a temporary Microsoft SharePoint document library named Library1. You need to create groups for the users. The solution must ensure that the groups are deleted automatically after 180 days. Which two groups should you create? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. a Microsoft 365 group that uses the Assigned membership type
- B. a Security group that uses the Assigned membership type
- C. a Microsoft 365 group that uses the Dynamic User membership type
- D. a Security group that uses the Dynamic User membership type
- E. a Security group that uses the Dynamic Device membership type

Correct Answer: AC

Community vote distribution

AC (90%)5%

kennynelcon

Highly Voted

2 years, 11 months ago

Selected Answer: AC

Correct Answer: A and C
Only O365 groups support automatic deletion after 180 days.
upvoted 58 times

jackdryan

2 years, 2 months ago

A and C are correct
upvoted 7 times

ConanBarb

7 months, 2 weeks ago

Sorry y'all AC:s, but you're wrong
Correct, according to Microsoft own sample exam questions is: CD

Microsoft exam question answers:
"a security group that uses the dynamic membership type"
"a Microsoft 365 group that uses the dynamic membership type"

Corresponds to
A. a Microsoft 365 group that uses the Assigned membership type
B. a Security group that uses the Assigned membership type
x C. a Microsoft 365 group that uses the Dynamic User membership type
x D. a Security group that uses the Dynamic User membership type
E. a Security group that uses the Dynamic Device membership type

"Rationale: Groups that use dynamic membership rules reduce the overhead of access management by providing attribute-based membership and access to resources. Based on membership rules the membership, and resulting access, can be granted and removed automatically."

<https://learn.microsoft.com/en-us/certifications/resources/az-104-sample-questions>
upvoted 9 times

MrBlueSky

2 years, 2 months ago

This is a different question. The reason why A and C is correct is because the answer specifies that the group needs automatic deletion and that's only supported by Microsoft 365 groups.
upvoted 30 times

Lazylinux

Highly Voted

2 years, 10 months ago



i Agree A&C
Security groups are used to give group members access to applications, resources and assign licenses. Group members can be users, devices, service principals, and other groups.

Microsoft 365 groups are used for collaboration, giving members access to a shared mailbox, calendar, files, SharePoint site, and so on. Group members can only be users. With the increase in usage of Microsoft 365 groups and Microsoft Teams, administrators and users need a way to clean up unused groups and teams. A Microsoft 365 groups expiration policy can help remove inactive groups from the system and make things cleaner.

When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, team, etc.) are also deleted.

When a group expires it is "soft-deleted" which means it can still be recovered for up to 30 days.

upvoted 17 times

  **Afsan** 2 years, 4 months ago

Thanks

upvoted 1 times

  **4f45fce** Most Recent 3 weeks, 4 days ago

Selected Answer: AB

ChatGPT says that A and C are both related to SharePoint access, but only A supports automatic expiration, which is the key part of your question. So A, B is correct

upvoted 1 times

  **Bhuru** 3 months, 1 week ago

Selected Answer: AC

Security groups do not support expiration policies, it is only supported by Microsoft 365 groups, so A and C are correct.

upvoted 2 times

  **RealmTarget** 5 months ago

Selected Answer: AC

A & C are correct. Expiration policies only valid for Microsoft 365 groups.
<https://learn.microsoft.com/en-us/entra/identity/users/groups-lifecycle>



upvoted 2 times

  **Mark74** 5 months ago

Selected Answer: AC

A and C for me is correct



upvoted 1 times

  **Dankho** 6 months, 2 weeks ago

Selected Answer: AC

Both related to SharePoint, others are not.

upvoted 3 times

  **FredFrom** 6 months, 2 weeks ago

Selected Answer: AC

To meet the requirement of granting access to a SharePoint document library and ensuring that the groups are automatically deleted after 180 days, the solution should use Microsoft 365 groups with expiration policies. Security groups do not have built-in expiration policies.

Correct Answers:

- A. a Microsoft 365 group that uses the Assigned membership type
- C. a Microsoft 365 group that uses the Dynamic User membership type

upvoted 1 times

  **Xpinguser** 6 months, 3 weeks ago



Selected Answer: AE

Here's why:

Microsoft 365 Group (Assigned Membership): This option allows you to directly add User1, User2, and User3 to the group. Microsoft 365 groups are inherently linked to SharePoint sites, making it a good fit for document library access.

Security Group (Dynamic Device Membership - with limitations): While less conventional, this approach can work with some limitations. You can create a security group and configure dynamic membership based on a specific device property. However, this requires assigning a unique device to each user (User1, User2, User3) and setting the dynamic membership rule to include those specific devices. This can be cumbersome and not ideal for large numbers of users.

upvoted 1 times

  **Chuong0810** 7 months ago

Selected Answer: AB

For this scenario, the most appropriate choices are: A & B

Both options allow you to manually assign users (User1, User2, and User3) to the group and set an expiration policy to ensure the groups are deleted automatically after 180 days.

A is widely used for collaboration purposes and integrates well with Microsoft 365 services like SharePoint. B is more general-purpose but can be used similarly for managing access.

upvoted 2 times

  **stanislaus450** 7 months, 2 weeks ago

Selected Answer: AD

Anwser: A & D



To grant access to the temporary Microsoft SharePoint document library named Library1 for the users User1, User2, and User3, you should create the following groups:

Microsoft 365

A Microsoft 365 group that uses the Assigned membership type: This group allows you to explicitly assign members and manage their access. You can add User1, User2, and User3 to this group, granting them access to Library1. After 180 days, you can delete this group to ensure automatic cleanup.

A Security group that uses the Dynamic User membership type: This type of group dynamically adds or removes members based on specified criteria (such as user attributes or roles). You can configure this group to automatically include User1, User2, and User3 based on their attributes or roles. After 180 days, the group will no longer include these users, achieving the desired automatic deletion.

upvoted 2 times

  **Josh219** 7 months, 2 weeks ago

As of now, Azure AD does not offer an expiration policy feature for security groups. The expiration policy feature is specifically available for Microsoft 365 groups.

If you need to manage the lifecycle of security groups, you might consider implementing manual processes or using automation scripts with Azure AD PowerShell or Microsoft Graph API to periodically review and clean up unused groups.

So, correct is A & C



upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: AC

A & C are correct

upvoted 1 times

  **Nico1973** 9 months, 4 weeks ago

Answer: C and D

To grant User1, User2, and User3 access to the temporary Microsoft SharePoint document library named Library1 and ensure that the groups are automatically deleted after 180 days, you should create the following two groups:

- A Microsoft 365 group that uses the Dynamic User membership type
- A Security group that uses the Dynamic User membership type

upvoted 1 times

  **justjeroen** 11 months ago

The question states: Which 2 groups SHOULD you create?

Why Should i create 2groups in the first place? Why is 1 group not enough?

upvoted 1 times

  **rhv9** 6 months, 2 weeks ago

there are two different tenants

upvoted 1 times

  **Hommedollars** 11 months, 2 weeks ago

Selected Answer: AC

To meet the requirements of granting access to a temporary Microsoft SharePoint document library and ensuring that the groups are deleted automatically after 180 days, you need to create groups that support expiration policies. This functionality is supported by Microsoft 365 groups but not by security groups.

Therefore, the correct answers are:

- A. A Microsoft 365 group that uses the Assigned membership type
- C. A Microsoft 365 group that uses the Dynamic User membership type

These choices ensure that:

The groups are part of Microsoft 365, which supports group expiration policies.

The groups can be configured to automatically delete after 180 days.


Security groups do not support the automatic deletion feature based on expiration policies, making options B, D, and E incorrect for this scenario.

upvoted 2 times

  **Malkymagic** 11 months, 2 weeks ago

Why A and C? Why not just A? Is it something to do with the SPO library needs created with a group (365-Outlook) and then another 365 group for the users? So confused.

upvoted 3 times

  **Stunomatic** 6 months, 2 weeks ago

because each answer provide a complete solution.

upvoted 1 times

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table:

Name	Type	Member of
User1	Member	Group1
User2	Guest	Group1
User3	Member	None
UserA	Member	Group2
UserB	Guest	Group2

User3 is the owner of Group1.

Group2 is a member of Group1.

You configure an access review named Review1 as shown in the following exhibit:

Create an access review

Access reviews enable reviewers to attest user's membership in a group or access to an application.

* Review name:

Description:

* Start date:

Frequency:

Duration (in days):

End:

* Number of times:

* End date:

Users

Users to review:

Scope: ☒ Guest users only ☐ Everyone

* Group:

Reviewers

Reviewers:

Programs

Link to program:

Upon completion settings

Advanced settings

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

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
User3 can perform an access review of User1	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserB	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User3 can perform an access review of User1	<input type="radio"/>	<input checked="" type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input checked="" type="radio"/>
User3 can perform an access review of UserB	<input checked="" type="radio"/>	<input type="radio"/>

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

  **AlleyC** Highly Voted 7 months, 2 weeks ago

Tested in lab
Correct Answers:

User3 can perform an access review of User1 = No
User1 is a Member and not a Guest Account, Access Review specified Guests only.



User3 can perform an access review of UserA = No
User1 is a Member and not a Guest Account, Access Review specified Guests only.

User3 can perform an access review of UserB = No
Created Group 1 and Group 2, added Group 2 as a member in Group 1,
Added guest Accounts to Group 1 and Group 2,
In the Access Review results only the Guest Accounts in Group 1 appeared for review and "Not" the Guest accounts in Group 2.
upvoted 225 times

  **Wheels90** 1 year, 10 months ago


No, No, Yes
Reviewing a role with nested groups assigned: For users who have membership through a nested group, the access review will not remove their membership to the nested group and therefore they will retain access to the role being reviewed.

So, it will maintain the access.
upvoted 12 times



  **ggogel** 1 year, 5 months ago

I'm seeing this repeated over and over again without people actually understanding what this is about.

The sentence does not state anything about being able to REVIEW this user. Instead, this is about not applying changes made during a review process to a user from a nested group. The section in the documentation is called "Apply the changes" and not "Retrieve the results", what this question is actually about.
upvoted 6 times



  **Key94** 2 years, 9 months ago

If group 2 is a member of group 1, do the members of group 2 not get reviewed through that membership ?
upvoted 5 times

  **a6bd45e** 9 months, 3 weeks ago

Access Review supports nesting of groups.

upvoted 3 times

  **morito** 2 years, 2 months ago

This seems to be supported by the statement provided here by Microsoft themselves: <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-perform-azure-ad-roles-and-resource-roles-review#approve-or-deny-access>.

upvoted 2 times

  **Armina** Highly Voted 2 years, 11 months ago

User3 can perform an access review of User1. /No
User3 can perform an access review of UserA. /No
User3 can perform an access review of UserB. /No

Explanation:

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access. If you need to routinely review access, you can also create recurring access reviews.

Review1 reviews access for guest users who are member of Group1. The group owner is specified as the reviewer.

User3 is the owner of Group1. User2 is the only guest user in Group1.

Note: Dynamic groups and nested groups are not supported with the Access review process.

Reference: Create an access review of groups and applications in Azure AD access reviews : <https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

upvoted 57 times



  **MCLC2021** 1 year ago

When you add a nested group to another group, the members of the nested group do not inherit the ownership or administrative privileges of the parent group.

The owners of the parent group do not automatically become owners of the nested group.

Explanation in: https://www.youtube.com/watch?v=O032Kz-5R2Q&list=PLIKA5U_Yqgof3H0YWhzvarFixW9QLTr4S&index=18

upvoted 3 times

  **atilla** 2 years, 11 months ago

in think it NNY, guest users are included in nested groups, its not excluded in the link you provided

upvoted 22 times

  **Mat21445** 2 years, 9 months ago

You're right.

Look for possible scenarios with nested groups here:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-service-limits-restrictions>

upvoted 5 times

  **Lazylinux** 2 years, 10 months ago

U R right and Armina is WRONG..see my comments

upvoted 7 times

  **saadraaz** Most Recent 2 weeks, 2 days ago

Go through this very carefully, It is the correct answer with logic:

Statement 1: User3 can perform an access review of User1

Answer: No

Reason: User1 is a member-type user, and scope is "guest users only"

Statement 2: User3 can perform an access review of UserA

Answer: No

Reason: UserA is a member-type user and also, UserA is part of a nested group (Group2), not a direct member of Group1

Statement 3: User3 can perform an access review of UserB

Answer: No

Even though UserB is a guest, they are in a nested group (Group2), not directly in Group1.

Nested group users are not included in the access review

Final answer:

No, No, No.

upvoted 1 times

  **Jay_D_Lincoln** 2 months, 2 weeks ago

NNY

Answer is correct

From ms doc:

In a group review, nested groups will be automatically flattened, so users from nested groups will appear as individual users. If a user is flagged for removal due to their membership in a nested group, they will not be automatically removed from the nested group, but only from direct group membership.

upvoted 1 times

  **bpal** 3 months, 2 weeks ago

N,N,Y

The question is only asking if User3 can perform access review and not removal.

Per MS:

In a group review, nested groups will be automatically flattened, so users from nested groups will appear as individual users. If a user is flagged for

removal due to their membership in a nested group, they will not be automatically removed from the nested group, but only from direct group membership.

upvoted 1 times



  **RVivek** 6 months ago

User3 can perform an access review of User1 = No
User1 is a Member and not a Guest Account, Access Review specified Guests only.

User3 can perform an access review of UserA = No
User1 is a Member and not a Guest Account, Access Review specified Guests only.

User3 can perform an access review of UserB = Yes
Created Group 1 and Group 2, added Group 2 as a member in Group 1

<https://imgur.com/a/2DTRhVb>
<https://learn.microsoft.com/en-us/entra/id-governance/create-access-review>
In a group review, nested groups will be automatically flattened, so users from nested groups will appear as individual users
upvoted 2 times

  **jamesf** 6 months, 2 weeks ago

No, No, Yes
Reviewing a role with nested groups assigned: For users who have membership through a nested group, the access review won't remove their membership to the nested group and therefore they retain access to the role being reviewed.
upvoted 2 times

  **mantwosmart** 7 months, 2 weeks ago

User3 can perform an access review of User1. /No
User3 can perform an access review of UserA. /No
User3 can perform an access review of UserB. /No
Explanation:

Explanation for User3 can perform an access review of UserB. /No

Note

In a team or group access review, only the group owners (at the time a review starts) are considered as reviewers. During the course of a review, if the list of group owners is updated, new group owners will not be considered reviewers as well as old group owners will still be considered reviewers. However, in the case of a recurring review, any changes on the group owners list will be considered in the next instance of that review.

<https://learn.microsoft.com/en-us/entra/id-governance/create-access-review>
Create a single-stage access review => Next: Reviews
upvoted 2 times



  **[Removed]** 7 months, 3 weeks ago

Wrong

No
No
No



it's specified to review only "Guest users"

User1 = Member
UserA = Member
UserB = is in Group2 which is a Member of Group1
upvoted 2 times

  **smorar** 11 months, 3 weeks ago

User3 can perform an access review of User1. No
User3 can perform an access review of UserA. No
User3 can perform an access review of UserB. No

User 3 can not perform an access review of UserB, because only guests of Group 1 are reviewed not the members and Group 2 is a member of Group 1.
upvoted 4 times

  **3c5adce** 11 months, 4 weeks ago

For this round going with NNY
upvoted 1 times

  **varinder82** 1 year ago

Final Answer: No No NO
upvoted 1 times

  **af68218** 1 year, 1 month ago

The answer does, in fact, appear to be NNY.

I created an access review just now scoped to review just the guest users of a group I had called Lab Administrators. All the members added

directly to Lab Administrators were other groups, and the only result I got from the access review was the one guest user I had as a member of one of the nested groups.

upvoted 3 times

  **I3gcertgrinders** 1 year, 2 months ago


User 3 CANNOT perform an access review of User B:

"Common scenarios in which certain denied users can't have results applied to them may include the following: ...
Reviewing a role with nested groups assigned: For users who have membership through a nested group, the access review won't remove their membership to the nested group and therefore they retain access to the role being reviewed. "

From: <https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-perform-roles-and-resource-roles-review>
upvoted 1 times

  **lebeyic620** 1 year, 1 month ago

It says that they retain access not but that is after they have been reviewed so User3 can review them just can't do anything about it
upvoted 1 times

  **monks** 1 year, 2 months ago

CORRECT
upvoted 1 times

  **labsinghlab** 1 year, 3 months ago

3) NO because nested group
upvoted 2 times

  **Indy429** 1 year, 4 months ago

Even without much technical knowledge, you can answer this question correctly by applying basic comprehensive reading skills. User3 is Group 1 OWNER, Group 2 is MEMBER of Group 1, User3 can perform access reviews on GUESTS ONLY.
Correct answer is:
No
No
Yes
upvoted 3 times

HOTSPOT -

You have the Azure management groups shown in the following table:

Name	In management group
Tenant Root Group	<i>Not applicable</i>
ManagementGroup11	Tenant Root Group
ManagementGroup12	Tenant Root Group
ManagementGroup21	ManagementGroup11

You add Azure subscriptions to the management groups as shown in the following table:

Name	Management group
Subscription1	ManagementGroup21
Subscription2	ManagementGroup12

You create the Azure policies shown in the following table:

Name	Parameter	Scope
Not allowed resource types	virtualNetworks	Tenant Root Group
Allowed resource types	virtualNetworks	ManagementGroup12

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in Subscription2.	<input type="radio"/>	<input type="radio"/>
You can add Subscription1 to ManagementGroup11.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	You can create a virtual network in Subscription1.	<input type="radio"/>	<input checked="" type="radio"/>
	You can create a virtual machine in Subscription2.	<input type="radio"/>	<input checked="" type="radio"/>
	You can add Subscription1 to ManagementGroup11.	<input type="radio"/>	<input checked="" type="radio"/>

  **fedztetz** Highly Voted 4 years, 4 months ago

Answer is Wrong : It should Be NO NO NO
- subscription should be moved by can't be added to 2 groups.
upvoted 257 times

  **Kirintas** 1 month, 3 weeks ago

At first I thought you are right, but isn't the second statement about creating a virtual machine?
There is no policy neither allowing nor preventing the creation of a virtual machine, only virtual networks.
upvoted 1 times

  **Durden871** 2 years, 1 month ago



From Udemy: NYN



Explanation



1. The azure policy (not allowed resource types – Virtual networks) is inherited to Subscription1. So, Virtual networks are not allowed to create in Subscription1.



2. Policy assignments get evaluated top-to-bottom. The most restrictive policy assignment will always win, i.e. a DENY on any level will take precedence over an ALLOW on any other level. So the azure policy (not allowed resource types – Virtual networks) will be applied to Subscription2. The deny policy is only for virtual networks. This allows to create a virtual machine by leveraging existing VNet's.
3. Each management group and subscription can only support one parent. Subscription1 is already part of a management group. We can't add this to another management group though we can move.



<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>
upvoted 63 times



  **avidlearner** 1 year, 8 months ago
No - Tenant Root not allowed
No - Azure policy is a Strict Deny system, Any deny policy on top level is not overridden by lower level allows. Since you are not allowed to create a VNet you can't create a VM without a VNet.
No- you don't add a subscription group which is already assigned to other .
upvoted 8 times



  **Ruzhdi** 1 year, 1 month ago
Answer 2: is Yes - ManagementGroup12 is allowed to create VNet as mentioned in the assignment.
upvoted 2 times

  **alexn76** 2 years, 1 month ago
N Y N
You can create VM on existing network
upvoted 3 times

  **KrisJin** 2 years ago
Who told you there is an existing VNET?
upvoted 9 times



  **Batiste2023** 1 year, 5 months ago
Who told you there isn't? - Actually, who would make policies like this, if there weren't any VNets available already? (I know, it's a Microsoft scenario, but still...)
upvoted 1 times



  **ki01** 1 year, 5 months ago
no one in their right mind would make policies like these, but this is not a real world tenant in a company. this is an exam question to test if you know how allows and denies trickle down through management groups. No need to get philosophical on this
upvoted 4 times

  **ggogel** 1 year, 5 months ago
"Allowed Resource Type (Deny): Defines the resource types that you can deploy. Its effect is to deny all resources that aren't part of this defined list."



See: <https://learn.microsoft.com/en-us/azure/governance/policy/overview#policy-definition>



So the answer to the second question is NO. Only vNets are in the list, so only vNets can be created. Anything else is denied.
upvoted 8 times



  **Zemar** 2 years, 1 month ago
No - Sub1 > Group21 > Group11 > TenantRoot (Not allowed)
No - Sub2 > Group12 > TenantRoot (Not allowed)
No - Only one management group can be assigned to a subscription (Group21 is already assigned to sub1)
upvoted 21 times

  **tita_tovenaar** 3 years, 10 months ago
not agreed for answer 2.
Only virtual networks are mentioned in the policy. Nothing is said about virtual machines.

Result: NO - YES - NO
upvoted 30 times

  **tita_tovenaar** 3 years, 10 months ago
sorry, my bad. answer 2 is No.By allowing networks, you deny all the rest.
upvoted 15 times

  **pieronegri** 4 years, 4 months ago
you are right, "move" is the right verb.
upvoted 2 times

  **mlantonis** Highly Voted 7 months, 2 weeks ago
Allowed Resource Type (Deny): Defines the resource types that you can deploy. Its effect is to deny all resources that aren't part of this defined list.
Not allowed resource types (Deny): Prevents a list of resource types from being deployed.



Based on the Policies, VNets are not allowed in the Tenant Root Group scope, so you cannot deploy VNets. Also, VNets only allowed in ManagementGroup12 scope, but you cannot deploy any other resource.



Box 1: No
Subscription1 is a member of ManagementGroup21, ManagementGroup21 is a member of ManagementGroup11, ManagementGroup11 is a member of the Tenant Root Group, The Tenant Root group has ‘Not allowed resource types for virtual network’.



Box 2: No:
You cannot create a VM, because based on the Policy you can only create VNETs in Sybscription2 (ManagementGroup12).



Box 3: No
You cannot ADD Subscription1 to ManagementGroup11, but you can MOVE Subscription1 from ManagementGroup21 to ManagmentGroup11. Subscriptions can only be a member of ONE ManagementGroup at a time.
upvoted 251 times



  **vrn1358** 3 months, 2 weeks ago
Good Explanation dude :)
upvoted 2 times



  **EIDakhli** 2 years, 4 months ago
Perfect comment, thank you :)
upvoted 5 times



  **Harssh** 3 years, 5 months ago
Box 1 and Box 2 are ok; however, I have a doubt that when all management groups here are under management group Tenant Root Group which has a policy barring Virtual Networks, so how come ManagementGroup12 can allow Virtual network creation in the first place? Do'nt member management groups inherit policies from host management group?
upvoted 1 times



  **Harssh** 3 years, 5 months ago
My question is can a nested management group override policy defined at its parent management group level by creating its own contradictory policy?
upvoted 3 times

  **SumanSaurabh** 2 years, 4 months ago
Exactly, I do have same question. Can some help to understand
upvoted 1 times

  **joergsi** 3 years, 4 months ago
Your reply for box 2 makes no sense because the question is: You can create a VM in Sun 2?
And you are saying: Box 2: No:
You cannot create a VM, because based on the Policy you can only create VNETs in Sybscription2 (ManagementGroup12).
But then the answer needs to be yes based on your argument, correct?
upvoted 4 times

  **kilowd** 2 years, 11 months ago
Allowed Resource Type (Deny): Defines the resource types that you can deploy. Its effect is to deny all resources that aren't part of this defined list.
upvoted 1 times

  **xavigo** 3 years ago
If you can *only* create VNETS then it follows you cannot create other things like VMs. What's so hard to grasp?
upvoted 6 times



  **saadraaz**



Most Recent ⌵



 2 weeks, 2 days ago
Statement-1 You can create a virtual network in Subscription1
Answer: No - Denied at Tenant Root, inherited down.

Statement-2 You can create a virtual machine in Subscription2
Answer: No - Blocked by "Allowed resource types" policy that excludes VMs.

Statement -3 You can add Subscription1 to ManagementGroup11
Answer: Yes - Permitted with proper RBAC.
upvoted 1 times

  **Ponpon3185** 2 months, 1 week ago
To my mind No/Yes/No, cause if Vnet exist you're able to create VM
upvoted 1 times

  **Dankho** 6 months, 2 weeks ago
NYN -
1 - can't create the network
2 - you can create VMs all day long
3 - can't add and have 2 parents; the answer says move but move != add
upvoted 2 times

  **NickyDee** 7 months, 2 weeks ago
Nested groups galore!

NO, you cannot create a Vnet in Subscription1:

Subscription1 is a member of Group21, Group21 is a member of Group11, Group11 is a member of the Tenant Root Group, The Tenant Root group is Not allowed resource types for virtual network.

NO, you cannot create a Vnet in Subscription2:
Subscription2 is is a member of ManagementGroup12, ManagementGroup12 is a member of the Tenant Root Group, The Tenant Root group is Not allowed resource types for virtual network.

NO, you cannot ADD Subscription1 to ManagementGroup11, but you can MOVE subscription1 from ManagementGroup21 to ManagmentGroup11. Subscriptions can only be a member of ONE managementGroup at a time.

upvoted 9 times

  **Penagache** 4 years, 4 months ago



Second question is for vm, not for vnet.
upvoted 11 times

  **oooMooo** 4 years, 4 months ago

Thank you for this detailed response!
upvoted 2 times

  **Bruce_dB** 4 years, 3 months ago

Yes, but,
The process of moving a subscription is by using the add functionality:
"To move a subscription in CLI, you use the add command"
<https://docs.microsoft.com/en-us/azure/governance/management-groups/manage>
upvoted 4 times

  **shnz03** 3 years, 11 months ago

Good one! the verb "add" in CLI is confirmed as move.
upvoted 1 times

  **AubinBakana** 7 months, 2 weeks ago

Creating a Virtual Machine alone still requires that you create a virtual network Essentially, a virtual machine is a virtual network with 1 PC.
Meaning, you cannot create a VM if this action is denied.


If however, the VM existed before the policy was created, which is stated nowhere, by the way, that'd be something entirely different. The question doesn't state anything about there being an existing VNet.

This means the answer to question 2 should be NO.

As for question 3, Subscriptions can be moved, I am not sure what they mean by Add. So this one also isn't quite clear.

If by "add" they mean "move", then the answer is Yes.

So it should be: NO, NO, YES
upvoted 4 times

  **Chiboy** 7 months, 2 weeks ago

This is simple:
1. Virtual Networks are not allowed at the Tenant Root Group for ALL Management Groups. So number 1 is a No. Though virtual network is allowed for one management group, that management group is still under a Tenant root group where vnet is not allowed.
2. You cannot create a virtual Machine without a Virtual Network. Since virtual networks are not allowed, the answer is also No.
3. This is a YES for me. The architecture of a subscription forces it to trust ONLY one Directory at a time. Hence, when the question asks if we can add the subscription to a different mgt group, it was asking if we can "move" it, since architecturally, you can not have a subscription in more than 1 directory at the same time. I admit the question should have been specific in using the word "move" instead of "add". But then, it may also have been part of the question to see if we understand that a subscription can only trust one directory at time.
upvoted 2 times


  **Frost312321** 7 months, 2 weeks ago

Box 3: Yes.

Move subscriptions
Add an existing Subscription to a management group in the portal

Log into the Azure portal.
Select All services > Management groups.
Select the management group you're planning to be the parent.
At the top of the page, select Add subscription.
Select the subscription in the list with the correct ID.
Screenshot of the 'Add subscription' options for selecting an existing subscription to add to a management group.
Select "Save".

<https://docs.microsoft.com/en-us/azure/governance/management-groups/manage>
upvoted 2 times



  **yana_b** 7 months, 2 weeks ago



Box1: No -> because VNets are only allowed for MG12. (here the question in principle whether the allowed VNet for MG12 overrides the previous rule that VNets are forbidden on Tenant root level, which will then mean that such a rule forbids totally the creation of new VNets).
Box 2: Yes -> because forbidding VNets creation does not automatically forbit VMs creation, we can still create new VNs within the already existing Vnets.

Box 3: Yes -> we can move subscriptions from one MG to another, and here we have MG21 under MG11
<https://docs.microsoft.com/en-us/learn/modules/create-windows-virtual-machine-in-azure/2-create-a-windows-virtual-machine>
<https://docs.microsoft.com/en-us/azure/governance/management-groups/manage>
upvoted 3 times

  **[Removed]** 7 months, 3 weeks ago
Wrong

NO
NO
NO
upvoted 1 times



  **Iewisjcsc300** 8 months ago
Adding sub1 isnt the same as moving Sub1
upvoted 1 times



  **TheFivePips** 9 months, 1 week ago
NYN. In general, polices are inherited through a hierarchical structure consisting of Management Groups > Subscriptions > Resource Groups > and Resources. However policies, even more restrictive policies, can be over-ridden at those lower levels.



The first answer is No because it inherits the restrictive policy from the root group and there is nothing to over-ride that policy.

The second answer is Yes because even though it inherits a restrictive policy from the root group, it explicitly allows VNETs to be created at a lower, more granular, management level. I know the question is asking about VM creation, but you need VNETs to create VMs and there is no policy specifically about allowing or disallowing VM creation.

The third answer is No because, as other have said, you cannot have a subscription in 2 management groups. It cannot be added, but it can be moved.
upvoted 1 times

  **TheFivePips** 9 months, 1 week ago
After reading more about this it seems that actually the more restrictive policy will apply. I must have read that from old information or something. You can however exclude resources from a policy in azure, although this is not mentioned in this particular question. So the Answer is actually NNN. The second answer is No because it inherits the more restrictive policy, and even though it is explicitly allowed, the more restrictive inherited policy will prevent VNETs and therefor VMs from being created. What a journey we've been on
upvoted 2 times

  **amurp35** 10 months, 1 week ago
NNN - disallowed by explicit deny; explicit allow is implicit deny on all else; cannot be a member of multiple management groups.
upvoted 1 times

  **23169fd** 10 months, 3 weeks ago
Given answers are correct.
1. No
The "Not allowed resource types" policy for virtualNetworks is scoped to the Tenant Root Group.
2. Yes
There is no policy that restricts or disallows creating virtual machines in ManagementGroup12 or Tenant Root Group.
The allowed resource types for virtualNetworks doesn't impact the creation of virtual machines.
3. Yes
There are no policies or constraints provided that explicitly prevent moving Subscription1 to ManagementGroup11.
upvoted 1 times

  **Charumathi** 11 months ago
Tenant Root Group (Not Allowed Resource - Virtual N/W)
|
|__Management Group 11
||
|__Management Group 21
| (Sub 1)
|
|__Management Group 12
(Sub 2)
(Allowed Resource - Virtual N/W)

Answers,

1. You can create a virtual network in Sub1 - No
Reason: Subscription 1 is under Tenant Root Group, hence we will not be able to create Virtual Network
2. You can create a virtual machine in Sub2 - No
Reason: Subscription 2 is also under Tenant Root Group with overrides the allow resource type in Management Group 12. You will not be able to create a Virtual network, without creation of virtual network, we will not be able to create a Virtual Machine.
3. You can add Sub1 to Management Group11 - No
Reason: We cannot add subscription from one group to the other.
upvoted 1 times

  **varinder82** 11 months, 2 weeks ago

Final Answer : NYN
upvoted 2 times

You have an Azure policy as shown in the following exhibit:

SCOPE

Scope ([Learn more about setting the scope](#))

Subscription 1

Exclusions

Subscription 1/ContosoRG1

BASICS

Policy definition

Not allowed resource types

Assignment name ⓘ

Not allowed resource types

Assignment ID

/subscriptions/5eb8d0b6-ce3b-4ce0-a631-9f5321bedabb/providers/Microsoft.Authorization/policyAssignments/0e6fb866bf854f54acc ae2a9

Description

Assigned by

admin1@contoso.com

PARAMETERS

Not allowed resource types ⓘ

Microsoft.Sql/servers

What is the effect of the policy?

- A. You are prevented from creating Azure SQL servers anywhere in Subscription 1.
- B. You can create Azure SQL servers in ContosoRG1 only.
- C. You are prevented from creating Azure SQL Servers in ContosoRG1 only.
- D. You can create Azure SQL servers in any resource group within Subscription 1.

Correct Answer: B

Community vote distribution

B (100%)

- Nalex9ja

Highly Voted

4 years, 4 months ago

The Picked Option (B) is the correct option

upvoted 92 times
- Ikrom

4 years, 4 months ago

Agree.

It says: Exclusions and RG1 is there.

upvoted 12 times
- fedztetz

Highly Voted

4 years, 4 months ago

Answer is Correct. B

upvoted 37 times
- RajeshwaranM

Most Recent

4 months, 2 weeks ago

Selected Answer: B

Exclusion is the Key word here, So B is the correct option :)

upvoted 2 times

  **Priyanshu_Ji** 4 months, 3 weeks ago

Selected Answer: B

B is correct option , as current policy prevents creation of sql servers in sub1 , but due to exclusion , only inside ContosoRG1 , you can create sql servers.

upvoted 2 times

  **minura** 5 months, 2 weeks ago

Selected Answer: B

Answer is B
RG1 is excluded, so you can create SQL Servers

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

B is corerct
upvoted 1 times

  **tashakori** 1 year, 1 month ago

B is right
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

B is correct
upvoted 2 times

  **stanislaus450** 1 year, 2 months ago

B THIS ANSWER
upvoted 1 times

  **Awoyemi** 1 year, 7 months ago

Selected Answer: B

RG1 is excluded
upvoted 2 times

  **stonwall12** 1 year, 11 months ago

The key is the "Exclusions" within the policy. Find that for answer.
upvoted 1 times

  **Firdous586** 1 year, 11 months ago

B is correct
upvoted 1 times

  **habbey** 2 years ago

The answer is B. The exclusion negates any negatives statements in the option.
upvoted 2 times



  **Madbo** 2 years ago

The correct answer is B. The policy only applies to the resource group ContosoRG1 and allows the creation of Azure SQL servers only in that resource group. The policy does not prevent the creation of Azure SQL servers in other resource groups in Subscription 1.
upvoted 1 times

  **ruqing888** 2 years, 1 month ago

Selected Answer: B

Look at the exclusion from policy.
upvoted 1 times



  **myarali** 2 years, 2 months ago

Selected Answer: B

You are prevented from creating Azure SQL servers anywhere in Subscription 1 with the exception of ContosoRG1
upvoted 5 times

  **garmatey** 2 years, 1 month ago

lol thanks for just commenting with the exact answer given
upvoted 1 times

  **MarMar2022** 2 years, 3 months ago

Selected Answer: B

B Correct.
upvoted 1 times

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table:

Name	Type	Resource group	Tag
RG6	Resource group	<i>Not applicable</i>	<i>None</i>
VNET1	Virtual network	RG6	Department: D1

You assign a policy to RG6 as shown in the following table:

Section	Setting	Value
Scope	Scope	Subscription1/RG6
	Exclusions	<i>None</i>
Basics	Policy definition	Apply tag and its default value
	Assignment name	Apply tag and its default value
Parameters	Tag name	Label
	Tag value	Value1

To RG6, you apply the tag: RGroup: RG6.

You deploy a virtual network named VNET2 to RG6.

Which tags apply to VNET1 and VNET2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

VNET1:

▼

None
Department: D1 only
Department: D1, and RGroup: RG6 only
Department: D1, and Label: Value1 only
Department: D1, RGroup: RG6, and Label: Value1

VNET2:

▼

None
RGroup: RG6 only
Label: Value1 only
RGroup: RG6, and Label: Value1

Answer Area

Correct Answer:

VNET1:

▼

None
Department: D1 only
Department: D1, and RGroup: RG6 only
Department: D1, and Label: Value1 only
Department: D1, RGroup: RG6, and Label: Value1

VNET2:

▼

None
RGroup: RG6 only
Label: Value1 only
RGroup: RG6, and Label: Value1

 **Parmjeet** Highly Voted 2 years, 11 months ago

Correct answer is:

VNET1 will only have Department: D1 tag & VNET 2 will only have Label : Value1 tag

upvoted 369 times

 **XristophD** 2 years, 5 months ago

agree, remediation task is needed to assign new tags to already existing resources (VNET1 existed before Policy was assigned), therefore VNET1 has no tags from the policy assigned.

This would be the case if a remediation task has been performed on the policy assignment, but this was not mentioned in the question.

upvoted 26 times

  **happpieee** 6 months, 2 weeks ago

That is correct (on the contentious VNET1) and assuming the wordings of the Azure Policy to be applied is "Add a tag to resource groups", then VNET1 will only have Department: D1 tag. It will not inherit the Label: Value1 tag as it is an existing resource. For it to inherit the tag, you will need policy name "Inherit a tag from the resource group".

Info: <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

upvoted 6 times

  **Mucker973** 2 years, 10 months ago

nope, your answer is incorrect and the answers given are correct. You are assuming that Dept: D1 overwrites label:value (well I assume you did based on your answer), but resources can have any amount of tags applied. PLUS I have confirmed this in a lab

upvoted 6 times

  **cnduknthm** 2 years, 6 months ago

Its not about OVERWRITING... Its about the assignment of policy. The policy applies to resources that are created only after policy was applied but VNET1 is created before assigning the policy to Resource Group and for that reason VNET1 has only one tag which is Department : D1

upvoted 12 times

  **amiban** 2 years, 5 months ago

but can't be applied by policy, we need to be compliant while creating the resources wrt the tags.

upvoted 1 times

  **Dennis_SOn** 2 years, 9 months ago

what is the answer? your answer seems not in the options?

upvoted 2 times

  **Dennis_SOn** 2 years, 9 months ago

are you referring to this answer?

tag. vnet1 : departement D1 tag only.

VNET1 - Department: D1 only VNET2 - Label: Value1 only

upvoted 5 times

  **Dennis_SOn** 2 years, 9 months ago

tag. vnet1 --- Department: D1 only.

VNET1 - Department: D1 only VNET2 --- Label: Value1 only

upvoted 2 times

  **shash_ank** Highly Voted  2 years, 11 months ago

resources created before policy creation will not inherit the policy rules. so, VNET1 will only have Department: D1 tag, VNET 2 will have Label : Value1

upvoted 193 times

  **Bernard_2nd** 2 years, 11 months ago

Agree with you too.

The policy name "Apply tag and its default vualt" does not change previously tag of resource.

upvoted 6 times

  **Mucker973** 2 years, 10 months ago

Correct, but it does say you create the resources AFTER the policy is created. Tbh the question is worded poorly and contradicts itself but it is implied the resources are created later.

upvoted 3 times

  **Wigoth** 2 years, 9 months ago

Nope, VNET1 is already in place BEFORE the policy is created, so it doesn't get the Label:value1 tag...

upvoted 6 times

  **pgmpp** 2 years, 9 months ago

It does not specify anywhere that VNET1 is again created after the policy creation. Only VNET2 is created after the policy creation.

upvoted 4 times

  **Abiram** 2 years ago

Agree, I tested this on the portal and it works. BDW, there is no such policy called "Apply tag and its default value xxxx" - I can only see "Append tag and its default value xxxx"

Perhaps Microsoft has renamed it recently?

upvoted 3 times

  **saadraaz** Most Recent  2 weeks, 1 day ago

VNET1: Department: D1 only

VNET2: Label: Value1 only



upvoted 1 times

  **Odc4dd8** 3 months, 2 weeks ago

correct answer is VNET 1 will only have Department:D1 and Vnet 2 none



the policy is only applied on the RG an is not inherited by the vnet 1 or vnet2

upvoted 2 times

  **DT95** 6 months, 1 week ago

VNET1: "Department: D1 only"
VNET2: "Label: Value1 only"



upvoted 3 times

  **kejo2** 6 months, 1 week ago

Most of you guys giving the wrong answer, the best way to found out is to test it on your lab.
Just did the practical test on my lab and my result is:



VNET1 = Department:D1
VNET2 = Label: Value1

upvoted 4 times

  **mwho00** 6 months, 1 week ago

Well the mentioned policy is not even existing in azure. So we never know I guess.

upvoted 2 times

  **Chuong0810** 7 months ago

VNET1:
Inherits the policy tag (Label: Value1)
Keeps its existing tag (Department: D1)
Inherits the direct tag applied to RG6 (RGroup: RG6)
Tags: Department: D1, RGroup: RG6, Label: Value1
VNET2:
Inherits the policy tag (Label: Value1)
Inherits the direct tag applied to RG6 (RGroup: RG6)
Tags: RGroup: RG6, Label: Value1

upvoted 2 times

  **ThatDowntownSmell** 7 months, 2 weeks ago

This is really easy to test. What came out of doing this for real (in the specific order that the question poses) with the policy "APPEND tag and its default value" is Vnet1 has only Department:D1, and Vnet2 has only Label:Value1.

The text of the policy in the question does not match what is available in the policies in real life (append vs apply). In any case, here are the take-aways:

Applying a tag to the resource group itself has no bearing on what the resources in the RG group get tagged with. Direct resource group tags are not inherited by resources in the group.

Existing resources do not get the tagging applied when the policy is applied.

Subsequent resources added after the policy is applied do get the tagging applied.

It appears possible to create a policy that would create the tags on existing resources, but it requires usage of a managed identity; presumably this managed identity would be given access to modify the resources (as necessary to add and/or reset a tag+value).

upvoted 17 times

  **KSoul** 7 months, 2 weeks ago

VNET1: Department: D1, and Label:Value1 only.
VNET2: Label:Value1 only.

Above answers are correct.
Reason in simple wording -

1ST - Tags are not inherited to resources from Resource groups. But for first scenario there was no tag assigned to RG6 rather a Azure policy was applied to RG6.

So for VNET1 the value is, it's own tags and azure policy tag that was applied to RG6

2ND - There was no tag assigned to VNET2. Forget about RGroup :RG6 tag because recourse group's tag is not inherited. As per Microsoft document, if no tag is applied to recourses, it add the label and value from the Recourse group's policy which was Label:Value1 in this case.

Please read microsoft doc - Add a tag to resources ---> Adds the specified tag and value when any resource missing this tag is created or updated.
Existing resources can be remediated by triggering a remediation task. If the tag exists with a different value it will not be changed. Does not modify tags on resource groups.



upvoted 8 times

  **[Removed]** 7 months, 3 weeks ago

Wrong

VNET1: Department: D1 only
VNET2: Label: Value1 only

upvoted 3 times

  **lewisjcsc300** 8 months ago

Default tag policy comes into play when no tag has been applied.
If vnet1 already had the tag department....the policy will no affect it.
The policy will affect vnet2, policy will remediate/append the tag by adding the default tag; =value1

upvoted 1 times



  **[Removed]** 8 months ago

Wrong

VNET1: Department: D1 only

VNET2: Label: Value1 only

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

Finally the definitive answer. Thanks for sharing.

VNET1 = Department:D1

VNET2 = Label: Value1

upvoted 6 times

  **Nushin** 1 year ago

Existing resources can be remediated by triggering a remediation task. If the tag exists with a different value it will not be changed. Does not modify tags on resource groups.

upvoted 1 times

  **tashakori** 1 year, 1 month ago

- Department: D1 only

- Label: Value1 only

upvoted 3 times

  **Pirand92** 1 year, 2 months ago

About "To RG6, you apply the tag: RGroup: RG6." I think it should be "Department: D1 and RGroup: RG6 only". Let me know if i'm wrong in some way

upvoted 2 times

You have an Azure subscription named AZPT1 that contains the resources shown in the following table:

Name	Type
storage1	Azure Storage account
VNET1	Virtual network
VM1	Azure virtual machine
VM1Managed	Managed disk for VM1
RVAULT1	Recovery Services vault for the site recovery of VM1

You create a new Azure subscription named AZPT2.
You need to identify which resources can be moved to AZPT2.
Which resources should you identify?

- A. VM1, storage1, VNET1, and VM1Managed only
- B. VM1 and VM1Managed only
- C. VM1, storage1, VNET1, VM1Managed, and RVAULT1
- D. RVAULT1 only

Correct Answer: C

Community vote distribution

C (68%)

A (30%)

mlantonis

Highly Voted

7 months, 2 weeks ago

Correct Answer: C

All of them. Moving a resource only moves it to a new Resource Group or Subscription. It doesn't change the location of the resource.

Reference:
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources>
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftcompute>
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftnetwork>
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftstorage>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftrecoveryservices>
upvoted 177 times

knarik

1 month, 1 week ago

remember this guy, u r going to need him here

upvoted 2 times

klexams

2 years, 6 months ago

Yep. In saying that, there are some limitations on some resources eg. standard LB resource cannot be moved.

upvoted 18 times

OmarMac

Highly Voted

7 months, 2 weeks ago

The answer is C.
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription>
Microsoft.Compute

virtualMachines
disks
Microsoft.Network

networkInterfaces
publicIPAddresses
networkSecurityGroups
virtualNetworks
Microsoft.Storage

storageAccounts
<https://azure.microsoft.com/en-us/updates/azure-backup-support-to-move-recovery-services-vaults/#:~:text=A%20Recovery%20Services%20vault%20is,needs%20natively%20in%20the%20cloud.&text=Flexibility%20to%20move%20across%20subscriptions,across%20resource%20groups%20and%20subscriptions.>

You can move the vault across resource groups and subscriptions.
upvoted 7 times

🗨️ 👤 **saadraaz** Most Recent 2 weeks, 1 day ago

Selected Answer: B

Correct Answer: B (VM1 and VM1Managed only)

Correct: VM1 and its managed disk can be moved together.

- VNET1 is likely in use by VM1 — in-use networks can't be moved.
- storage1 may be used for diagnostics — can't assume it's unused.
- RVAULT1 is used for Site Recovery — not movable.

upvoted 1 times

🗨️ 👤 **RabidRod** 2 days, 3 hours ago

all of the items are moveable, the question is only asking to identify what can be moved (all) not whether they can be moved in certain circumstances (i.e. in use or whatever)

upvoted 1 times

🗨️ 👤 **10ab2ab** 2 months, 1 week ago

Selected Answer: A

Recovery service vault cannot moved should be recreated

upvoted 1 times

🗨️ 👤 **0703448** 2 months, 4 weeks ago

Selected Answer: A

To move a vault, you must delete and recreate it in the new subscription

upvoted 1 times

🗨️ 👤 **Cloudg33k** 2 weeks, 6 days ago

This is incorrect. You can move them as long as they are in the same tenant.

upvoted 1 times

🗨️ 👤 **azuredbaadmin** 3 months, 1 week ago

Selected Answer: A

Generally, the following resources can be moved between subscriptions:

- Virtual Machines (VMs)
- Storage Accounts
- Virtual Networks (VNETs)
- Managed Disks

However, some resources, such as Recovery Services vaults, cannot be moved between subscriptions

upvoted 1 times

🗨️ 👤 **dma799** 2 months, 4 weeks ago

Recovery service vaults can be moved between subscriptions: <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftrecoveryservices>

upvoted 3 times

🗨️ 👤 **lumax007** 1 month, 2 weeks ago

Recovery service vault can be moved between subscripits. It is mentioned in the link you shared.

upvoted 1 times

🗨️ 👤 **manishk39** 3 months, 3 weeks ago

A is correct answer. Keyvault can't move from subscription1 to subscription2

upvoted 1 times

🗨️ 👤 **KC21** 4 months, 2 weeks ago

Selected Answer: C

You can move a Recovery Services Vault associated with a VM if you are also moving the VM itself to a different Azure subscription, but you need to ensure the VM is moved to the same subscription within the same tenant and you must also move the VM to the same subscription as the vault to maintain backup functionality.

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-move-recovery-services-vault>

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription>

upvoted 4 times

🗨️ 👤 **SHAHIN_STA** 4 months, 3 weeks ago

Selected Answer: C

Correct Answer: C.

Explanation:

Virtual Machines (VM1 and VM1Managed):

Azure allows moving VMs and managed disks if there are no unsupported configurations like proximity placement groups or availability sets.

Storage Accounts (storage1):

Storage accounts can be moved unless they are linked to dependent services such as diagnostic logs or backups.


Virtual Networks (VNET1):
Virtual networks and related components can be transferred if they are not tied to non-transferable resources.

Recovery Services Vault (RVAULT1):
Recovery Services Vaults can also be moved if they don't have active backups or other dependencies that block the move.

Why not other options?

Options A & B miss eligible resources like storage1 and RVAULT1.
Option D only includes RVAULT1, ignoring other transferable resources.
For more details, check the official Azure documentation on moving resources between subscriptions.

upvoted 1 times

  **Chuong0810** 7 months ago

Selected Answer: A

All resource can move but not sure to be reused

upvoted 3 times

  **[Removed]** 8 months ago

Selected Answer: C

C is corerct


upvoted 1 times

  **divzrajshekar123** 9 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

  **23169fd** 10 months, 3 weeks ago

Selected Answer: A

Recovery Services Vaults cannot be moved between subscriptions as they have dependencies and configurations tied to the original subscription that are not easily transferable.

upvoted 5 times

  **Blaze34tg** 11 months ago

Selected Answer: C

C is correct. All cane be moved.

upvoted 2 times

  **23169fd** 11 months, 1 week ago

Correct Answer: A

Recovery Services vault cannot be moved to different subscriptions based on the latest Azure Policy.

upvoted 2 times

  **3c5adce** 11 months, 4 weeks ago

Going with C on this round

upvoted 1 times

  **tashakori** 1 year, 1 month ago

C is correct

upvoted 1 times



You recently created a new Azure subscription that contains a user named Admin1. Admin1 attempts to deploy an Azure Marketplace resource by using an Azure Resource Manager template. Admin1 deploys the template by using Azure PowerShell and receives the following error message: `User failed validation to purchase resources. Error message: `Legal terms have not been accepted for this item on this subscription. To accept legal terms, please go to the Azure portal (<http://go.microsoft.com/fwlink/?LinkId=534873>) and configure programmatic deployment for the Marketplace item or create it there for the first time.` You need to ensure that Admin1 can deploy the Marketplace resource successfully. What should you do?


- A. From Azure PowerShell, run the Set-AzApiManagementSubscription cmdlet
- B. From the Azure portal, register the Microsoft.Marketplace resource provider
- C. From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet
- D. From the Azure portal, assign the Billing administrator role to Admin1

Correct Answer: C

Community vote distribution

C (100%)



-   **mlantonis**

Highly Voted 



 3 years, 11 months ago

Correct Answer: C



Set-AzMarketplaceTerms -Publisher <String> -Product <String> -Name <String> [-Accept] [-Terms <PSAgreementTerms>] [-DefaultProfile <IAzureContextContainer>] [-WhatIf] [-Confirm] [<CommonParameters>]

upvoted 272 times
-   **Techfall** 2 years, 2 months ago



For anyone wondering how we are supposed to know this while studying for 104, it's hiding here under VM docs: <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/cli-ps-findimage>

upvoted 44 times
-   **umavaja** 1 year, 3 months ago



The correct url for documentation <https://learn.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-11.2.0>


upvoted 5 times
-   **lingxian** 3 years, 10 months ago

I found mlantonis's answers are the most credible.

upvoted 61 times
-   **kennynelcon** 3 years ago



I will sit for one in few weeks and I am following his answers, a gem


upvoted 11 times
-   **xclusivetp3**

Highly Voted 

 4 years, 9 months ago

answer is correct



upvoted 26 times
-   **lumax007**

Most Recent 

 1 month, 2 weeks ago



Selected Answer: C

From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet

upvoted 1 times
-   **RajeshwaranM** 4 months, 2 weeks ago

Selected Answer: C

Set-AzMarketplaceTerms -Publisher <String> -Product <String> -Name <String> [-Accept] [-Terms <PSAgreementTerms>] [-DefaultProfile <IAzureContextContainer>] [-WhatIf] [-Confirm] [<CommonParameters>]

upvoted 1 times
-   **lionleo** 5 months ago

Selected Answer: C

The answer is correct, check the follwoing link <https://about-azure.com/accept-legal-terms-using-powershell-to-deploy-arm-templates/>

upvoted 1 times

- 🗲️ 👤 **Darkfire** 6 months, 4 weeks ago

Selected Answer: C

<https://learn.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-12.3.0>

upvoted 1 times

- 🗲️ 👤 **[Removed]** 8 months ago

Selected Answer: C

C is corerct

upvoted 1 times

- 🗲️ 👤 **3c5adce** 11 months, 4 weeks ago

ChatGPT 4 says C

upvoted 1 times

- 🗲️ 👤 **tashakori** 1 year, 1 month ago

C is correct

upvoted 1 times

- 🗲️ 👤 **Tallgeese** 1 year, 2 months ago

Selected Answer: C

The answer is C because everyone else said so.

upvoted 2 times

- 🗲️ 👤 **oopspruu** 1 year, 8 months ago

Selected Answer: C

Answer is correct.

Source: <https://learn.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-10.2.0>

Set-AzMarketplaceTerms -Publisher "microsoft-ads" -Product "windows-data-science-vm" -Name "windows2016" -Accept

upvoted 1 times

- 🗲️ 👤 **Madbo** 2 years ago

C. The solution to ensure that Admin1 can deploy the Marketplace resource successfully is to run the Set-AzMarketplaceTerms cmdlet from Azure PowerShell. This cmdlet allows you to accept the legal terms for a Marketplace item in your subscription. Once the legal terms are accepted, the user should be able to deploy the resource without any issues.

upvoted 3 times

- 🗲️ 👤 **umavaja** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-11.2.0>

upvoted 1 times

- 🗲️ 👤 **lokii9980** 2 years, 1 month ago

C. From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet.

The error message indicates that the user needs to accept the legal terms for the Marketplace item before they can deploy it. To do this programmatically, you can use the Set-AzMarketplaceTerms cmdlet in Azure PowerShell to accept the legal terms for the subscription. The cmdlet takes the name of the publisher, the name of the offer, and the terms agreement type as parameters. Once the legal terms have been accepted, the user should be able to deploy the Marketplace resource successfully.

upvoted 3 times

- 🗲️ 👤 **Mazinger** 2 years, 2 months ago

Selected Answer: C

To resolve the error message and enable Admin1 to deploy the Azure Marketplace resource successfully, you need to accept the legal terms for the Marketplace resource in the Azure portal. The error message indicates that the legal terms have not been accepted for the resource, and you need to do so before the resource can be deployed.

Therefore, the correct answer is:

C. From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet

You can use the Set-AzMarketplaceTerms cmdlet to accept the legal terms for the Marketplace resource in Azure PowerShell. This cmdlet will open a browser window and prompt you to sign in to the Azure portal to accept the terms for the resource. After you have accepted the terms, you can use the Azure Resource Manager template to deploy the resource without encountering the validation error.

The other options listed are not relevant to the error message and will not resolve the issue.

upvoted 3 times

- 🗲️ 👤 **km_2022** 2 years, 3 months ago

Answer C -

Some VM images in the Azure Marketplace have additional license and purchase terms that you ...

To view an image's purchase plan information, run the Get-AzVMImage cmdlet. If the PurchasePlan property in the output is not null, the image has terms you need to accept before programmatic deployment.

upvoted 1 times

- 🗲️ 👤 **LUISGAR** 2 years, 4 months ago

C no doubt

upvoted 1 times



coskun3firat 2 years, 5 months ago

answer is correct;)

upvoted 1 times



You have an Azure Active Directory (Azure AD) tenant that contains 5,000 user accounts.
You create a new user account named AdminUser1.
You need to assign the User administrator administrative role to AdminUser1.
What should you do from the user account properties?


- A. From the Licenses blade, assign a new license
- B. From the Directory role blade, modify the directory role
- C. From the Groups blade, invite the user account to a new group

Correct Answer: B

Community vote distribution

B (100%)



-   **mlantonis**

Highly Voted 



 3 years, 11 months ago


Correct Answer: B

Active Directory -> Manage Section -> Roles and administrators-> Search for Admin and assign a user to it.

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>
upvoted 147 times
-   **ik96** 3 years, 7 months ago



B is correct.


upvoted 14 times
-   **dan7777**

Highly Voted 

 4 years, 9 months ago

This is the correct answer(select Active directory --> Users--> select the username --> Assigned roles --> click on +add Assignments --> select User administrator role



upvoted 76 times
-   **lumax007**

Most Recent 

 1 month, 2 weeks ago



Selected Answer: B

From the Directory role blade, modify the directory role

upvoted 1 times
-   **[Removed]** 8 months ago



Selected Answer: B

B is corerct



upvoted 2 times
-   **3c5adce** 11 months, 4 weeks ago

B. From the Directory role blade, modify the directory role

To assign the User administrator administrative role to AdminUser1, you should go to the Directory role blade of the user account properties in Azure AD. From there, you can add AdminUser1 to the appropriate administrative role. This action directly assigns the necessary permissions to manage other user accounts within the tenant.

upvoted 3 times
-   **tashakori** 1 year, 1 month ago

B is correct

upvoted 2 times
-   **MarMar2022** 1 year, 7 months ago

Selected Answer: B

B. From the Directory role blade, modify the directory role

Here's how you can do it:

Sign in to the Azure portal using an account that has the necessary administrative privileges.

In the left-hand menu, go to "Azure Active Directory."

Under "Azure Active Directory," click on "Roles and administrators."

In the "Directory roles" blade, locate the "User administrator" role.

Click on the "User administrator" role to open it.

In the "User administrator" blade, click on the "Add assignments" button.

Search for and select the user account "AdminUser1."

Click the "Add" button to assign the "User administrator" role to AdminUser1.

This will grant AdminUser1 the necessary administrative privileges as a User administrator in Azure AD. Option B is the correct choice for this task.
upvoted 4 times

  **Hades231** 1 year, 8 months ago

Selected Answer: B

B is correct.
upvoted 1 times

  **dhivyamohanbabu** 1 year, 10 months ago

Correct Answer: B
upvoted 1 times

  **Madbo** 2 years ago

Option B is correct. From the Directory role blade, you can modify the directory role of a user and assign the User administrator role to AdminUser1. Option A is not relevant to assigning administrative roles. Option C is about inviting the user to a group, which is not relevant to assigning administrative roles.
upvoted 1 times

  **Mazinger** 2 years, 2 months ago

Selected Answer: B



To assign the User administrator administrative role to AdminUser1, you need to modify the directory role for the user account. The User administrator role provides full access to manage user accounts and groups in Azure AD. Therefore, the correct answer is:
B. From the Directory role blade, modify the directory role
upvoted 2 times


  **LUISGAR** 2 years, 4 months ago

B no doubt
upvoted 1 times

  **daerlnaxe** 2 years, 5 months ago

Interface must have changed since answers, you can find by eliminate the two others but it's totally different now.
"Assigned roles" under "manage"
upvoted 8 times

  **TonySuccess** 2 years, 1 month ago
Can confirm this is now Assigned Roles.
upvoted 2 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) " From the Directory role blade, modify the directory role"

upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

Selected Answer: B

Roles and administrators under AZ AD
upvoted 1 times

  **manalshowaei** 2 years, 10 months ago

Selected Answer: B

B. From the Directory role blade, modify the directory role
upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains 100 user accounts. You purchase 10 Azure AD Premium P2 licenses for the tenant. You need to ensure that 10 users can use all the Azure AD Premium features. What should you do?



- A. From the Licenses blade of Azure AD, assign a license
- B. From the Groups blade of each user, invite the users to a group
- C. From the Azure AD domain, add an enterprise application
- D. From the Directory role blade of each user, modify the directory role


Correct Answer: A

Community vote distribution

A (95%)

5%



-   **mlantonis**

Highly Voted 



 3 years, 11 months ago


Correct Answer: A

Active Directory-> Manage Section > Choose Licenses -> All Products -> Select Azure Active Directory Premium P2 -> Then assign a user to it.

upvoted 188 times
-   **sreekan** 3 years, 9 months ago



yes its true!!! apart from this we need to add location of User also


upvoted 17 times
-   **zyta**

Highly Voted 

 4 years, 9 months ago

that's true - licences need to be assigned

upvoted 56 times
-   **SHAHIN_STA**

Most Recent 

 4 months, 2 weeks ago

Selected Answer: A



Note =>

Starting September 1st, the Microsoft Entra ID Admin Center and the Microsoft Azure portal will no longer support the assignment of licenses through their user interfaces. To manage license assignments for users and groups, administrators are required to use the Microsoft 365 Admin Center. This update is designed to streamline the license management process within the Microsoft ecosystem. This change is limited to the user interface. API and PowerShell access remain unaffected. For detailed guidance on assigning licenses using the Microsoft 365 Admin Center, refer to the following resources:

Assign or Unassign Licenses for Users in the Microsoft 365 Admin Center



Add Users and Assign Licenses in Microsoft 365

Assign Licenses to a Group Using the Microsoft 365 Admin Center



upvoted 9 times
-   **MackD** 5 months, 3 weeks ago

Answer us in correct.

Adding, removing, and reprocessing licensing assignments is only available within the M365 Admin Center.

upvoted 2 times
-   **Bolthen** 6 months, 2 weeks ago

Deprecated. You can now assign licenses only from the M365 portal.

upvoted 6 times
-   **hstorm** 7 months, 2 weeks ago



A) WRONG : Assigning a license to AD does not give specific users the license.

B) WRONG/TRUE ? - This could work, if the license has been assigned to the group (Not stated in the question)

C) WRONG : Enterprise applications has nothing to do with assigning licenses to specific users.



D) WRONG - directory roles does not give licenses

In my oppinion "best answer" is B - The only answer that could be TRUE, guessing question is a little different in real exam, under any sercumstances something has to be done for each of the users...

upvoted 2 times
-   **OmegaGeneral** 4 years, 8 months ago



You need to assign P2 license to users specifically.

upvoted 7 times

  **HHT** 4 years, 7 months ago

your comment is just wrong. A is the correct answer. P2 licenses need to be assigned to your users

upvoted 7 times

  **niceeu** 4 years, 6 months ago

My opinion is that you shouldn't comment if you don't know the right answer.


upvoted 26 times

  **balflearchen** 4 years, 4 months ago

if you don't know, please do not give wrong answer.

Is that difficult to have a Lab for verify? Please don't mislead the others

upvoted 5 times

  **MarMar2022** 7 months, 2 weeks ago

Selected Answer: A

A. From the Licenses blade of Azure AD, assign a license

Here's how you can do it:

Sign in to the Azure portal using an account with administrative privileges.

In the left-hand menu, go to "Azure Active Directory."

Under "Azure Active Directory," click on "Licenses."

In the "Licenses" blade, you should see the purchased Azure AD Premium P2 licenses.

Select the Azure AD Premium P2 license.


In the "Assignments" section, click on "Add assignments."

Choose the users you want to assign the licenses to. In this case, select 10 users.

Click the "Save" button to assign the Azure AD Premium P2 licenses to the selected users.

This action will ensure that these 10 users have access to all Azure AD Premium features included with the P2 license.

upvoted 5 times

  **Billy_Butcher** 1 year, 6 months ago

Bien explicado, muchas gracias.

upvoted 1 times

  **theelicht** 8 months ago

As of September 1st 2024 non of the above are correct. However, the answer mlantonis gave up until now was correct.

upvoted 3 times

  **[Removed]** 8 months ago

Selected Answer: A

A is corerct

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

A. From the Licenses blade of Azure AD, assign a license

To ensure that the 10 users can use all the Azure AD Premium P2 features, you need to assign each of these users a Premium P2 license. This is done from the Licenses blade in the Azure Active Directory section of the Azure portal. Here, you can manage and assign licenses directly to individual users or to a group that these users are part of. Assigning the license enables the users to access Premium features such as Identity Protection, Privileged Identity Management, and more.

upvoted 1 times

  **TobeReto** 1 year, 6 months ago

The answer is

Yes

Yes

No

A Cloud Device Administrator can add any device to any group as long as he it is an assigned membership group.

Also, a User Admin can add any device to a group as long as it is not a Dynamic membership type of group.

A Cloud Device Administrator cannot manually add devices to a group that has a dynamic device membership type.



Dynamic device groups automatically add and remove devices based on a set of rules that you define.

upvoted 1 times

  **stevegod0** 1 year, 7 months ago

Correct A

upvoted 1 times

  **TamerX** 1 year, 9 months ago

Selected Answer: A

The correct answer is A

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups>

upvoted 1 times

  **[Removed]** 1 year, 10 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups>

upvoted 1 times

  **dhivyamohanbabu** 1 year, 10 months ago

Correct Answer: A

upvoted 1 times

  **theGwyn** 1 year, 10 months ago

Selected Answer: A

No doubt

upvoted 2 times

  **BowSec** 2 years ago

Selected Answer: A

Correct Answer: A

upvoted 3 times

You have an Azure subscription named Subscription1 and an on-premises deployment of Microsoft System Center Service Manager. Subscription1 contains a virtual machine named VM1. You need to ensure that an alert is set in Service Manager when the amount of available memory on VM1 is below 10 percent. What should you do first?

- A. Create an automation runbook
- B. Deploy a function app
- C. Deploy the IT Service Management Connector (ITSM)
- D. Create a notification

Correct Answer: C

Community vote distribution

C (74%)

B (16%)

11%

mlantonis

Highly Voted

3 years, 11 months ago

Correct Answer: C

IT Service Management Connector (ITSMC) allows you to connect Azure to a supported IT Service Management (ITSM) product or service. Azure services like Azure Log Analytics and Azure Monitor provide tools to detect, analyze, and troubleshoot problems with your Azure and non-Azure resources. But the work items related to an issue typically reside in an ITSM product or service. ITSMC provides a bi-directional connection between Azure and ITSM tools to help you resolve issues faster. ITSMC supports connections with the following ITSM tools: ServiceNow, System Center Service Manager, Provance, Cherwell.

upvoted 166 times

OmegaGeneral

Highly Voted

4 years, 8 months ago

Correct, you can use the connector to bridge them together

upvoted 35 times

tita_tovenaar

3 years, 10 months ago

Agreed. But interesting to reflect why the rest is wrong. A and B are technically possible too, but the question is what to do *first*. In both cases you'd need to create a trigger first (runbooks and function apps don't run by themselves) eg. with a rule and webhook. D is fairly obviously nonsense, that won't do anything to get you to Service Manager.

upvoted 14 times

d0bermannn

3 years, 3 months ago

hi! for a&b as asways ms need the simplest way to go, technically a&b may be implemented

upvoted 2 times

58b2872

Most Recent

4 months, 1 week ago

Selected Answer: C

The correct answer is:

C. Deploy the IT Service Management Connector (ITSM)

This connector integrates Azure Monitor with System Center Service Manager, allowing alerts to be created and managed within Service Manager.

upvoted 1 times

VictorVE

7 months, 2 weeks ago

"Allows you to connect Azure with ITSM products. The IT Service Management Connector Solution enables you to provide faster resolution of incidents by bringing service desk and monitoring data together. It provides a bi-directional connection between Azure and supported ITSM tools : ServiceNow, System Center Service Manager, Provance and Cherwell."

upvoted 5 times

kklohit

7 months, 2 weeks ago

Selected Answer: A

Option C, "Deploy the IT Service Management Connector (ITSM)", is a valid solution for integrating Azure Monitor with Service Manager to generate incidents based on alerts.

The IT Service Management Connector is designed to work with Azure Monitor, allowing you to get insights and take action on alerts raised by Azure resources in Service Manager.

Therefore, both options A and C are correct as they both can be used to configure the integration between Azure Monitor and Service Manager.

To monitor the available memory on VM1, you would need to install the Microsoft Monitoring Agent on the virtual machine first. So option A, "Install the Microsoft Monitoring Agent on VM1," would be the first step. After the agent is installed, you can configure the appropriate monitoring rules or alerts in System Center Service Manager or other monitoring solutions.

upvoted 2 times

🗳️ 👤 **jackill** 7 months, 2 weeks ago

Selected Answer: C

I agree the correct answer is "C" - "Deploy the IT Service Management Connector (ITSM)", but the referenced documentation <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview> appears to be not clear enough, because it says "Azure Monitor supports connections with the following ITSM tools: ServiceNow ITSM or IT Operations Management (ITOM), BMC", so not telling that the IT Service Management Connector (ITSMC) can also connect Azure to the on-premises deployment of Microsoft System Center Service Manager (SCSM). Instead, I've found the page <https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-definition?source=recommendations#install-it-service-management-connector>, where the image reported in the second step, shows the description of the ITSMC service which states: "It provides a bidirectional connection between Azure and supported ITSM tools: ServiceNow, * System Center Service Manager *, Provance and Cherwell". I also checked the description directly from the Azure Portal and it is the same.

upvoted 1 times

🗳️ 👤 **[Removed]** 8 months ago

Selected Answer: C

C is corerct

upvoted 1 times

🗳️ 👤 **3c5adce** 11 months, 4 weeks ago

To ensure that an alert is set in Service Manager when the available memory on VM1 is below 10 percent, you should first deploy the IT Service Management Connector (ITSM) in Azure. This connector allows you to integrate Azure monitoring and management capabilities with your on-premises Service Manager. By deploying the ITSM Connector, you establish the necessary connection to forward alerts generated in Azure based on specific metrics (like memory utilization of VM1) directly to your System Center Service Manager for processing and response.

upvoted 1 times

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

C is right

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-classic.overview>

upvoted 1 times

🗳️ 👤 **Madbo** 2 years ago

C. Create a management solution. To set an alert in Service Manager when the amount of available memory on VM1 is below 10 percent, you need to first create a management solution in Azure Monitor. This solution should include a metric alert rule that monitors the available memory on VM1 and sends an alert to Service Manager when the available memory falls below 10 percent. Once the management solution is created and the alert rule is set, you can configure Service Manager to receive the alert and create a ticket for the issue.

upvoted 3 times

🗳️ 👤 **typales2005** 2 years, 3 months ago

Selected Answer: B

On the 09/01/2023 exam

upvoted 3 times

🗳️ 👤 **alirasouli** 2 years, 6 months ago

Selected Answer: C

The answer is correct. As per documentation:

Azure Monitor provides a bi-directional connection between Azure and ITSM tools to help you resolve issues faster. You can create work items in your ITSM tool based on your Azure alerts (Metric Alerts, Activity Log Alerts, and Log Analytics alerts).

Azure Monitor supports connections with the following ITSM tools:

- ServiceNow ITSM or ITOM
- BMC

upvoted 1 times

🗳️ 👤 **majerly** 2 years, 7 months ago

Today in exam, is C

upvoted 1 times

🗳️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: C

C) " Deploy the IT Service Management Connector (ITSM)"



upvoted 2 times

🗳️ 👤 **EmnCours** 2 years, 8 months ago

Selected Answer: C

Correct Answer: C

upvoted 1 times

  **viveksen1** 2 years, 8 months ago
C is correct - Use a connector bridge
upvoted 1 times

You sign up for Azure Active Directory (Azure AD) Premium P2.
You need to add a user named admin1@contoso.com as an administrator on all the computers that will be joined to the Azure AD domain.
What should you configure in Azure AD?

- A. Device settings from the Devices blade
- B. Providers from the MFA Server blade
- C. User settings from the Users blade
- D. General settings from the Groups blade

Correct Answer: A

Community vote distribution

A (100%)

  **mlantonis** Highly Voted 7 months, 2 weeks ago
Correct Answer: A



When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principles to the local administrators group on the device:

- ☞ The Azure AD global administrator role
- ☞ The Azure AD device administrator role
- ☞ The user performing the Azure AD join



In the Azure portal, you can manage the device administrator role on the Devices page. To open the Devices page:

1. Sign in to your Azure portal as a global administrator or device administrator.
2. On the left navbar, click Azure Active Directory.
3. In the Manage section, click Devices.
4. On the Devices page, click Device settings.
5. To modify the device administrator role, configure Additional local administrators on Azure AD joined devices.



upvoted 219 times

  **magichappens** 3 years, 1 month ago
The "Manage Additional local administrators on all Azure AD joined devices" actually just forwards you to the directory roles. Since this is a role nowadays, you could actually also set it up from the user settings...



upvoted 4 times

  **Gde360** 3 years, 9 months ago
Good to know the steps.
However, please be aware that the option of "Additional local administrators on Azure AD joined devices." requires an Azure AD Premium tenant.



upvoted 4 times

  **muhammadazure** 2 years, 11 months ago
you are true legend mlantonis



upvoted 6 times

  **OmegaGeneral** Highly Voted 4 years, 8 months ago
Correct you can specifically specify administrator roles on the devices through device settings in the Azure portal



upvoted 20 times

  **SrWalk49** Most Recent 7 months ago
Is mlantonis back or is someone playing a cruel joke? 😂

upvoted 2 times

  **[Removed]** 8 months ago
Selected Answer: A
A is corerct

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago
A. Device settings from the Devices blade / Think: Computers in question = Devices

To add a user as an administrator on all computers that will be joined to the Azure AD domain, you need to configure the device settings from the Devices blade in Azure AD. Here, you can set a policy to grant specific users administrative privileges on all Azure AD joined devices. This setting allows you to define who can manage the devices that are registered and joined to your Azure AD domain.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 10 months ago

Selected Answer: A

A

upvoted 1 times

🗨️ 👤 **morito** 2 years, 2 months ago

This answer is a possible way, its considered best practice regarding least privilege. However please not that all Global Admins are automatically administrators on the joined devices.

upvoted 2 times

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

Selected Answer: A

Configuring user settings from the Users blade in Azure AD will not allow you to add a user as an administrator on all the computers that will be joined to the Azure AD domain.

To achieve this, you can use Azure AD device management and configure device settings from the Devices blade. Specifically, you can configure device settings to add a user as a local administrator on all devices joined to Azure AD.

So the correct answer is A. Device settings from the Devices blad

upvoted 2 times

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

Selected Answer: A

To add a user as an administrator on all computers joined to the Azure AD domain, you should configure device settings from the Devices blade in Azure AD.

Here's how to do it:

1. Sign in to the Azure portal with your Azure AD Premium P2 account.
2. Navigate to the Azure Active Directory blade.
3. Click on the Devices blade.
4. Select Device settings.
5. Under Additional local administrators on Azure AD joined devices, click Add.
6. In the Add additional administrators pane, type in the email address for the user you want to add as an administrator, in this case, admin1@contoso.com.
7. Click Save to add the user as an additional local administrator on all Azure AD joined devices.

Note that this will only work for Azure AD joined devices, not for devices that are joined to other directory services or are not joined to any directory service.

upvoted 3 times

🗨️ 👤 **silver1987** 2 years, 3 months ago

answer A

from azure portal --> azure active directory --> devices --> device settings --> manage additional local administrators on all azure ad joined devices --> add assignments --> select user/group as a local admin

upvoted 2 times

🗨️ 👤 **Onobhas01** 2 years, 5 months ago

A is correct

upvoted 1 times

🗨️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: A

A) " Device settings from the Devices blade "

upvoted 1 times

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

Selected Answer: A

Correct Answer: A

upvoted 1 times

🗨️ 👤 **viveksen1** 2 years, 8 months ago

A is correct

upvoted 1 times

🗨️ 👤 **libran** 2 years, 8 months ago

Selected Answer: A

Device settings from the Devices blade

upvoted 1 times

🗨️ 👤 **Lipegj** 2 years, 9 months ago

RESPOSTA A

upvoted 1 times

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

Selected Answer: A

A is correct
upvoted 1 times

HOTSPOT -

You have Azure Active Directory tenant named Contoso.com that includes following users:

Name	Role
User1	Cloud device administrator
User2	User administrator

Contoso.com includes following Windows 10 devices:

Name	Join type
Device1	Azure AD registered
Device2	Azure AD joined

You create following security groups in Contoso.com:

Name	Membership Type	Owner
Group1	Assigned	User2
Group2	Dynamic Device	User2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can add Device2 to Group1	<input type="radio"/>	<input type="radio"/>
User2 can add Device1 to Group1	<input type="radio"/>	<input type="radio"/>
User2 can add Device2 to Group2	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
User1 can add Device2 to Group1	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add Device1 to Group1	<input checked="" type="radio"/>	<input type="radio"/>
User2 can add Device2 to Group2	<input type="radio"/>	<input checked="" type="radio"/>

Correct Answer:

- Armina** Highly Voted 2 years, 11 months ago

User1 can add Device2 to Group1: No
User2 can add Device1 to Group1: Yes
User2 can add Device2 to Group2: No
Explanation:
Groups can contain both registered and joined devices as members.
As a global administrator or cloud device administrator, you can manage the registered or joined devices. Intune Service administrators can update and delete devices. User administrator can manage users but not devices.
User1 is a cloud device administrator. Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.

User2 is the owner of Group1. He can add Device1 to Group1.

Group2 is configured for dynamic membership. The properties on which the membership of a device in a group of the type dynamic device are defined cannot be changed by either an end user or an user administrator. User2 cannot add any device to Group2.
upvoted 285 times
- go4adil** 1 year, 3 months ago

Correct; Answer is:

User1 can add Device2 to Group1: No (because User1 is Cloud Device Admin and cannot change the group membership for Group1)

User2 can add Device1 to Group1: Yes (because User2 is Group Owner which has the requisite authority for changing group membership. furthermore, Group1 has Assigned membership type)

User2 can add Device2 to Group2: No (because though User2 is Group Owner with requisite rights but Group2 has Dynamic Device membership type)

See below 'Tasks' with their 'Least Privileged Roles':

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task#groups>

upvoted 8 times

  **klasbeatz** 2 years, 10 months ago

But user 2 is the owner of the group? So because of the dynamic membership of the device this changes even abilities for the owner of the group?

upvoted 2 times

  **klasbeatz** 2 years, 8 months ago

Found my answer : "With Cloud Device administrator role, you can Delete/Disable/Enable devices in Azure Active Directory but you cannot Add/Remove Users in the directory."

upvoted 6 times

  **klasbeatz** 2 years, 7 months ago

Confusing you would think a cloud device admin could....Just reviewing this question again during my studies.

upvoted 2 times

  **Durden871** 2 years, 2 months ago

1. Yes.

Group 1 Owner - User 1.

Group 1 membership type - assigned.

User 1 can add the device to the group because they're the owner of said group.

2. Yes

User 2 -



Not the owner of group 1. However, User administrator role has the permission to update group membership.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

3. No

Despite user 2 being an owner, they can't add dynamic devices to the group.



upvoted 12 times

  **Stunomatic** 6 months, 2 weeks ago

I doesn't mean if I am the owner of certain group I can rule over any other device

so Y Y N makes sense. but if (Cloud device admin cannot add/join devices) = True then NYN

upvoted 2 times

  **ChaBum** 1 year, 7 months ago

User administrator role has the permission to update group membership, but only users, not devices.

upvoted 1 times

  **chair123** 1 year, 7 months ago



it says Group 1 & 2 owner is User 12?.

upvoted 2 times

  **klexams** 2 years, 11 months ago

User1 can add Device2 to Group1 should be YES coz User1 is the owner of Group1, the same statement you made for User2

upvoted 3 times

  **Chiboy** 2 years, 10 months ago



Take a second look. User1 does not own any of the Groups. Answer is No.

upvoted 22 times

  **[Removed]** 1 year, 3 months ago

But the answer says that User1 is Owner of Group1. So the question is wrong.

upvoted 1 times

  **jeru81** 1 year, 2 months ago

How can be a question wrong? User2 is clearly Owner of both Groups. ANSWER is wrong.

upvoted 6 times



  **FabrityDev** 1 year, 4 months ago



Read the details carefully please before answering, you are causing confusion. User2 is the owner of both groups.



upvoted 8 times

  **Lazylinux** Highly Voted  2 years, 10 months ago



NO Cloud device admin cannot add/join devices
YES: user admin can add device/user/groups
NO: Dynamic groups dont require manual intervention, it uses criteria to add or remove devices/users/groups only assigned groups you can add
upvoted 127 times



  **Hyrydar** 2 years, 8 months ago
the best and straight forward explanation lazylinux. good job
upvoted 3 times



  **micro9000** 2 years, 3 months ago
I agreed on this answer (NYN)
based on these documents:
<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-device-administrator>
1. N - because adding or removing device actions aren't mention on the actions list
2. Y - because user 2 is the owner
<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>
3. N - because You can't manually add or remove a member of a dynamic group.
upvoted 7 times



  **Durden871** 2 years, 2 months ago
Careful, I believe the uploaded the question wrong. I believe group 1 SHOULD be User 1 is the owner of Group 1.
If User 1 is the owner of Group 1:
Y, Y, N



If user 2 is the owner of both groups,
NYN
upvoted 8 times

  **dc2k79** 2 years, 6 months ago
User Admin CANNOT ADD devices.
upvoted 5 times



  **Asfajaf** 2 years, 6 months ago
User2 is owner of Group2, User2 can add/remove members regardless of role
upvoted 6 times



  **darthfodio** 2 years, 4 months ago
Group2 is dynamic, therefore no one, including the owner, can manually add an object.
upvoted 4 times



  **MeysamBayani** 2 years, 2 months ago
but he/she can add new role for add devices. in question mention user2 can ...
upvoted 1 times


  **Durden871** 2 years, 2 months ago
Based on the question, the answer for 3 is no.

I'm cross-referencing with Udemy and the question on Udemy has "User 1 is the user of group 1" Which would make this question, "YYN". The way the question is loaded makes it "NYN".
upvoted 1 times

  **huyhq** Most Recent 1 month, 2 weeks ago
I think
1. User1 can add Device2 to Group1? No
Group1 has Membership Type is "Assigned", so Owner Or Global Administrator has permission add device.
User1 is a Cloud device administrator, but isn't owner Group1, so User1 don't add Device2 to Group1.
2. User2 can add Device1 to Group1? Yes
User2 is Owner of Group1 and Group1 has Membership Type Assigned.
User2 has permission for member management, So can add Device1 to Group1.
3. User2 can add Device2 to Group2? (No)
Group2 has Membership Type is "Dynamic Device", so Azure AD automated member management based on predefined rules..
Users cannot manually add devices to Dynamic Device Groups, even if they are the group owners
upvoted 1 times

  **iamsks** 1 month, 3 weeks ago
No
No
Yes
upvoted 1 times

  **iamsks** 1 month, 3 weeks ago
I am correcting my previous response...
No
Yes
No
upvoted 1 times


-  **BWLZ** 2 months ago

User1 can add Device2 to Group1: No

User1 is a Cloud Device Administrator and does not have permissions to manage group memberships.
User2 can add Device1 to Group1: Yes


User2 is a User Administrator and has the necessary permissions to manage group memberships, including adding devices to security groups.
User2 can add Device2 to Group2: No

Group2 is a Dynamic Device group, and User2, even as a User Administrator, cannot manually add devices to a dynamic group. Dynamic groups are managed automatically based on rules.


upvoted 1 times
-  **Jay_D_Lincoln** 2 months, 2 weeks ago

NYN


As a cloud admin User1 do not have permission to add a device. However if User1 was the owner of Group1, then User1 would have full control of membership (which is not the case here)

upvoted 1 times
-  **allinict_111** 3 months, 1 week ago


User2 cannot add Device2 to Group2 because it is a dynamic group

upvoted 1 times
-  **GreenTick** 6 months ago

fundamentally bad and confusing azure architecture, when user and device "admin" can't add objects to AD group, unless the admin also has permission to modify the group.


upvoted 1 times
-  **bacana** 6 months, 1 week ago

From real life.
User1 needs to be member of users administrator to add computer or user as member. As cloud device administrator he can't.


upvoted 1 times
-  **LinuxLewis** 6 months, 1 week ago

for the question about user admins, as I thought they can only delegate user related queries and not to devices, however...


<https://learn.microsoft.com/en-us/answers/questions/1340769/can-an-user-with-user-administrator-role-add-an-az>

upvoted 1 times
-  **mwho00** 6 months, 1 week ago

No one can add any device to group2 because its a dynamic group, Static members cant be added.

upvoted 1 times
-  **Mshaty** 7 months, 1 week ago


i think the correct answer is Yes Yes No. User 1 is a cloud device administrator he can add a device to a group, User 2 is the owner of the Group so they can add members despite them being devices. Group 2 is a dynamic group hence you can not manually add a member

upvoted 2 times
-  **cloudy_man** 7 months, 2 weeks ago

(User administrator) can update the membership of both the groups, regardless of whether he is owner of the group or not because User administrator role has the permission to update group membership. He can add users, devices, other groups to any group in Azure AD. Below is the permission that user administrator role has:

On the other hand Cloud Device administrator can add members to the Group of which he is the owner. and he can add users, devices and other groups only to that Group.

With Cloud Device administrator role, you can Delete/Disable/Enable devices in Azure Active Directory but you cannot Add/Remove Users in the directory.
With User administrator role, you can Add/Remove users in Azure AD but cannot Delete/Disable/Enable the devices.
Hence, The answers are:
No
Yes
No

upvoted 2 times
-  **Navigati0n** 7 months, 2 weeks ago



The access rights for User1 (Cloud Device Administrator) and User2 (User Administrator) in Azure AD, as well as the device status (Azure AD registered or Azure AD joined), will determine what actions each user can perform.

>> User1 can add Device2 to Group1 - No. A Cloud Device Administrator can manage devices in Azure AD but cannot manage groups (including adding devices to a group). That task typically falls under the responsibilities of a User Administrator or a Group Owner.

>> User2 can add Device1 to Group1 - Yes. As the owner of Group1 and a User Administrator, User2 has the rights to add devices to Group1. The fact that Device1 is Azure AD registered does not restrict it from being added to Group1.

>> User2 can add Device2 to Group2 - No. User2 cannot manually add any device to Group2 because it is a dynamic device group. Memberships in dynamic device groups are determined by rules and conditions, rather than manual assignment. Even though User2 is a User Administrator and the owner of Group2, he cannot manually add devices to a dynamic device group.

upvoted 7 times

  **18c2076** 7 months, 2 weeks ago

User1 can add Device2 to Group 1: NO -
Explanation: Cloud Device Admins can enable/disable/delete devices in Azure. Cloud Device Admin DOES NOT grant permission to manage ANY other properties of these devices; Including group membership.

User2 can add Device1 to Group1: YES
Explanation: User2 is the OWNER of Group1. This user can add and remove membership to this group under any circumstance as the group membership type is ASSIGNED - Implying that any membership affiliation must be manually given to any given resource.

User2 can add Device2 to Group2: NO
Explanation: Group2 is stated to be a DYNAMIC membership assignment - This implies that any given resource MUST MEET the criteria/requirement outlined within the group dynamic membership scope to be added to this group as a member. The properties of dynamic group membership requirements CANNOT be changed by either end user nor user administrator.

Additionally, Dynamic Groups feature require Entra ID Premium P1 or P2 licensing.
Hope this helps. Happy studying!

upvoted 3 times

  **[Removed]** 7 months, 3 weeks ago

Wrong

No



Yes

No

Owner = User2

User2 + Azure AD registered + Assigned

upvoted 1 times

  **lenthuccrma** 8 months, 2 weeks ago

ChatGPT answer:
User1 can add device2 to group1: NO

Reason: User1 is a Cloud Device Admin, but Group1 is an assigned group, and they are not listed as the owner of the group. Only the owner or a user with appropriate permissions (e.g., User admin) can assign devices to this group.
User2 can add device1 to group1: YES

Reason: User2 is a User Admin and the owner of Group1. As the group owner and with the User Admin role, they have the necessary permissions to add devices to Group1.
User2 can add device2 to group2: NO

Reason: Group2 is a Dynamic Device group, meaning its membership is determined automatically by rules based on device attributes. Devices cannot be manually added to dynamic groups, even by the owner.

upvoted 2 times

You have an Azure subscription that contains a resource group named RG26.

RG26 is set to the West Europe location and is used to create temporary resources for a project. RG26 contains the resources shown in the following table.

Name	Type	Location
VM1	Virtual machine	North Europe
RGV1	Recovery Services vault	North Europe
SQLD01	SQL server in Azure VM	North Europe
sa001	Storage account	West Europe

SQLDB01 is backed up to RGV1.

When the project is complete, you attempt to delete RG26 from the Azure portal. The deletion fails.

You need to delete RG26.

What should you do first?

- A. Delete VM1
- B. Stop VM1
- C. Stop the backup of SQLDB01
- D. Delete sa001

Correct Answer: C

Community vote distribution

C (100%)

- NaoVaz**

Highly Voted

2 years, 7 months ago

Selected Answer: C

C) " Stop the backup of SQLDB01"

VM's running or not would not block the deletion of a Resource Group.
Storage Accounts also don't block the deletion of a Resource Group.

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/delete-resource-group?tabs=azure-powershell#required-access-and-deletion-failures>

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault?tabs=portal#before-you-start>

upvoted 11 times
- BenStokes**

Highly Voted

3 years, 10 months ago

Answer is correct - C

upvoted 9 times
- villanz**

3 years, 10 months ago

Yes correct - c

upvoted 1 times
- [Removed]**

Most Recent

8 months ago

Selected Answer: C

C is corerct

upvoted 1 times
- leoiq91**

1 year ago

Stop the Backup of SQL =CORRECT!

upvoted 2 times
- Shif**

1 year ago

Ans is C.

upvoted 1 times
- tashakori**

1 year, 1 month ago

C is right

upvoted 1 times

🗨️ 👤 **Wojer** 1 year, 3 months ago

You can't delete a Recovery Services vault with any of the following dependencies:

- 1.You can't delete a vault that contains protected data sources (for example, IaaS VMs, SQL databases, Azure file shares).
- 2.You can't delete a vault that contains backup data. Once backup data is deleted, it will go into the soft deleted state.
- 3.You can't delete a vault that contains backup data in the soft deleted state.
- 4.You can't delete a vault that has registered storage accounts.

To delete a vault, Go to vault Overview, click Delete, and then follow the instructions to complete the removal of Azure Backup and Azure Site Recovery items.

upvoted 7 times

🗨️ 👤 **Mehedi007** 1 year, 9 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-delete-vault?tabs=portal>

upvoted 1 times

🗨️ 👤 **TonySuccess** 1 year, 10 months ago

Selected Answer: C

It should be C

upvoted 1 times

🗨️ 👤 **bcristella** 2 years, 1 month ago

Right answer = C.

You can't delete a Recovery Services vault with any of the following dependencies:

1. You can't delete a vault that contains backup data. Once backup data is deleted, it will go into the soft deleted state.
2. You can't delete a vault that contains backup data in the soft deleted state.

upvoted 5 times

🗨️ 👤 **zellck** 2 years, 3 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-delete-vault?tabs=portal#before-you-start>

You can't delete a Recovery Services vault with any of the following dependencies:

- You can't delete a vault that contains backup data. Once backup data is deleted, it will go into the soft deleted state.
- You can't delete a vault that contains backup data in the soft deleted state.

upvoted 4 times

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

Today in exam, is C

upvoted 2 times

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

Selected Answer: C

Correct Answer: C

upvoted 2 times

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

Tested in lab and C is the correct answer

upvoted 3 times

🗨️ 👤 **Moezey** 3 years, 2 months ago

Correct ans: C

This happened to my lab environment where i couldnt delete a RG because i hadnt stopped the backups in the vault.

upvoted 3 times

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

Answer is C

upvoted 1 times

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

Owners of dynamic groups must have a global administrator, group administrator, Intune administrator, or user administrator role to edit group membership rules

user2 is the owner of group2 and also assigned " user administrator" role, which means user2 can modify the rule and add device2 if required

upvoted 2 times

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1. Subscription1 has a user named User1. User1 has the following roles:

- ⇒ Reader
- ⇒ Security Admin
- ⇒ Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users. What should you do?



- A. Remove User1 from the Security Reader and Reader roles for Subscription1.
- B. Assign User1 the User Access Administrator role for VNet1.
- C. Assign User1 the Network Contributor role for VNet1.
- D. Assign User1 the Network Contributor role for RG1.


Correct Answer: B

Community vote distribution

B (85%)



C (15%)


-   **js_indore**

Highly Voted 

 3 years, 7 months ago

agree, its B

upvoted 14 times
-   **Madbo**

Highly Voted 

 2 years ago



Option B is the correct answer.


The User Access Administrator role allows users to manage user access to Azure resources, but it does not provide the ability to assign roles to other users.

The Network Contributor role grants users the ability to manage networks, but it also does not provide the ability to assign roles to other users.

The Security Admin and Security Reader roles are not relevant to the task at hand.

Therefore, the correct option is to assign User1 the User Access Administrator role for VNet1, which will allow them to assign the Reader role to other users for that specific virtual network.



upvoted 12 times
-   **[Removed]**

Most Recent 

 8 months ago



Selected Answer: B

B is corerct

upvoted 1 times
-   **mtc9** 1 year, 7 months ago

Any variations of Contributor role does not allow to grant roles to other users. Contributor can be understood as resource read/write permission. To assing roles to other users you need some variation of Owner to repurce or Administrator role.

Roles do not exclude each other, so if you have Read and Contributor role, you're still a Contributor and gain nothing by removing Reader role.

upvoted 5 times
-   **The1BelowAll** 1 year, 8 months ago



Selected Answer: B

B. User Access Administrator do the following.

Manage user access to Azure resources

Assign roles in Azure RBAC



Assign themselves or others the Owner role

upvoted 4 times
-   **Mehedi007** 1 year, 9 months ago

Selected Answer: B

"Lets you manage user access to Azure resources."

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>

upvoted 2 times
-   **[Removed]** 1 year, 10 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>
Lets you manage user access to Azure resources.

upvoted 1 times

🗨️ 👤 **bcristella** 2 years, 1 month ago

Right answer is B.
Contributor = Can't grant access to others
User Access Administration = Manage user access to Azure resources
upvoted 2 times

🗨️ 👤 **GoldBear** 2 years, 1 month ago

This is a tricky question since it uses an Azure RBAC role Network Contributor as a possible answer. The question is for Azure Active Directory which does not have a Network Contributor built-in role.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>
upvoted 1 times

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

Selected Answer: C

To allow User1 to assign the Reader role for VNet1 to other users, you can assign the Network Contributor role for VNet1 to User1. The Network Contributor role provides the permissions required to manage virtual networks, including the ability to assign the Reader role. Option C is correct.

Option A is not correct because removing User1 from the Security Reader and Reader roles for Subscription1 does not provide the required permission for managing VNet1.

Option B is not correct because the User Access Administrator role does not provide the permission to assign the Reader role for VNet1 to other users.

Option D is not correct because assigning the Network Contributor role for RG1 only provides permission to manage resources in the resource group, but does not specifically provide permission to manage VNet1.

upvoted 4 times

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

Wrong.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>
"Lets you manage networks, but not access to them." Microsoft.Authorization/*/read does not give assign permissions, see here:
<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftauthorization>
upvoted 1 times

🗨️ 👤 **amiray** 2 years, 2 months ago

Network Contributor -> Lets you manage networks, but not access to them.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>
upvoted 2 times

🗨️ 👤 **zelck** 2 years, 3 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>
User Access Administrator
- Lets you manage user access to Azure resources
upvoted 2 times

🗨️ 👤 **Aliciuzza** 2 years, 5 months ago

Selected Answer: B

Access administrator
upvoted 1 times

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

User administrator role
upvoted 2 times

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

Hope, Contributor role could not able to assign access role hence B is right answer as User Access Admin role to assign access to others
upvoted 1 times

🗨️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) " Assign User1 the User Access Administrator role for VNet1."

User Access Administrator - "Lets you manage user access to Azure resources. "

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>
upvoted 5 times

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

Selected Answer: B

Correct Answer: B
upvoted 2 times



EleChie 2 years, 8 months ago

OR

Assign User1 the Owner role for VNet1
upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant named contosocloud.onmicrosoft.com.
Your company has a public DNS zone for contoso.com.
You add contoso.com as a custom domain name to Azure AD.
You need to ensure that Azure can verify the domain name.
Which type of DNS record should you create?

- A. MX
- B. NSEC
- C. PTR
- D. RRSIG

Correct Answer: A

Community vote distribution

A (95%)

5%

- ms70743**

Highly Voted

4 years, 4 months ago

TXT and MX are valid answers.

upvoted 108 times
- sidharthwader**

Highly Voted

4 years ago

So guys i will try to give an expiation to this question.
When you add a custom domain in azure u are not allowed to use that unless u prove its your domain.So once u add the custom domain name azure asks u to verify and you have to provide some inputs to verify that its your these inputs can be provided in TXT or MX. So its MX in this case

upvoted 84 times
- Amrinder101**

2 years, 5 months ago

Why would you update MX record? Its used for mail servers. The email delivery will stop working if you update MX records. TXT is always used for domain verification.

upvoted 10 times
- jackill**

1 year, 10 months ago

Although the reference provided (<https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>) do not mention MX record, my understanding is that both TXT and MX can be used to perform the validation step. The TXT/MX record added is needed only for the verification step (to assure that you are the owner of the domain), after that it can be removed.
The similar document for Microsoft 365 clarifies this: <https://learn.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide#verify-with-an-mx-record>
It also clarify that you can add this verification MX record with an high priority number to avoid the record to be effectively used to forward emails: "This MX record's Priority must be the highest of all existing MX records for the domain. Otherwise, it can interfere with sending and receiving email. You should delete this records as soon as domain verification is complete."
I suppose that the usage of MX record was introduced due to some restriction on the handling of TXT records by some DNS registrars, but I do not have found direct evidence for this.

upvoted 3 times
- e_karma**

3 years, 5 months ago

I didn't know mx was there usually it is txt record ..thanks for this

upvoted 7 times
- sairaj9396**

3 years ago

same here. i thought mx is explicitly for mail exchange

upvoted 7 times
- Howard20717**

1 year ago

yea, me too. Never use MX record for this purpose

upvoted 2 times
- JayBee65**

3 years, 10 months ago

Thank you - the process is covered here where you can see either TXT or MX can be chosen: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>

upvoted 18 times
- Lamini**

3 years, 6 months ago

Hopefully they update the reference; its not valid. The reference above by JayBee65 is correct as there is no mention of MX in current reference.

upvoted 4 times

🗄️ 👤 **nnamacha** Most Recent 🔍 1 month, 3 weeks ago

Selected Answer: C

I would go for PTR looking at the available options . The correct answer should be TXT <https://www.cloudflare.com/learning/dns/dns-records/dns-ptr-record/>

upvoted 1 times

🗄️ 👤 **Mark74** 5 months ago

Selected Answer: A

Mx record for me is correct

upvoted 1 times

🗄️ 👤 **[Removed]** 8 months ago

Selected Answer: A

A is corerct

upvoted 1 times

🗄️ 👤 **Amir1909** 1 year, 2 months ago

A is correct

upvoted 1 times

🗄️ 👤 **DWILK** 1 year, 6 months ago

Why would a Mail Exchange record have to be created? Mail isn't mentioned in the question. This has to be wrong

upvoted 3 times

🗄️ 👤 **nmnm22** 1 year, 7 months ago

if this list had the Cname record option, would we still need to pick "MX" as an answer? can someone explain why, please?

upvoted 1 times

🗄️ 👤 **abrar_jahat** 1 year, 8 months ago

Selected Answer: A

upvoted 2 times

🗄️ 👤 **itguyeu** 1 year, 10 months ago

I used free version access for this site and it helped me pass the exam. Some questions that I had on the exams, I took the exam more than once, are not available under the free tier access, but 80% of the questions came from here. I do recommend investing a bit of money and getting full access to this site. I didn't memorise answers but analysed them and studied as Microsoft does tweak them a bit.

This Q was on the exam and answer is correct.

upvoted 1 times

🗄️ 👤 **TonySuccess** 1 year, 10 months ago

Selected Answer: A

Of the available options this is MX (A)

upvoted 1 times

🗄️ 👤 **Madbo** 2 years ago

Option A is correct.

When you add a custom domain name to Azure AD, you need to verify that you own the domain by creating a DNS record in your domain's DNS zone that points to Azure AD. In this case, you added contoso.com as a custom domain name to Azure AD, which means you need to create a DNS record in the DNS zone for contoso.com.

The type of DNS record that you need to create is a TXT record, which contains a verification code that Azure AD provides. The TXT record should be created in the DNS zone for the domain name you added to Azure AD (in this case, contoso.com), and the value of the TXT record should be set to the verification code provided by Azure AD. Once you create the TXT record, Azure AD can verify that you own the domain name and you can start using it in Azure AD.

Therefore, option A is correct as an MX record is used for mail exchange, NSEC and RRSIG records are used for DNSSEC validation, and a PTR record is used for reverse DNS lookups.

upvoted 3 times

🗄️ 👤 **kklohit** 2 years, 2 months ago

No, MX record is used to specify the mail server responsible for accepting email messages for the domain, it is not used to verify the domain for Azure AD. The correct answer is TXT record, which is used to verify the ownership of the domain.

To verify the domain name in Azure AD, you need to create a DNS TXT record in your public DNS zone for contoso.com. The value of the record should be the domain verification code that you can get from the Azure portal. Therefore, the correct answer is not listed among the options given.

upvoted 2 times

🗄️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: A

A) "MX".



Booth "MX" and "TXT" entries can be created to validate a custom domain.

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#verify-your-custom-domain-name>
upvoted 4 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: A

Correct Answer: A
upvoted 1 times

  **libran** 2 years, 8 months ago

Selected Answer: A

MX is the Answer
upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

Selected Answer: A

A is correct either TXT and MX are correct but becareful if asked about App Services custom domain it is then A or CNAME record
upvoted 7 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev. You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group. Solution: On Subscription1, you assign the DevTest Labs User role to the Developers group. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (100%)

- mlantonis

Highly Voted

7 months, 2 weeks ago

Correct Answer: B

The Azure DevTest Labs is a role used for Azure DevTest Labs, not for Logic Apps.

DevTest Labs User role only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.

The Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

upvoted 84 times
- Lilyli

3 years, 10 months ago

What does "let you manage logic app ,but not access to them" mean? if you can manage them ,why can't you access to them?

upvoted 6 times
- klexams

3 years, 1 month ago

It means it manages the app but it does not manage access. So it cannot give other users access to the app

upvoted 9 times
- asd1234asd

Highly Voted

4 years, 6 months ago

Clearly No, Azure DevTest Labs is a service that has nothing to do with Logic App

upvoted 22 times
- chaudha4

3 years, 11 months ago

Trick question. Too much use of "dev" keyword to trick people into thinking that somehow DevTest Labs is related to all these "dev" resources !!

upvoted 11 times
- 58b2872

Most Recent

4 months, 1 week ago

Selected Answer: B

for sure no

upvoted 1 times
- minura

7 months, 1 week ago

Correct Answer: B

<https://learn.microsoft.com/en-us/azure/devtest-labs/devtest-lab-add-devtest-user>

upvoted 1 times
- [Removed]

7 months, 3 weeks ago

Selected Answer: B

B is correct

On Dev, you assign the Contributor role to the Developers group.

upvoted 1 times
- [Removed]

8 months ago

Selected Answer: B

B is corerct

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

No, this solution does not meet the goal.

The DevTest Labs User role, while it allows for managing DevTest Labs resources, does not specifically grant the necessary permissions to create Azure Logic Apps. To allow the Developers group to create Azure Logic Apps in the Dev resource group, you would need to assign a role that specifically includes permissions for managing Logic Apps, such as the Logic App Contributor role or a custom role that specifically includes those permissions if more granular control is needed.

upvoted 1 times

  **tashakori** 1 year, 1 month ago

No is right



upvoted 1 times

  **Madbo** 2 years ago

B. No.

Assigning the DevTest Labs User role to the Developers group does not provide them with the ability to create Azure Logic Apps in the Dev resource group. Instead, you should assign the Logic App Contributor role to the Developers group on the Dev resource group.

upvoted 3 times

  **zellck** 2 years, 3 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#devtest-labs-user>

DevTest Labs User

- Lets you connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.

upvoted 1 times

  **majerly** 2 years, 7 months ago

Today in exam is B

upvoted 1 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) "No".

The "DevTest Labs User" Role does not give the required permissions to interact with Logic Apps.

<https://docs.microsoft.com/en-us/azure/devtest-labs/devtest-lab-add-devtest-user#devtest-labs-user>

upvoted 1 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B



Correct Answer: B

upvoted 1 times

  **cryptostud** 2 years, 8 months ago

No is the correct answer but the explanation has a typo; Logic App Contributor role lets you manage logic apps, BUT NOT change access to them. Manage means that you can create, edit and delete logic apps if you have the role.

upvoted 1 times

  **libran** 2 years, 8 months ago

Selected Answer: B

B NO is the Answer

upvoted 1 times

  **Dannxx** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B

The Azure DevTest Labs is a role used for Azure DevTest Labs, not for Logic Apps.

DevTest Labs User role only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.

The Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

upvoted 2 times

  **Lazylinux** 2 years, 10 months ago

Agreed B is answer

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers.

Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Subscription1, you assign the Logic App Operator role to the Developers group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (100%)

  **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer: B

You would need the Logic App Contributor role.

Logic App Operator - Lets you read, enable, and disable logic apps, but not edit or update them.

Logic App Contributor - Lets you create, manage logic apps, but not access to them.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-operator>
upvoted 88 times

  **OmarMac** Highly Voted 4 years, 5 months ago

Logic App Operator Role - Lets you read, enable, and disable logic apps, but not edit or update them.
upvoted 35 times

  **[Removed]** Most Recent 8 months ago

Selected Answer: B

B is corerct

upvoted 1 times

  **tashakori** 1 year, 1 month ago

No is right

upvoted 1 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: B

Logic App Contributor role is required.

"Lets you read, enable, and disable logic apps, but not edit or update them."

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-operator>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-contributor>

Passed the exam on 26 July 2023. Scored 870. Exact question came.

upvoted 3 times

  **Madbo** 2 years ago



B. No

The Logic App Operator role only allows users to view and manage logic apps. It does not allow them to create new ones. Therefore, assigning the Logic App Operator role to the Developers group will not meet the goal of providing them with the ability to create Azure logic apps in the Dev resource group.

upvoted 2 times

  **Michal128** 2 years, 1 month ago

The answer is B even the Dev users group should have Access only for RSG not to entier subscription.
upvoted 1 times

  **zellck** 2 years, 3 months ago


Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-operator>
Logic App Operator

- Lets you read, enable, and disable logic apps, but not edit or update them.

upvoted 1 times

  **majerly** 2 years, 7 months ago

Today in exam is B

upvoted 2 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) "No".

Logic App Operator - Lets you read, enable, and disable logic apps, but not edit or update them.

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-operator>

upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

  **Dannxx** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B

You would need the Logic App Contributor role.

Logic App Operator - Lets you read, enable, and disable logic apps, but not edit or update them.



Logic App Contributor - Lets you create, manage logic apps, but not access to them.

upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

Agreed B is the correct answer

upvoted 1 times

  **Sillyon** 2 years, 10 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

  **manalshowaei** 2 years, 10 months ago

Selected Answer: B

Answer: B. No

upvoted 1 times

  **Marusyk** 3 years ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

  **Azure_daemon** 3 years, 2 months ago

To create Logic App you need the Contributor role not operator, so the correct answer is B

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev. You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group. Solution: On Dev, you assign the Contributor role to the Developers group. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Community vote distribution

A (100%)

- mlantonis

Highly Voted

3 years, 11 months ago

Correct Answer: A

The Contributor role can manage all resources (and add resources) in a Resource Group. Contributor role can create logic apps.

Alternatively, we can use the Logic App Contributor role, which lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

upvoted 71 times
- fedztetz

Highly Voted

4 years, 4 months ago

Answer is Correct. YES (A)

Contributor role can create logic apps

upvoted 43 times
- [Removed]

Most Recent

8 months ago

Selected Answer: A

A is corerct

upvoted 1 times
- Madbo

2 years ago

A. Yes, this meets the goal as the Contributor role would allow the Developers group to create and manage resources within the Dev resource group, including Azure logic apps.

upvoted 1 times
- Mazinger

2 years, 2 months ago

Selected Answer: A

Yes, assigning the Contributor role to the Developers group on the Dev resource group would meet the goal of providing the group with the ability to create Azure logic apps in the Dev resource group.

The Contributor role grants full access to manage all resources in the resource group, including the ability to create and manage logic apps. By assigning the Contributor role to the Developers group, you are giving them the necessary permissions to create and manage logic apps in the Dev resource group.

upvoted 1 times
- zelck

2 years, 3 months ago

Selected Answer: A

A is the answer.

Contributor

- Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.


upvoted 1 times
- liketopass

2 years, 5 months ago

I have made a lab, created a Resource group and a user under my pas-as-you-go subscription and then assign the contributor role on the subscription to the user, but the user cannot create a logic app. In the process of creating the logic app, when selecting the resource group, the user gets the message it says (in red):

You cannot perform this action without all of the following permissions (Microsoft.Storage/storageAccounts/write, Microsoft.Web/ServerFarms/write, Microsoft.Web/Sites/write)

upvoted 1 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: A

A) "Yes".

Contributor - "Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries."

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#contributor>



upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

  **Dannxx** 2 years, 8 months ago

Selected Answer: A

Correct Answer: A

The Contributor role can manage all resources (and add resources) in a Resource Group. Contributor role can create logic apps.

Alternatively, we can use the Logic App Contributor role, which lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

A is correct

upvoted 1 times

  **Sillyon** 2 years, 10 months ago

Selected Answer: A

Correct answer is A.

upvoted 1 times

  **manalshowaei** 2 years, 10 months ago

Selected Answer: A

A. Yes is correct

upvoted 1 times

  **Marusyk** 3 years ago

Selected Answer: A



Answer is Correct. YES (A)

upvoted 1 times

  **Azure_daemon** 3 years, 2 months ago

Obviously A is the correct answer



upvoted 1 times

  **Prano** 3 years, 4 months ago

Ans : A

Contributor can create logic apps

upvoted 1 times

  **mse89** 3 years, 4 months ago

answer is correct, the role contributor is applied to the resource group

upvoted 1 times

DRAG DROP -

You have an Azure subscription that is used by four departments in your company. The subscription contains 10 resource groups. Each department uses resources in several resource groups.

You need to send a report to the finance department. The report must detail the costs for each department.

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

Answer Area

Assign a tag to each resource group.

Assign a tag to each resource.

Download the usage report.

From the Cost analysis blade, filter the view by tag.

Open the **Resource costs** blade of each resource group.

⬅️

➡️

⬆️

⬆️

Actions

Answer Area

Assign a tag to each resource group.

Assign a tag to each resource.

Download the usage report.

From the Cost analysis blade, filter the view by tag.

Open the **Resource costs** blade of each resource group.

⬅️

➡️

⬆️

⬆️

Correct Answer:

Assign a tag to each resource.

From the Cost analysis blade, filter the view by tag.

Download the usage report.

Box 1: Assign a tag to each resource.

You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy. After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Each resource or resource group can have a maximum of 15 tag name/value pairs. Tags applied to the resource group are not inherited by the resources in that resource group.

Box 2: From the Cost analysis blade, filter the view by tag

After you get your services running, regularly check how much they're costing you. You can see the current spend and burn rate in Azure portal.

1. Visit the Subscriptions blade in Azure portal and select a subscription.

You should see the cost breakdown and burn rate in the popup blade.

2. Click Cost analysis in the list to the left to see the cost breakdown by resource. Wait 24 hours after you add a service for the data to populate.

3. You can filter by different properties like tags, resource group, and timespan. Click Apply to confirm the filters and Download if you want to export the view to a Comma-Separated Values (.csv) file.

Box 3: Download the usage report

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags> <https://docs.microsoft.com/en-us/azure/billing/billing-getting-started>

mlantonis

Highly Voted



3 years, 11 months ago

Correct Answer:



Box 1: Assign a tag to each resource

Box 2: From the Cost analysis blade, filter the view by tag
Box 3: Download the usage report

upvoted 267 times

  **Takloy** 3 years, 6 months ago



Yup! also tested it.
upvoted 13 times

  **Jey117** 2 years, 10 months ago

How do you guys test all of this? You have access to Azure in your company and they give you permissions to deploy and test? I mean this one can be tested by a free account but other things can't be tested though. I wonder how people can test so many things xD
upvoted 12 times

  **SkippyPGD** 2 years, 8 months ago

Join Microsoft's Developer Program for free, and then you get a free E5 tenant to use (includes 25 licenses) and they renew it every 3 months as long as its detected that it has non-production usage.
upvoted 21 times

  **allyQ** 2 years, 2 months ago

I have a subscription in my own tenant. As long as you delete resources quickly after a 'Lab' then you can really keep monthly costs low. You cant test everything, like you say, but I can test most stuff and delete same day.
upvoted 4 times

  **muhammadazure** 2 years, 11 months ago

thank you mlantonis
upvoted 3 times

  **moekyisin** Highly Voted  4 years, 5 months ago

Ans is correct
upvoted 18 times

  **lumax007** Most Recent  1 month, 2 weeks ago

1: Assign a tag to each resource
2: From the Cost analysis blade, filter the view by tag
3: Download the usage report
upvoted 1 times

  **[Removed]** 8 months ago

correct
upvoted 1 times

  **rocky48** 2 years, 1 month ago



Correct Answer:

Box 1: Assign a tag to each resource
Box 2: From the Cost analysis blade, filter the view by tag
Box 3: Download the usage report

upvoted 3 times

  **testoneAZ** 2 years, 4 months ago



Answer is correct
upvoted 1 times

  **Yugang** 2 years, 4 months ago


Box 1: Assign a tag to each resource
Box 2: From the Cost analysis blade, filter the view by tag
Box 3: Download the usage report
Correct Answer
upvoted 1 times

  **Pinkshark** 2 years, 5 months ago

correct as defined in the result box
upvoted 1 times

  **mahtab** 2 years, 5 months ago

Correct
upvoted 1 times

  **NaoVaz** 2 years, 7 months ago

1) Assign a Tag to each resource;
2) From the Cost analysis blade, filter the view by tag;
3) Download the Usage Report.

upvoted 4 times

  **EmnCours** 2 years, 8 months ago

Correct Answer:



Box 1: Assign a tag to each resource
Box 2: From the Cost analysis blade, filter the view by tag
Box 3: Download the usage report
upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

Given answer is correct
upvoted 2 times

  **manalshowaei** 2 years, 10 months ago

1: Assign a tag to each resource
2: From the Cost analysis blade, filter the view by tag
3: Download the usage report
upvoted 1 times

  **hm67** 3 years, 2 months ago

Was on exam recently.
my answer:

Assign a tag to each resource
From the Cost analysis blade, filter the view by tag
Download the usage report
upvoted 2 times

  **ABhi101** 3 years, 4 months ago

Correct Answer
upvoted 1 times

  **Sara_Mo** 3 years, 5 months ago

Correct Answer
upvoted 1 times

  **flash007** 3 years, 9 months ago

You tag individual resources not groups
upvoted 3 times

  **klasbeatz** 2 years, 10 months ago

No you tag resource group and resources inherit the tag. You can also tag individual resources
upvoted 1 times

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1. You need to view the error events from a table named Event. Which query should you run in Workspace1?

- A. Get-Event Event | where {\$_.EventType == "error"}
- B. search in (Event) "error"
- C. select * from Event where EventType == "error"
- D. search in (Event) * | where EventType -eq "error"

Correct Answer: B

Community vote distribution



GepeNova Highly Voted 3 years, 7 months ago

Correct B
Tested in lab Home>>Monitor>>Logs
All command queries return syntax error except Search in (Event) "error"
upvoted 48 times

djhyfdgjk 1 year, 2 months ago
Just testet in actual Azure LAW. "B" returns syntax error.
upvoted 1 times

NaoVaz Highly Voted 2 years, 7 months ago

Selected Answer: B
B) 'search in (Event) "error"'

Seems to be the correct option. Tested in lab.
upvoted 7 times

Ivanvazovv Most Recent 1 month, 3 weeks ago

Selected Answer: B
Got curious because I've never used such syntax in KQL so I tested.
A is a powershell type query, while C is a SQL type. Strangely enough B worked and is the correct answer.
upvoted 1 times

RVivek 6 months, 1 week ago

Selected Answer: B
<https://learn.microsoft.com/en-us/kusto/query/search-operator?view=microsoft-fabric#search-a-specific-table>
upvoted 3 times

Sifon_n 6 months, 1 week ago

Selected Answer: B
Definitely B
upvoted 1 times

happpieee 6 months, 2 weeks ago

Selected Answer: B
B, with correct KQL syntax.
upvoted 1 times

mcc 7 months, 2 weeks ago

Correct B
// 1. Simple term search over all unrestricted tables and views of the database in scope
search "billg"

// 2. Like (1), but looking only for records that match both terms
search "billg" and ("steveb" or "satyan")

// 3. Like (1), but looking only in the TraceEvent table
search in (TraceEvent) and "billg"

// 4. Like (2), but performing a case-sensitive match of all terms
search "BillB" and ("SteveB" or "SatyaN")

// 5. Like (1), but restricting the match to some columns
search CEO:"billg" or CSA:"billg"

// 6. Like (1), but only for some specific time limit
search "billg" and Timestamp >= datetime(1981-01-01)

// 7. Searches over all the higher-ups
search in (C*, TF) "billg" or "davec" or "steveb"

// 8. A different way to say (7). Prefer to use (7) when possible
union C*, TF | search "billg" or "davec" or "steveb"

upvoted 3 times

  **MCLC2021** 7 months, 2 weeks ago

The correct option in Kusto Query Language (KQL) is C:

Option C: select * from Event where EventType == "error"
This command selects all rows from the table named "Event" where the value of the column "EventType" is equal to "error".
The other options are not syntactically correct in KQL:



Option A: Get-Event Event | where {\$_.EventType == "error"}
This is not a valid syntax in KQL. The "Get-Event" command does not exist in KQL.
Option B: search in (Event) "error"
Although it resembles KQL, it is not a valid syntax. The keyword "search" is not used this way in KQL.
Option D: search in (Event) * | where EventType -eq "error"
Similar to option B, the "search" keyword is not used this way in KQL. Additionally, the comparison should be with "=", not "-eq".

upvoted 4 times

  **[Removed]** 8 months ago

Selected Answer: B



B is corerct
upvoted 1 times

  **Neel2211** 8 months, 1 week ago

The correct correct answer would be :
D. search in (Event) * | where EventType -eq "error"

Log Analytics Workspace has its root usage with the querying of data/logs specifically using the KQL. Option D represents the correct syntax for querying using KQL.

upvoted 1 times

  **Wojer** 1 year, 1 month ago

Event | where EventLevelName == "Error"
upvoted 2 times

  **ricardona** 1 year, 6 months ago

Selected Answer: B

The correct query to run in Workspace1 to view the error events from a table named Event is:

B. search in (Event) "error"

This query will search for the term "error" in the Event table. The other options are not valid queries for Azure Log Analytics. Azure Log Analytics uses a version of the Kusto query language, and these queries do not conform to the correct syntax. For example, the 'select' statement is not used in Kusto, and PowerShell-style syntax (like option A) is not applicable here. Option D is incorrect because it attempts to use a mix of Kusto and PowerShell syntax.

upvoted 2 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: B

Tested in lab.
upvoted 1 times



  **Andreas_Czech** 1 year, 11 months ago

Selected Answer: B

like GepeNova
Correct is B
Tested in LAB
upvoted 2 times

  **Mysystemad** 1 year, 11 months ago

B correct
upvoted 1 times

  **Exilic** 1 year, 12 months ago

Selected Answer: D

OpenAI

"The correct query to view the error events from the table named Event in the Azure Log Analytics workspace Workspace1 is:

D. search in (Event) * | where EventType -eq "error"

Explanation:

Option A is a PowerShell command, not a Log Analytics query language (KQL) command.

Option B is not a valid KQL query. The correct syntax for searching for events in a Log Analytics workspace is "search <query>".

Option C is a valid KQL query, but it is not the best option since it selects all columns from the Event table. It is recommended to select only the necessary columns to improve the query performance.

Option D is a valid KQL query that searches for all events in the Event table where the EventType column equals "error". This is the correct query to view the error events from the Event table."

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

B is correct.

Option D uses a syntax that is similar to KQL, but the correct syntax would be:

D. search in (Event) * | where EventType == "error"

upvoted 2 times



  **Nana1990** 1 year, 10 months ago

Apologies for the confusion. You are correct. The correct query to view the error events from the "Event" table in Azure Log Analytics Workspace1 is:

B. search in (Event) "error"


This query uses the 'search' operator to search for the keyword "error" within the "Event" table in Azure Log Analytics Workspace1. It will return all the events that contain the keyword "error".

upvoted 1 times

  **xRiot007** 1 year, 11 months ago

Lab tests show B is the correct option. This should override whatever OpenAI answered.

upvoted 3 times

  **hz78** 2 years ago

D is correct.

D. search in (Event) * | where EventType -eq "error"

Explanation:



Option A is a PowerShell command and not a Log Analytics query language (KQL) query. It won't work in Workspace1.

Option B is a search query, but it is using a different syntax than KQL. The correct syntax for KQL is 'search' instead of 'search in', and the where clause should be used to filter the results.

Option C is a KQL query, but it is using a wrong syntax. The correct syntax to filter data based on a condition is using 'where' instead of '=' in KQL.

Option D is a valid KQL query to search the Event table in Workspace1 and filter the results based on the 'EventType' field that contains the value "error". Therefore, option D is the correct answer.

upvoted 4 times

  **jackill** 1 year, 9 months ago

"D" is not correct because the equality operator is not "-eq", but "==".

See <https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/logicaloperators>

upvoted 1 times

HOTSPOT -

You have an Azure subscription that contains a virtual network named VNET1 in the East US 2 region. A network interface named VM1-NI is connected to VNET1.

You successfully deploy the following Azure Resource Manager template.

```
{
  "apiVersion": "2017-03-30",
  "type": "Microsoft.Compute/virtualMachines",
  "name": "VM1",
  "zones": "1",
  "location": "EastUS2",
  "dependsOn": [
    "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"
  ],
  "properties": {
    "hardwareProfile": {
      "vmSize": "Standard_A2_v2"
    },
    "osProfile": {
      "computerName": "VM1",
      "adminUsername": "AzureAdmin",
      "adminPassword": "[parameters('adminPassword')]"
    },
    "storageProfile": {
      "imageReference": "[variables('image')]",
      "osDisk": {
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"
        }
      ]
    }
  }
},
{
  "apiVersion": "2017-03-30",
  "type": "Microsoft.Compute/virtualMachines",
  "name": "VM2",
  "zones": "2",
  "location": "EastUS2",
  "dependsOn": [
    "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"
  ],
  "properties": {
    "hardwareProfile": {
      "vmSize": "Standard_A2_v2"
    },
    "osProfile": {
      "computerName": "VM2",
      "adminUsername": "AzureAdmin",
      "adminPassword": "[parameters('adminPassword')]"
    },
    "storageProfile": {
      "imageReference": "[variables('image')]",
      "osDisk": {
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"
        }
      ]
    }
  }
}
```

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

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
VM1 and VM2 can connect to VNET1	<input type="radio"/>	<input type="radio"/>
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input type="radio"/>
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
VM1 and VM2 can connect to VNET1	<input checked="" type="radio"/>	<input type="radio"/>
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	<input checked="" type="radio"/>	<input type="radio"/>
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

Box 2: Yes -
VM1 is in Zone1, while VM2 is on Zone2.

Box 3: No -
Reference:
<https://docs.microsoft.com/en-us/azure/architecture/resiliency/recovery-loss-azure-region>

- pakman**

Highly Voted

3 years, 7 months ago

YES
YES
NO

upvoted 118 times
- rigonet**

3 years, 7 months ago

How do you know VM2-NI is connected to VNET1?

upvoted 51 times
- alex_p**

3 years, 7 months ago

the question actualy is - "VM1 and VM2 can connect VNET1 ? - Yes, they can because both are in tha same region where VNET1 is.

upvoted 52 times
- Philly_cheese_steak**

3 years, 6 months ago

NO YES NO
There is no mention of VM2NI connected to VNET1??

upvoted 46 times
- Ponpon3185**

1 month, 3 weeks ago

There is a mention on tempalte about VM2NI, both VM are on EastUS so VM2NI is able to connect to VNET1, to my mind.

upvoted 1 times
- alsmk2**

8 months, 2 weeks ago

The question says you "successfully" deploy the VM's. Only VNET1 is mentioned and you cannot deploy a VM without a VNET. If both were successful, the only logical assumption is that both use vnet1.

upvoted 8 times

  **Hyrydar** 2 years, 8 months ago

Do you really connect a NIC to a VNet or to a VM? Back in the day when we configured PCs at the street corner shops, we connected the network interface cards to the pc.

upvoted 8 times

  **klexams** 2 years, 6 months ago

Nic to vm but all within a vnet

upvoted 1 times

  **ZooZoo72** 2 years, 7 months ago

Yes but you also connected those cards to a network...hopefully.

upvoted 7 times

  **xRiot007** 1 year, 11 months ago

There is no specification that VM2 NIC is created. In an ARM template I can write whatever I like, so for all we care, VM2 NIC does not exist.



upvoted 8 times

  **jesus_sanchez** 1 year, 10 months ago

Question says "you deploy successfully" and template says that it depends on a network interface named VM2-NI.

It could be clearer and explicit, but if we put those two pieces together it makes sense to infer its existence.

upvoted 8 times

  **76d5e04** 11 months ago

The below content is valid:

[Question says "you deploy successfully" and template says that it depends on a network interface named VM2-NI.]

The deployment would have failed if VM2-NI does not exist

upvoted 1 times

  **dhiii** 1 year, 3 months ago

The answer to first question is in the first sentence - "You have an Azure subscription that contains a virtual network named VNET1 in the East US 2 region" - There is no other Vnet in East US 2, and both VMs are in same region, so, VM2-NI must be connected to VNET1.

So, answer is Yes to first question.

upvoted 1 times

  **aqslatewala** Highly Voted  3 years, 6 months ago

No because VM2NI is not connected to VNET1

Yes



No

upvoted 71 times

  **a4andrew** 3 years, 6 months ago

There is only one VNET mentioned. By default VM2NI is connected to VNET1. According to the template there is no explicit indication that either NIC is assigned to the VNET1, thus my conclusion is that both are assigned to VNET1. My answer for #1 is YES



upvoted 13 times

  **MrAzureGuru** 3 years, 5 months ago

1NI belongs to VNet1, the template mentions no other Vnet, thus it defaults VM2 to VNet1.

The question is primarily testing if you understand default routing between zones, plus availability of VM's if they exist in separate zones.

upvoted 10 times

  **mksdubey** 3 years, 1 month ago

If you see the ARM template JSon for VM2 , in that they have mentioned that VM2 depends on VM2NI and VM2NI is connected to Vnet1 hence it is part of Vnet1

upvoted 2 times

  **xRiot007** 1 year, 11 months ago

VM2NI does not even exist.

upvoted 2 times

  **binhdortmund** 1 year, 2 months ago

ARM was successfully deployed => VM2-NI exists and connected to VNET cause u cant create VM2-NI withou VNet

upvoted 3 times

  **GreenTick** Most Recent  2 months, 2 weeks ago

this ridiculous question, reflecting the stupidity of the questioner.

clearly they would like to test the knowledge

1. zones within vnet can communicate by default.


2. vm can't be created without vnet.

the pitfall is, by giving the half fact that VM1NI connected to VNET1,


this shift the focus whether VM2NI connected to VNET1 or not

if they expected you to answer NO, that's very dumb, low quality question.


upvoted 1 times

-  **junkz** 6 months ago

in my opinion, for first question, we should not even consider the nic to VNET aspect, and focus solely on the region. even if subnet id is not explicitly mentioned in the template, the phrasing is "can connect?". the answer would be yes because of same region. so even if vm2 is "connected" already from template deployment to another vnet in eastus2, it "can connect" also if it needs to vnet1, because same region

upvoted 4 times
-  **Stunomatic** 6 months, 2 weeks ago


for those who think that vm2 is by default connecting to vnet1 ? how you know ? and why he is only mentioned that vm1 connected to vnet1. maybe there are more vnets why are we assuming ? maybe successfully deploy in vnet100000000000000. haha NYN

upvoted 2 times
-  **EmnCours** 7 months, 2 weeks ago

1. No - because it's not stated the VM2-NI is connected to the VNET1 in the description - the question is can they both connect to VNET1 - so you don't know for VM2-NI

2. Yes - because the question embraces both the machines - and VM2 is spread over 2 zones, not being in the same DC.

3. No - being both machines in EastUS2 - when the region goes down - both of them sink too.

upvoted 4 times
-  **NaoVaz** 7 months, 2 weeks ago

Answers:

1) VM1 and VM2 can connect to VNET1 = YES

2) If an Azure datacenter becomes unavailable, VM1 or VM2 will be available = YES


3) If the East US 2 region becomes unavailable, VM1 or VM2 will be available = NO

Explanation:

1) Being in the same region booth VM's can connect to the same VNET.

2) VM1 and VM2 are in different Zones, so if a Datacenter becomes unavailable, either one or another will still be available.

3) Booth VM's are on the same Region, so if it goes down booth VM's will be down also.

upvoted 10 times
-  **NickTim** 7 months, 2 weeks ago

Copilot Says:

YES:

VM1 and VM2 can connect to VNET1: Both VMs are connected to the virtual network VNET1.


YES:

If an Azure datacenter becomes unavailable, VM1 or VM2 will be available: Since VM1 and VM2 are in different availability zones, if one datacenter (zone) becomes unavailable, the other VM in a different zone will still be available.


NO:

If the East US 2 region becomes unavailable, VM1 or VM2 will be available: If the entire East US 2 region becomes unavailable, both VMs will be affected and will not be available.

(Region Pair is not applicable because not mentioned on ARM template and should be setting up in advance)

upvoted 2 times
-  **[Removed]** 8 months ago

correct


upvoted 1 times
-  **CheMetto** 9 months, 1 week ago

mmmh, the answer in this case is completely personal. I'll go for YYN, but the other side is NNN. I did some research, and based from this link: <https://github.com/Azure/azure-quickstart-templates/blob/master/quickstarts/microsoft.network/vnet-2subnets-service-endpoints-storage-integration/azuredeploy.json>


effectively in the template is missing the part of the subnet related to vnic, so this one:

"subnet": {
 "id": "[variables('subnetId')[copyIndex()]]"
},


Although is missing this one, so it should be NNN, is Microsoft really so a*****e to do that? Idk. I'll go for YYN

upvoted 1 times
-  **varinder82** 11 months, 3 weeks ago

Final Answer: Y Y N



upvoted 2 times
-  **af68218** 1 year, 1 month ago

For those who, like me, were struggling to understand why VM1 and VM2 can both connect to VNET1 despite having different NICs, see the excerpt below, and know that I tested this by creating a couple of VMs, each on their own networks, and was able to log into one and RDP into the other from it.
"Each NIC attached to a VM must exist in the same location and subscription as the VM. Each NIC must be connected to a VNet that exists in the same Azure location and subscription as the NIC. "
<https://learn.microsoft.com/en-us/azure/virtual-network/network-overview>

upvoted 6 times
-  **Amir1909** 1 year, 2 months ago

Correct

upvoted 1 times

  **dhiii** 1 year, 3 months ago

The answer to first question is in the first sentence - "You have an Azure subscription that contains a virtual network named VNET1 in the East US 2 region" - There is no other Vnet in East US 2, and both VMs are in same region, so, VM2-NI must be connected to VNET1.

So, answer is Yes to first question.

upvoted 3 times

  **SgtDumitru** 1 year, 5 months ago

1. NO - There is no mention that VM2 is deployed in VNET1 or that NIC2 is connected to VNET1

2. YES - If a datacenter will be unavailable, at least one on VM will be available since their are in different data centers a.k.a zones

3. NO - Both VMs are in same Region

upvoted 2 times

  **SgtDumitru** 1 year, 4 months ago

Ok, so based on answer in this thread, first question is YES, despite not having any mentioning of VM2-NIC related to VNET1. Question suppose that you deploy VM1 & VM2 to same VNET, but different zones. Since they are "by Microsoft logic" deployed in same VNET, yes they can connect.

upvoted 3 times

  **FlaShhh** 1 year, 4 months ago

bro came back to correct himself, Respect.Have you given the exam yet? your comment seems the latest here

upvoted 2 times

  **amsioso** 1 year, 6 months ago

YES, YES, NO

<https://learn.microsoft.com/en-us/azure/virtual-network/network-overview#virtual-machines>

upvoted 1 times

  **Babustest** 1 year, 7 months ago

Nowhere it's mentioning VM2-NI is in VNET1.

upvoted 2 times

You have an Azure subscription named Subscription1. Subscription1 contains the resource groups in the following table.

Name	Azure region	Policy
RG1	West Europe	Policy1
RG2	North Europe	Policy2
RG3	France Central	Policy3

RG1 has a web app named WebApp1. WebApp1 is located in West Europe.

You move WebApp1 to RG2.

What is the effect of the move?



- A. The App Service plan for WebApp1 remains in West Europe. Policy2 applies to WebApp1.
- B. The App Service plan for WebApp1 moves to North Europe. Policy2 applies to WebApp1.
- C. The App Service plan for WebApp1 remains in West Europe. Policy1 applies to WebApp1.
- D. The App Service plan for WebApp1 moves to North Europe. Policy1 applies to WebApp1.

Correct Answer: A

Community vote distribution

A (86%)

9%

  **mlantonis**



Highly Voted

 3 years, 11 months ago

Correct Answer: A

You can only move a resource to a Resource Group or Subscription, but the location stays the same. When you move WebApp1 to RG2, the resource will be restricted based on the policy of the new Resource Group (Policy2).

upvoted 133 times

  **Veks** 3 years ago



I agree with the answer (A is correct), but your comments don't seem correct. you are moving app from one region to another. Procedure is listed below:

- Create a back up of the source app.
- Create an app in a new App Service plan, in the target region.
- Restore the back up in the target app
- If you use a custom domain, bind it preemptively to the target app with 'awverify'. and enable the domain in the target app.
- Configure everything else in your target app to be the same as the source app and verify your configuration.
- When you're ready for the custom domain to point to the target app, remap the domain name.

Here it states that you have to create new AppService plan in new region. So old plan stays where it is.



Reference:
<https://docs.microsoft.com/en-us/azure/app-service/manage-move-across-regions>

upvoted 20 times

  **klexams** 2 years, 11 months ago



@veks, so you're saying A is wrong then?!

upvoted 2 times

  **Ajinkyakore** 2 years, 11 months ago



So technically there will be no any migration or transfer happens?

upvoted 2 times

  **bryant12138** 1 year, 6 months ago



yeah I think you're right, both rg and subscription are ideological management tools

upvoted 1 times

  **klasbeatz** 2 years, 10 months ago



Your right.....New-AzAppServicePlan -Location "North Central US" -ResourceGroupName DestinationAzureResourceGroup -Name DestinationAppServicePlan -Tier Standard

upvoted 1 times

  **klasbeatz** 2 years, 10 months ago

But the question suggest that it is being moved...not "cloned"



upvoted 4 times



  **mcclane654** 1 year, 3 months ago



just to add to this. as I found the policy confusing. if they are talking about Azure policy: An evaluation will be ran before the move to verify that policy2 allows it.

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription#frequently-asked-questions>
upvoted 1 times



  **Cluster007** Highly Voted 4 years, 5 months ago
A is correct
upvoted 43 times



  **lumax007** Most Recent 1 month, 2 weeks ago
Selected Answer: A
The App Service plan for WebApp1 remains in West Europe. Policy2 applies to WebApp1.
upvoted 1 times



  **raidenstrike1945** 2 months, 3 weeks ago
Selected Answer: A
Moving an Azure Web App to another region typically involves creating a new App Service plan in the target region, as App Service plans are region-specific and cannot be directly moved across regions
upvoted 1 times



  **Jay_D_Lincoln** 3 months ago
Selected Answer: A
Resource Group Location ≠ Resource Location



A Resource Group (RG) is a logical container and does not dictate the physical region of the resources inside it. Resources within an RG can be spread across multiple regions.
upvoted 1 times



  **kejo2** 7 months, 1 week ago
Tested in my Lab. A is correct
upvoted 1 times

  **[Removed]** 8 months ago
Selected Answer: A
A is corerct
upvoted 1 times



  **TheFivePips** 9 months, 1 week ago
Selected Answer: A
My understanding is that App service plans cannot move regions. If you wanted to move it you would have to recreate it in a new region. And since the policies in this case are applied at the resource group level, and the only thing moving is the outsource webapp1, not the resource group itself, then the policies of the new RG2 will apply.
upvoted 3 times



  **robsoneuclides** 11 months, 1 week ago
Esta correta
upvoted 1 times



  **camwilson04** 1 year ago
Moving to a resource group in a different region doesn't also move the resources to the same region as the RG.. come on guys! RG just hold meta data of the connected resources
upvoted 2 times



  **Wojer** 1 year, 1 month ago
Selected Answer: B
App Service resources are region-specific and can't be moved across regions. You must create a copy of your existing App Service resources in the target region, then move your content over to the new app. If your source app uses a custom domain, you can migrate it to the new app in the target region when you're finished.

To make copying your app easier, you can clone an individual App Service app into an App Service plan in another region, but it does have limitations, especially that it doesn't support Linux apps.
upvoted 3 times

  **93d821b** 1 year, 5 months ago
https://www.youtube.com/watch?v=QBAOI2dZS_c
Answer is B
upvoted 2 times

  **2d153f5** 5 months, 3 weeks ago
Nooooooooooo. In the video, the answers are changed positions.
upvoted 2 times

  **Andmachado** 11 months ago
In the video you showed, the correct answer is the letter A, in the video the answer is stated, so A is the correct one.
upvoted 2 times

  **clg003** 1 year, 5 months ago

Selected Answer: C

I know its not the popular opinion but I think its correct. I got receipts...

Everyone seems to get that when you move a resource to a new resource group you dont change its location, but knowing that why do you think it changes its app service plan? App Service plan lays out the region resources for the apps that run in it and the you just agreed the region of the actual app service is not changing. So why would it then change to a app service plan that's laying out region specific limits.



Also according to MS...

"You can move an app to another App Service plan, as long as the source plan and the target plan are in the same resource group, geographical region, and of the same OS type."

According to this its not even possible to move the app to a new app service plan that's not in the same region or the same resource group... and why would it. Since the app service plan lays out the resources in a region that all of its apps will share?



<https://learn.microsoft.com/en-us/azure/app-service/app-service-plan-manage>

upvoted 5 times

  **clg003** 1 year, 7 months ago

Remember... "The resource group stores metadata about the resources. Therefore, when you specify a location for the resource group, you are specifying where that metadata is stored." This should help people understand why moving a resource into a new resource group will not change its location.

upvoted 4 times

  **mtc9** 1 year, 7 months ago

Respurce and RG can be in different regions. Moving a resource do different RG doesn;t change the resource's region.

upvoted 1 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: A

"you cannot change an App Service plan's region. If you want to run your app in a different region"

<https://learn.microsoft.com/en-us/azure/app-service/app-service-plan-manage#move-an-app-to-a-different-region>



<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations#move-across-subscriptions>

upvoted 2 times

  **Mehedi007** 1 year, 9 months ago

you cannot change an App Service plan's region.

upvoted 2 times

  **Rogit** 1 year, 9 months ago

Selected Answer: A

Came in test yesterday

upvoted 3 times

HOTSPOT -

You have an Azure subscription named Subscription1 that has a subscription ID of c276fc76-9cd4-44c9-99a7-4fd71546436e.

You need to create a custom RBAC role named CR1 that meets the following requirements:

- Can be assigned only to the resource groups in Subscription1
- Prevents the management of the access permissions for the resource groups
- Allows the viewing, creating, modifying, and deleting of resources within the resource groups

What should you specify in the assignable scopes and the permission elements of the definition of CR1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

"assignableScopes": [

"/"

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups"

,

"permissions": [

{

"actions": [

"x"

],

"additionalProperties": {},

"dataActions": [],

"notActions": [

"Microsoft.Authorization/*"

"Microsoft.Resources/*"

"Microsoft.Security/*"

],

"notDataActions": []

}

],

Answer Area

```
"assignableScopes": [  
  "  
  "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"  
  "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups"  
],  
"permissions": [  
  {  
    "actions": [  
      "  
    ],  
    "additionalProperties": {},  
    "dataActions": [],  
    "notActions": [  
      "  
      "Microsoft.Authorization/*"  
      "Microsoft.Resources/*"  
      "Microsoft.Security/*"  
    ],  
    "notDataActions": []  
  }  
],  
}
```

Correct Answer:



  **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"


"Microsoft.Authorization/"

upvoted 355 times

  **Awot** 1 year, 7 months ago

I have the feeling that the first option "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e" is wrong. because it doesn't specify the resource group, the implication is that the user will have access to all other things in the subscription.

upvoted 9 times

  **Slimus** 1 year, 11 months ago

Azure RBAC) is the authorization system you use to manage access to Azure resources.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

upvoted 2 times

  **justin19981** 2 years, 5 months ago

So often I have the feeling; This HAS to be wrong. And finding the community confirming my thoughts is nice :)

upvoted 15 times

  **Mitazure7** 1 year, 6 months ago

In Azure, the correct format for specifying a resource group's path within a subscription is as follows:

/subscriptions/<subscription_id>/resourceGroups/<resource_group_name>

upvoted 4 times

  **fedztetz** Highly Voted 4 years, 4 months ago

The Answer is Wrong.


First part should be "/Subscription/subcription_id" only. There is nothing called "resourceGroups" only or "resourceGroups/*" . You can specify either a subscription, specific resource group, management group or specific resource. for example it should

"/subcription/subcription_id/resourceGroups/resource_group_name"

Check <https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/role-based-access-control/role-definitions.md#role-definition-structure>

For second box. It is correct but missing "*". It should be "Microsoft.Authorization/*" . if you try this on az cli without "*". you will get an error

upvoted 243 times

  **JayBee65** 3 years, 10 months ago

This link <https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions> gives an example of

"/subscriptions/{subscriptionId}/resourceGroups/Network"

upvoted 10 times

  **tf444** 3 years, 11 months ago

```
{  
  "id": "/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}",  
  "name": "{resourceGroupName}",  
  "type": "Microsoft.Resources/resourceGroups",  
  "location": "{resourceGroupLocation}",  
}
```


```
"managedBy": "{identifier-of-managing-resource}",
"tags": {
},
"properties": {
"provisioningState": "{status}"
}
}
```

upvoted 2 times

  **rrobb** 4 years ago

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-rest#create-a-custom-role>
Can `/ {resourceGroup1}` be replaced by name or `*`?

upvoted 2 times

  **Acai** 3 years, 9 months ago

I don't know how you said there's no 'resourceGroups' and then put 'resourceGroups' in your example, also an asterisk/wildcard meaning denotes "all" this could imply there are multiple other fields the could be added in place of the wildcard. Regardless, I tested it, you can go to Subscriptions > [Your Subscription] > IAM > Custom Roles. You are correct but the explanation was quite confusing.

upvoted 7 times

  **mufflon** 3 years, 3 months ago

You can specify either a subscription, specific resource group, management group or specific resource. for example it should `"/subscription/subscription_id/resourceGroups/resource_group_name"`

So it you use `"/subscription/subscription_id/resourceGroups/resource_group_name"` then you need the `resource_group_name`

upvoted 2 times

  **lumax007** Most Recent 1 month, 2 weeks ago

You need to create a custom RBAC role named CR1 that meets the following requirements:

- Can be assigned only to the resource groups in Subscription1
- Prevents the management of the access permissions for the resource groups
- Allows the viewing, creating, modifying, and deleting of resources within the resource groups

Below are the correct answers

`"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"`

`"Microsoft.Authorization/"`

upvoted 1 times

  **rikininetysix** 7 months, 2 weeks ago

The given answer is correct. As the standard format for a resource ID is :

`"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/{resourceProviderNamespace}/{resourceType}/{resourceName}'`

It clearly contains `"/subscriptions/{subscriptionId}/resourceGroups/'` which should be the proper assignable scope. In order to prevents the management of the access permissions for the resource groups (requirement 2), you need to select `'Microsoft.Authorization/'` under permissions, notActions.

If the assignable scope is `"/subscriptions/{subscriptionId}/'` the notAction permission `'Microsoft.Authorization/'` would prevent the management of access permission at the subscription level, which is not asked in the question.

This link validates the resource ID structure - <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription>

upvoted 2 times

  **[Removed]** 7 months, 3 weeks ago

WRONG

`"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"`

`"Microsoft.Authorization/*"`

upvoted 2 times

  **Amir1909** 1 year, 2 months ago

Correct Answer: `"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"`

`"Microsoft.Authorization/"`

upvoted 2 times

  **Mitazure7** 1 year, 6 months ago

In Azure, the correct format for specifying a resource group's path within a subscription is as follows:

`/subscriptions/<subscription_id>/resourceGroups/<resource_group_name>`

upvoted 1 times

  **TedM2** 1 year, 6 months ago

The answer shown for the first part seems to be incorrect, per

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#assignablescope>

upvoted 1 times

  **Josete1106** 1 year, 9 months ago

Correct Answer:

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"
"Microsoft.Authorization/"
upvoted 3 times
```

  **Aluksy** 2 years ago

Correct Answer :

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"
"Microsoft.Authorization/"
```

Came out in my exam today 8th April 2023. Passed 830.
upvoted 11 times

  **rocky48** 2 years, 1 month ago

Correct Answer:

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"
"Microsoft.Authorization/"
upvoted 4 times
```



  **orionduo** 2 years, 3 months ago

It should be "/Subscription/subcription_id" only.



There is nothing called "resourceGroups" only or "resourceGroups/*"

Note: You can specify either a subscription, specific resource group, management group or specific resource. For example, it should be
"/subscription/subcription_id/resourceGroups/resource_group_name"

```
"Microsoft.Authorization/" is right
upvoted 3 times
```

  **CoachV** 2 years, 3 months ago



<https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>
upvoted 1 times

  **CoachV** 2 years, 3 months ago

The answers provided are actually correct. Look at the syntax of the JSON command below.

```
{
  "properties": {
    "roleName": "Billing Reader Plus",
    "description": "Read billing data and download invoices",
    "assignableScopes": [
      "/subscriptions/11111111-1111-1111-1111-111111111111"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Billing/*/read",
          "Microsoft.Commerce/*/read",
          "Microsoft.Consumption/*/read",
          "Microsoft.Management/managementGroups/read",
          "Microsoft.CostManagement/*/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

upvoted 1 times

  **sk4shi** 1 year, 10 months ago

CoachV does have a fair point, although this JSON is not showing the fuller picture. If you look at the link CoachV posted and look at Step 5, point 2 there is an information section above in the screenshot that reads: "Select a management group, subscription or resource group to add as an assignable scope. You can only choose from the scopes that you have access to." - that would indicate that the provided answers are correct
upvoted 1 times

  **RougePotatoe** 2 years, 3 months ago

Dawg the provided answer was /subscription/sub_id/resourceGroups. What you posted here is not the same thing.

upvoted 2 times

  **geisonferreira** 2 years, 3 months ago

Why are wrong answers not corrected? This site is sometimes more confused than helpful.

upvoted 11 times

  **NaoVaz** 2 years, 7 months ago

- 1) "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"
- 2) "Microsoft.Authorization/*"

"assignableScopes" must be the Subscription, so that this Custom Role can be only assignable to Resources Groups under the same Subscription.

"notActions" must deny only the actions that interact with the Authorization API Endpoints. Everything else must\can be allowed.

upvoted 11 times

  **ThatDowntownSmell** 2 years, 9 months ago

Regarding the assignable scopes part of the question: THERE IS NO WAY TO WILDCARD RESOURCEGROUPS AS AN ASSIGNABLE SCOPE!

You can add all of the resource groups in the subscription individually, but you cannot wildcard all of them using /resourceGroups. If you go into Azure Portal and create a custom role under a subscription, you will see clearly that it is not possible - you must select a resource group when using the /resourceGroups type of assignable scope. The result will look similar to:

/subscriptions/xxxxxxx-xxxxx-xxxx-xxxx-xxxxxxxxx/resourceGroups/RG1

upvoted 7 times

You have an Azure subscription.

Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by using site-to-site VPNs.

You have a line-of-business-app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016.

You need to ensure that the connections to App1 are spread across all the virtual machines.

What are two possible Azure services that you can use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.



- A. an internal load balancer
- B. a public load balancer
- C. an Azure Content Delivery Network (CDN)
- D. Traffic Manager
- E. an Azure Application Gateway


Correct Answer: AE

Community vote distribution

AE (87%)

7%

-   **mlantonis**

Highly Voted 

 3 years, 11 months ago

Correct Answer: A and E



A: The customer sites are connected through VPNs, so an internal load balancer is enough.

B: The customer sites are connected through VPNs, so there's no need for a public load balancer, an internal load balancer is enough.

C: A CDN does not provide load balancing for applications, so it not relevant for this situation.



D: Traffic manager is a DNS based solution to direct users' requests to the nearest (typically) instance and does not provide load balancing for this situation.

E: Azure Application Gateway is a valid option, as it provides load balancing in addition to routing and security functions



upvoted 545 times
-   **Veks** 3 years ago

I agree with an answer, this is only logical solution (A and E), but the questions are really.... stupid.



"Several virtual machines for running an app", that doesn't explicitly mean that I'll use load balancer. I could have lots of different VM configurations and not use load balancer. What if I'm doing an SPA app and have an API's on different VM (cause of any user defined, project specific needs). In that case what is my App then? Is it just a client side or is it a backend API. Anyway, sry for spamming, I just would like them to have more precise questions.

upvoted 7 times
-   **ShaulS** 3 years, 5 months ago



A: what do you mean by "internal LB is enough"?

upvoted 2 times
-   **e_karma** 3 years, 5 months ago



It means that nobody is accessing the resources through public ip ..So no need of a public load balancer.

upvoted 27 times
-   **juniorccs** 3 years, 9 months ago



Very nice and complete explanation, thanks a lot!

upvoted 3 times
-   **Sh4kE** 3 years, 3 months ago

But isn't answer B also an option which would suffice the requirements? It only states to load balance traffic to all VMs. It does not restrict how to access the services, even though we are already connected via vpn...



upvoted 3 times
-   **Def21** 2 years, 11 months ago

I'd say you are right. But they ask only for two answers and this would not be preferred solution.

upvoted 1 times
-   **klexams** 2 years, 11 months ago

there is a reason why people use VPN.

upvoted 1 times

  **zr79** 3 years, 2 months ago

VMs are internal and users connect through S2S and P2S VPN. you do not want to expose your internal workloads to the internet using public LB

upvoted 2 times

  **mgladh** Highly Voted  4 years, 5 months ago

i would say A and E is the correct answer.



upvoted 88 times

  **lumax007** Most Recent  1 month, 2 weeks ago

Selected Answer: AE

A & E is the correct answer

upvoted 1 times

  **Ponpon3185** 2 months ago

Selected Answer: DE

The question is "What are two possible Azure solutions", Internal Load Balancer is not an "Azure solution". Traffic Manager is an Azure solution witch make Load Balancing, so why "A"?

upvoted 1 times

  **achuphoenix** 2 months, 1 week ago

Selected Answer: AE

Exhausting Az104 exam Never coming back to this

upvoted 1 times

  **dnt91** 4 months, 3 weeks ago

Selected Answer: AD

Public Load Balancer cannot be used here as the connections must use a VPN (ie private ip addresses on Azure)

Application Gateway is not on option. a lob application is not a web app (even some old web app can be lob application.)

the first (and most natural) answer is an internal load balancer.

The second is traffic manager. You can configure a traffic manager with for example a routing method weighted and then add to your TM an external endpoint with a private IP address

upvoted 1 times

  **CloudEngJS** 5 months ago

Selected Answer: AB

Line of business app can be anything custom written, it never mentioned web app. App Gateway uses http and https, so it may not work, ergo internal and external load balancers are the answer by process of elimination.

upvoted 1 times

  **Sunth65** 5 months ago

NB! You have a line-of-business-app named App1 that runs on several Azure virtual machine.



upvoted 1 times

  **CloudEngJS** 5 months, 3 weeks ago

Selected Answer: AB

The question never stated this is a web app, therefore the only plausible answers are internal or public load balancer. Web app only support http(s)

upvoted 1 times

  **Dankho** 6 months, 2 weeks ago

Selected Answer: AE


Wouldn't pick the public one so...

upvoted 1 times

  **GuessWhoops** 7 months ago

You know what is complicated? Azure Application Gateway is used specific for HTTP/HTTPS based requests, in its setup, when you create the routing rule, there is an option that force you to select the Protocol either HTTP or HTTPS, there is a port option, but those are for custom ports, fact is, it is based on HTTP/S. This question does not specify if the line-of-business app is HTTP/S based, a WebApp. A public balancer here would be a more broad option to attend all scenarios, however, yes, it would have a cost for public IP and would be unnecessary since we already got VPNs setup. This is one of those scenarios that I would comment on the question, stating that is poorly worded. No doubt on Internal LB, but cant decide here between AAG/PLB.

upvoted 1 times

  **lokii9980** 7 months, 2 weeks ago


Two possible Azure services that can be used to spread connections to App1 across all virtual machines are:

A. An internal load balancer: This service can be used to distribute network traffic to virtual machines that are part of an availability set or a virtual machine scale set. It works by forwarding incoming traffic to healthy virtual machines in the backend pool. Since App1 runs on multiple virtual machines, an internal load balancer can be used to distribute the traffic evenly among them.

E. An Azure Application Gateway: This service is a layer 7 load balancer that can distribute traffic based on different criteria, such as URL path or host header. It can also perform SSL offloading, web application firewall, and other features that can enhance the performance and security of web

applications. Since App1 is a line-of-business app, it's likely that it runs over HTTP or HTTPS, which makes an Azure Application Gateway a suitable solution for load balancing.

upvoted 1 times

  **Madbo** 7 months, 2 weeks ago

Two possible Azure services that can be used to spread connections to App1 across all virtual machines are:

A. an internal load balancer: An internal load balancer can be used to distribute traffic among the virtual machines running App1. It can distribute traffic based on various algorithms such as round-robin, least connections, and IP hash. The internal load balancer is a layer 4 (Transport Layer) load balancer that can distribute traffic within a virtual network.

E. an Azure Application Gateway: An Azure Application Gateway is a layer 7 (Application Layer) load balancer that can distribute traffic based on various criteria such as URL path, host headers, and cookie. It can also perform SSL offloading, session affinity, and URL-based routing. It is typically used to route traffic to different backend services based on the incoming request's contents. It is a more advanced option than the internal load balancer but requires a public IP address.



upvoted 5 times

  **[Removed]** 8 months ago

Selected Answer: AE

A & E are correct



upvoted 1 times

  **SefOne** 1 year, 7 months ago

Selected Answer: AE

No doubt about it AE

upvoted 1 times

  **itguyeu** 1 year, 10 months ago

I used free version access for this site and it helped me pass the exam. Some questions that I had on the exams, I took the exam more than once, are not available under the free tier access, but 80% of the questions came from here. I do recommend investing a bit of money and getting full access to this site. I didn't memorise answers but analysed them and studied as Microsoft does tweak them a bit.

This Q was on the exam and the answer isA, E.

upvoted 3 times

  **Mazinger** 2 years, 2 months ago

Selected Answer: AE



Two possible Azure services that can be used to spread connections to App1 across all virtual machines are:

A. An internal load balancer: This can be used to distribute incoming traffic to virtual machines in a backend pool based on various routing rules and health probes. It is a Layer 4 (TCP/UDP) load balancer that is used for internal traffic within a virtual network.

E. An Azure Application Gateway: This can be used to route incoming traffic to virtual machines based on various routing rules, including URL path-based routing, cookie-based session affinity, and SSL offloading. It is a Layer 7 (HTTP/HTTPS) load balancer that can be used for both internal and external traffic.

Both of these services can be used to distribute incoming traffic across multiple virtual machines, improving availability and scalability of App1.

upvoted 2 times

  **Blippen** 2 years, 4 months ago

Correct Answer: A and E

Given that the application is a webapp.

upvoted 1 times



You have an Azure subscription.
You have 100 Azure virtual machines.
You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.
Which blade should you use?


- A. Monitor
- B. Advisor
- C. Metrics
- D. Customer insights

Correct Answer: B

Community vote distribution

B (100%)

-  **waterzhong**

Highly Voted 

 4 years, 3 months ago

The Advisor dashboard displays personalized recommendations for all your subscriptions. You can apply filters to display recommendations for specific subscriptions and resource types. The recommendations are divided into five categories:



Reliability (formerly called High Availability): To ensure and improve the continuity of your business-critical applications. For more information, see Advisor Reliability recommendations.


Security: To detect threats and vulnerabilities that might lead to security breaches. For more information, see Advisor Security recommendations.

Performance: To improve the speed of your applications. For more information, see Advisor Performance recommendations.

Cost: To optimize and reduce your overall Azure spending. For more information, see Advisor Cost recommendations.

Operational Excellence: To help you achieve process and workflow efficiency, resource manageability and deployment best practices. . For more information, see Advisor Operational Excellence recommendations.



upvoted 117 times
-  **mlantonis**


Highly Voted 

 3 years, 11 months ago

Correct Answer: B

Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.

upvoted 104 times
-  **lumax007**



Most Recent 

 1 month, 2 weeks ago

Selected Answer: B

Advisor advises you to optimize the use of your virtual machines. You can filter the advises as well.



upvoted 1 times

 **[Removed]** 8 months ago

Selected Answer: B



B is corerct

upvoted 1 times

 **Amir1909** 1 year, 2 months ago

Correct



upvoted 1 times

 **Mehedi007** 1 year, 9 months ago

Selected Answer: B

"Azure Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources."
<https://learn.microsoft.com/en-us/azure/advisor/advisor-reference-cost-recommendations>

upvoted 1 times

 **Navigati0n** 1 year, 9 months ago

B. Advisor

Explanation:

Azure Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource

configuration and usage telemetry and then recommends solutions that can help you improve the cost-effectiveness, performance, high availability, and security of your Azure resources.

With respect to your question, Azure Advisor can provide recommendations for underutilized VMs and suggest ways to reduce costs, for example, by resizing or shutting down underutilized VMs.

upvoted 1 times

  **Madbo** 2 years ago

B. Advisor blade in Azure can also provide cost recommendations, including recommendations to change service tiers for underutilized virtual machines.

Azure Advisor analyzes your usage data and provides personalized recommendations to optimize your resources, reduce costs, and improve the security and performance of your Azure environment. It can provide recommendations to change the service tier of underutilized virtual machines to a lower tier that better matches their actual resource usage.

Therefore, both the Monitor and Advisor blades can be used to identify underutilized virtual machines that can have their service tier changed to a less expensive offering. The Monitor blade provides real-time utilization data, while the Advisor blade provides personalized recommendations based on historical usage data.

upvoted 1 times

  **Mazinger** 2 years, 2 months ago

Selected Answer: B



The blade that you should use to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering is the "Advisor" blade.

The Advisor blade provides personalized recommendations to optimize and improve the security, performance, and high availability of your resources in Azure. It analyzes your usage and resource configuration data to identify opportunities to reduce costs, improve performance, and increase reliability.

To identify underutilized virtual machines, you can use the "Right-size virtual machines" recommendation in the Advisor blade. This recommendation provides a list of virtual machines that are running with less than 50% average CPU utilization over the past week, and which can potentially have their service tier changed to a less expensive offering.

By using this recommendation, you can quickly identify virtual machines that are underutilized and can potentially save costs by switching to a lower service tier.

upvoted 3 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) "Advisor"

". It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, Reliability (formerly called High availability), and security of your Azure resources." - <https://docs.microsoft.com/en-us/azure/advisor/advisor-overview>



upvoted 4 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

  **eporr** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

  **RichardBill** 2 years, 8 months ago

Selected Answer: B

Its the Advisor

upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

Selected Answer: B

I luv Honey because it is B



upvoted 3 times

  **manalshowaei** 2 years, 10 months ago

Selected Answer: B

B. Advisor

upvoted 1 times

  **Racinely** 2 years, 11 months ago

Azure Advisor

upvoted 1 times

  **Azure_daemon** 3 years, 2 months ago

Advisor is the correct answer
upvoted 1 times

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant.

You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

* Name

Policy1

**Assignments**

Users and groups ⓘ



0 users and groups selected

Cloud apps ⓘ



0 cloud apps selected

Conditions ⓘ



0 conditions selected

Access controls

Grant ⓘ



0 controls selected

Session ⓘ



Answer Area

* Name

Policy1



Assignments

Users and groups ⓘ



0 users and groups selected

Cloud apps ⓘ



0 cloud apps selected

Conditions ⓘ



0 conditions selected

Correct Answer:

Access controls

Grant ⓘ



0 controls selected

Session ⓘ



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa>

 **fedztetz** Highly Voted 4 years, 4 months ago

The Answer is correct .

- Select Users & Groups : Where you have to choose all users.
- Select Cloud apps or actions: to specify the Azure portal
- Grant: to grant the MFA.

Those are the minimum requirements to create MFA policy. No conditions are required in the question.

Also check this link beside the one provided in the answer

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies>

upvoted 305 times

 **Bigbluee** 2 years, 1 month ago

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa#create-a-conditional-access-policy>

- Select New policy.
- Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
- Under Assignments, select Users or workload identities.

Under Include, select All users

Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts.

- Under Cloud apps or actions > Include, select All cloud apps.

Under Exclude, select any applications that don't require multifactor authentication.

- Under Access controls > Grant, select Grant access, Require multifactor authentication, and select Select.

upvoted 17 times

 **redbeardbeer** 3 years, 11 months ago

Thanks for the great description. Very helpful.

upvoted 16 times

 **Shadoken** 2 years, 10 months ago

At the present you can't select Azure Portal. You have to choose «All cloud apps» options I think. Azure Portal doesn't appear as an app to choose.

upvoted 6 times

🗲️ 👤 **mlantonis** Highly Voted 👍 3 years, 11 months ago

Correct Answer:

- Select Users & Groups : Where you have to choose all users.
- Select Cloud apps or actions: To specify the Azure portal
- Select Grant: To grant the MFA.

upvoted 151 times

🗲️ 👤 **[Removed]** Most Recent ⌚ 8 months ago

correct

upvoted 2 times

🗲️ 👤 **rocky48** 2 years, 1 month ago

Correct Answer:

- Select Users & Groups : Where you have to choose all users.
- Select Cloud apps or actions: To specify the Azure portal
- Select Grant: To grant the MFA.

upvoted 2 times

🗲️ 👤 **CoachV** 2 years, 3 months ago

The following steps will help create a Conditional Access policy to require all users do multifactor authentication.

Sign in to the Azure portal as a Conditional Access Administrator, Security Administrator, or Global Administrator.

Browse to Azure Active Directory > Security > Conditional Access.

Select New policy.

Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Under Assignments, select Users or workload identities.

Under Include, select All users

Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts.

Under Cloud apps or actions > Include, select All cloud apps.

Under Exclude, select any applications that don't require multifactor authentication.

Under Access controls > Grant, select Grant access, Require multifactor authentication, and select Select.

Confirm your settings and set Enable policy to Report-only.

Select Create to create to enable your policy.

upvoted 8 times

🗲️ 👤 **AndreLima** 2 years, 4 months ago

Respostas bem confusas.

upvoted 1 times

🗲️ 👤 **NaoVaz** 2 years, 7 months ago

- 1) Assignments -> "Users and Groups"
- 2) Assignments -> "Cloud Apps"
- 3) Access Controls -> "Grant"

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies>

upvoted 4 times

🗲️ 👤 **EmnCours** 2 years, 8 months ago

The Answer is correct .

- Select Users & Groups : Where you have to choose all users.
- Select Cloud apps or actions: to specify the Azure portal
- Grant: to grant the MFA.

upvoted 1 times

🗲️ 👤 **klasbeatz** 2 years, 10 months ago

Tricky one This confused me but makes sense now...."CONDITIONS" is only to add MULTIPLE conditions you are already creating a conditional policy alone with this template

upvoted 5 times

🗲️ 👤 **SivaPannier** 1 year, 8 months ago

Yes.. look at the below link for more information..

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions>

upvoted 1 times

🗲️ 👤 **manalshowaei** 2 years, 10 months ago

Answer is correct

upvoted 1 times

🗲️ 👤 **Jvp21** 3 years, 2 months ago

- Select Users & Groups : To choose all users.
- Select Cloud apps or actions: To specify the Azure portal
- Select Grant: To grant IF only pass the MFA authentication.

upvoted 4 times

  **Mozbius_** 3 years, 3 months ago



Can you believe that "Conditional Access" is barely mentioned in the paid Microsoft training for az104 and yet students are expected to know about it in the exam?!?! Sooo frustrating!!!!

upvoted 8 times

  **Mozbius_** 3 years, 3 months ago


I literally have to GOOGLE many of the topics covered here because of how weak MS courses are toward az104 certification damn it.

upvoted 6 times

  **Empel** 3 years, 2 months ago

If the official course had to cover everything it will be a 3 month course at least. There is just no time to cover everything in 4 days. I took the course as well but the instructor told us that it was not enough.

upvoted 4 times

  **Scoobysnaks86** 2 years, 10 months ago



Just pass the test and get familiar with things. If you get the job, and aren't sure what to do in certain circumstances, there's google and the ms site where you can learn and use in your job.

upvoted 6 times

  **klasbeatz** 2 years, 10 months ago

Agreed just watch the crash course videos and just pass the exam you'll learn the rest on the job. Just get the cert to get a job.

upvoted 3 times

  **JamesChan0620** 3 years, 8 months ago

The answer is correct?

upvoted 3 times

  **omw2wealth** 3 years, 7 months ago



Yes it is correct

upvoted 1 times

  **mkoprivnj** 3 years, 10 months ago



- Select Users & Groups : Where you have to choose all users.
- Select Cloud apps or actions: to specify the Azure portal
- Grant: to grant the MFA.

upvoted 3 times

  **mg** 4 years, 1 month ago

Answer is correct

upvoted 1 times

  **ZUMY** 4 years, 1 month ago

Given answer is correct

1.user or groups

2.apps

3.grant or deny

upvoted 3 times

  **taka_hawk** 4 years, 2 months ago

The Answer is correct .Please check. "<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps>" - "Cloud apps or actions" - "Microsoft Azure Management" - "Azure portal"

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: `Unable to invite user user1@outlook.com `` Generic authorization exception.`

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- A. From the Users settings blade, modify the External collaboration settings.
- B. From the Custom domain names blade, add a custom domain.
- C. From the Organizational relationships blade, add an identity provider.
- D. From the Roles and administrators blade, assign the Security administrator role to Admin1.

Correct Answer: A

Community vote distribution

A (100%)

- moekyisin**

Highly Voted

4 years, 5 months ago

correct answer checked in portal .
Go to Azure AD--users--user settings --scroll down.--External users
Manage external collaboration settings
upvoted 188 times
- Acai**

3 years, 9 months ago

Yep Yep Yep
upvoted 15 times
- Gorl12**

3 years, 7 months ago

Your excitement is awesome!
upvoted 27 times
- Mentalfloss**

9 months, 3 weeks ago

Your excitement about Acai's excitement is awesome! \m/
upvoted 4 times
- Ibra992**

2 months ago

Your excitement about Gorl12's excitement about Acai's excitement is contagious!
upvoted 2 times
- fedztedz**

Highly Voted

4 years, 4 months ago

Answer is correct. You can adjust the guest user settings, their access, who can invite them from "External collaboration settings"
check this link <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/delegate-invitations>
upvoted 78 times
- Iumax007**

Most Recent

1 month, 2 weeks ago

Selected Answer: A

From the Users settings blade, modify the External collaboration settings
upvoted 1 times
- RajeshwaranM**

4 months, 1 week ago

Selected Answer: A

Go to Azure AD--users--user settings --scroll down.--External users
Manage external collaboration settings
upvoted 1 times
- [Removed]**

8 months ago

Selected Answer: A

A is corerct
upvoted 1 times
- tashakori**

1 year, 1 month ago

D is right

upvoted 2 times

  **Amir1909** 1 year, 2 months ago

- From the Users blade, modify the External collaboration settings
A is correct

upvoted 1 times

  **azahar08** 1 year, 4 months ago

yes lo mismo piendo yo

upvoted 1 times

  **Navigati0n** 1 year, 9 months ago

A. From the Users settings blade, modify the External collaboration settings.

Explanation:

The error message indicates that there's an issue with the external collaboration settings in your Azure Active Directory. These settings dictate who can invite external users and under what circumstances.

To address this issue, you need to adjust the external collaboration settings to allow Admin1 to invite external partners. These settings can be found in the "Users settings" blade in Azure Active Directory.

upvoted 5 times

  **Madbo** 2 years ago

The reason why option A is the correct answer is that the error message "Generic authorization exception" indicates that the external collaboration settings in Azure AD might be preventing the invitation of guest users to the tenant. By default, Azure AD allows guest users to sign in to the tenant using their personal email addresses, but this can be modified by an administrator.

upvoted 3 times

  **Anamika1818** 2 years, 1 month ago

A is correct

upvoted 1 times

  **Mazinger** 2 years, 2 months ago

Selected Answer: A

To allow Admin1 to invite the external partner to sign in to the Azure AD tenant, you should do the following:

A. From the Users settings blade, modify the External collaboration settings.

To enable external collaboration and allow Admin1 to invite the external partner, you need to modify the External collaboration settings.

To do this, follow these steps:

Sign in to the Azure portal as a global administrator or user administrator.

Go to the Azure Active Directory blade.

Click on the "Users settings" option under the "Manage" section.


Under the "External collaboration" section, select the "Guest users permissions" option.

Choose "Allow invitations" for the "Guest users permissions" setting.

Save the changes.

After you modify the External collaboration settings, Admin1 should be able to invite the external partner to sign in to the Azure AD tenant without receiving the "Generic authorization exception" error message.

upvoted 5 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: A

A) "From the Users settings blade, modify the External collaboration settings."



upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

  **libran** 2 years, 8 months ago

Selected Answer: A

A is the right answer

upvoted 1 times

  **manalshowaei** 2 years, 10 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

  **epomatti** 3 years ago

Selected Answer: A

A is correct. External collaboration settings, there's where you configured the Guest permissions.

upvoted 1 times

You have an Azure subscription linked to an Azure Active Directory tenant. The tenant includes a user account named User1. You need to ensure that User1 can assign a policy to the tenant root management group. What should you do?


- A. Assign the Owner role for the Azure Subscription to User1, and then modify the default conditional access policies.
- B. Assign the Owner role for the Azure subscription to User1, and then instruct User1 to configure access management for Azure resources.
- C. Assign the Global administrator role to User1, and then instruct User1 to configure access management for Azure resources.
- D. Create a new management group and delegate User1 as the owner of the new management group.

Correct Answer: C

Community vote distribution

C (85%)

Other


-   **mlantonis**

Highly Voted 



 3 years, 11 months ago

Correct Answer: C


No one is given default access to the root management group. Azure AD Global Administrators are the only users that can elevate themselves to gain access. Once they have access to the root management group, the global administrators can assign any Azure role to other users to manage it.

upvoted 321 times
-   **JoeGuan** 1 year, 7 months ago



Why would you assume that USER1 needs to be the Global Administrator, or is a Global Administrator, rather than assuming that I am the Global Administrator? Assuming I am the Global Administrator, and that I have granted myself User Access Administrator, then using the least privileged best practice I would pick B and assign User1 any other role, like Owner, rather than Global Administrator. Granting everyone/anyone GA to assign policies seems like a horrible idea. The Owner role is enough to assign policy to the root management group. There is no need to assign User1 Global Administrator so that User1 can grant themselves the role.

upvoted 12 times
-   **Alscoran** 1 year, 5 months ago


It cannot be A or B simply because subscriptions are underneath Management groups. So doing any thing to those does not fix the issue. Cannot be D since that is creating a new management group. B is the only answer that comes close. Your concerns about assigning a GA noted but no other answer is provided that would alleviate your concerns.

upvoted 11 times
-   **Techo1980** 11 months, 2 weeks ago



@Alscoran, you say B is close or you mean C is close?

upvoted 2 times
-   **SunitaMaurya** 10 months, 1 week ago

Does anyone have contributor access then please help me.



upvoted 1 times
-   **itgg11** 3 years, 4 months ago


Answer is C. Just tested in the lab.

upvoted 24 times
-   **mumu_myk** 3 years, 4 months ago

mlantonis is correct - the answer here should be C. Assign the Global administrator...

Assigning the owner role to the "tenant root" (not the subscription) or the resource policy contributor role wouldve been enough access for user1 but that is not one of the options in the choices. so the only choice that works is C.


upvoted 10 times
-   **Rajash**

Highly Voted 


 4 years ago

Ans C:



No one is given default access to the root management group. Azure AD Global Administrators are the only users that can elevate themselves to gain access. Once they have access to the root management group, the global administrators can assign any Azure role to other users to manage it.



upvoted 64 times
-   **brainmind** 3 years, 10 months ago



The answer is C, the user should be a GA and then elevate themselves to gain access.



upvoted 3 times
-   **Negrinho** 4 years ago



No, the correctly answer is B.
C is to control Azure AD (Global Administrators), not to control Management group.
If you need to control Management group, use: Access control (IAM)> Add role assignment> Role> Owner or Contributor (in this case you will use Owner). Don't exist "Global Administrators" inside of Access control (IAM)> Add role assignment.
The link between Azure AD and Management group will allow that you choose an user of your Azure AD, but not will inherit Azure AD role.
upvoted 49 times



  **shnz03** 3 years, 11 months ago
I agree. Basically there are 3 RBAC methods. They are for
1) Azure AD
2) Azure resources including Management group
3) Classic (used by Subscription)
upvoted 1 times

  **RamanAgarwal** 3 years, 11 months ago
B cant be right because the owner access is given at subscription level only.
upvoted 5 times



  **mdyck** 3 years, 11 months ago
This is right. Check the chart in this link. Owners assign policy.
upvoted 5 times

  **rawrkadia** 3 years, 10 months ago
How can it be right when the question specifies the root management group and B specifies a child subscription? The only way to ensure they can make changes to the root management group is to make them a GA on the tenant and then they can assign themselves the owner permissions to that group.
upvoted 6 times

  **adanit2011** Most Recent 2 months, 3 weeks ago
Selected Answer: D
Is D the correct option.
The question is about applying a policy on the root management group. You cannot apply a policy on the root management group directly, so you need to create a new management group and assign user1 the "owner" role, because Entra ID roles do not apply to policies.
upvoted 1 times

  **happpieee** 6 months, 2 weeks ago
Selected Answer: C
Based on principle of least privileges, Owner access is sufficient to assign access policies, however point A mention using default conditional access that is wrong. Hence, the other possible answer will be Azure AD Global admin.



upvoted 1 times



  **Madbo** 7 months, 2 weeks ago
The reason Option C is the correct answer is that the Global administrator role grants the highest level of access to Azure AD, which includes the ability to manage all aspects of the directory, including access management for Azure resources and management of the root management group.

To assign a policy to the tenant root management group, the user needs to be able to access and manage the root management group in Azure AD. By assigning the Global administrator role to User1, they will have the necessary permissions to manage the root management group and assign policies to it.



Once User1 has the Global administrator role, they can navigate to the Azure portal and configure access management for Azure resources, including the root management group. From there, they can assign policies to the root management group and manage access to Azure resources.

In summary, assigning the Global administrator role to User1 is the most appropriate solution because it grants them the necessary permissions to manage the root management group and assign policies to it.
upvoted 2 times

  **[Removed]** 8 months ago
Selected Answer: C
it's C
upvoted 1 times

  **amurp35** 10 months, 1 week ago
Selected Answer: C
Out of the available options, only C will work since the root management group is higher than the subscription in the hierarchy, and the user must be either made an Owner of the management group (option not provided), or be able to make themselves an Owner on it.
upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago
ChatGPT4 says C
upvoted 3 times

  **3c5adce** 12 months ago
D. Create a new management group and delegate User1 as the owner of the new management group.
Assigning ownership of a new management group to User1 allows them to manage policies and access controls within that management group,

including assigning policies to the tenant root management group if necessary. This approach provides User1 with the necessary permissions to manage policies effectively while maintaining proper governance over Azure resources.



upvoted 1 times

  **Nushin** 1 year ago

To ensure that User1 can assign a policy to the tenant root management group, you should choose Option C: Assign the Global administrator role to User1, and then instruct User1 to configure access management for Azure resources.

The Global Administrator role in Azure Active Directory has permissions to all administrative features. This role is the most powerful role, and it can assign policies to the tenant root management group. The Owner role for the Azure subscription does not have this level of access. Therefore, options A and B would not meet the requirements. Option D is not relevant as it involves creating a new management group, which is not necessary in this case.

upvoted 1 times

  **MelKr** 1 year, 1 month ago

Selected Answer: C


Just verified this. Owner of the subscription is not enough to assign a policy at the root management group. The user needs to have at least the "Microsoft.Authorization/policyAssignments/write"-Permission and probably a couple more read permissions at the root management group. So given the options answer C fulfills this.

upvoted 2 times

  **tashakori** 1 year, 1 month ago

C is right



upvoted 2 times

  **Cg007** 1 year, 1 month ago

Selected Answer: B

By assigning the Owner role for the Azure subscription to User1, they will have the necessary permissions to manage resources within the subscription, including assigning policies to management groups. Then, instructing User1 to configure access management for Azure resources will allow them to assign policies to the tenant root management group.

upvoted 1 times

  **bacana** 1 year, 2 months ago

It depends. If the subscription is attached to a subgroup manager, the user cannot modify the root group's IAM. If a subscription is attached to the root, the user can modify IAM.

If the user is global, then he can gain access across all subscriptions using an "Elevate access" option.

I would go with option C because it doesn't say what level the subscription is at.

upvoted 1 times

  **Pringlesucka** 1 year, 2 months ago

Correct Answer: C

reasoning: becuase

upvoted 2 times

  **stanislaus450** 1 year, 2 months ago

Selected Answer: B

The correct answer is B. Assign the Owner role for the Azure subscription to User1, and then instruct User1 to configure access management for Azure resources¹².

To assign a policy to the tenant root management group, User1 needs to have the Microsoft.Authorization/roleAssignments/write permission, such as those provided by the Owner role¹². Once User1 has the Owner role, they can configure access management for Azure resources, including assigning policies to the tenant root management group¹².

upvoted 1 times

  **HdiaOwner** 1 year, 2 months ago

Selected Answer: C

Answer should be C

upvoted 2 times

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named adatum.com. Adatum.com contains the groups in the following table.

Name	Group type	Membership type	Membership rule
Group1	Security	Dynamic user	(user.city -startsWith "m"
Group2	Microsoft 365	Dynamic user	(user.department -notIn ["human resources"])
Group3	Microsoft 365	Assigned	Not applicable

You create two user accounts that are configured as shown in the following table.

Name	City	Department	Office 365 license assigned
User1	Montreal	Human resources	Yes
User2	Melbourne	Marketing	No

Of which groups are User1 and User2 members? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

User2:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

Answer Area

Correct Answer:

User1:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

User2:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

Box 1: Group 1 only -

First rule applies -

Box 2: Group1 and Group2 only -

Both membership rules apply.
Reference:
<https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/create-collections>

- pakman**

Highly Voted

3 years, 7 months ago

Correct answer.
User 1: Group 1 only
User 2: Group 1 & 2
upvoted 147 times
- SofiaLorean**

11 months, 3 weeks ago

please help to explain why user 1 not be in group 3? Thanks.
upvoted 4 times
- DevOpposite**

3 years, 7 months ago

why cant user 1 not be in grp 3 plz?
upvoted 12 times
- nsknexus478**

3 years, 7 months ago

Someone has to assign users to Group3 if they have to be part of it and there is no mention of manual assignment in the question.
upvoted 70 times
- DevOpposite**

3 years, 6 months ago

thank you
upvoted 3 times
- Mozbius_**

3 years, 3 months ago

Thank you for the clarification.
upvoted 1 times
- Chi1987**

3 years, 7 months ago

I dont agree, User 1 is Office licensed, he can not be in Gr1. and user 2 is not with office license
Correct answer
User1 Group 3
User2 Group 1
upvoted 5 times
- sk1803**

3 years, 7 months ago

license has nothing to do with it.
upvoted 28 times
- sk1803**

3 years, 7 months ago

<https://www.examttopics.com/discussions/microsoft/view/20714-exam-az-103-topic-3-question-11-discussion/>
upvoted 4 times
- BeastOfCloud**

2 years, 1 month ago

Correct aim we only focus on Membership not o365 license cause you just limit them.
upvoted 4 times
- GepeNova**

Highly Voted

3 years, 7 months ago

Tested in lab.
User 1: Group 1 only
User 2: Group 1 & 2
upvoted 54 times
- JL2000**

Most Recent

3 weeks, 1 day ago

Given answer is correct - Came up in Exam today

User 1: Group 1 only
User 2: Group 1 & 2
upvoted 1 times
- JPA210**

6 months ago

Both responses are group 1and 2; because user.department of user1 is "Human Resources' not "human resources " , the condition is case sensitive
upvoted 1 times
- Download100**

3 months, 2 weeks ago

Properties of type string
department Any string value or null user.department -eq "value"

Double quotes are optional unless the value is a string.
Regex and string operations aren't case sensitive.
Ensure that property names are correctly formatted as shown, as they're case sensitive.
When a string value contains double quotes, both quotes should be escaped using the ` character, for example, user.department -eq `"Sales`" is

the proper syntax when "Sales" is the value. Single quotes should be escaped by using two single quotes instead of one each time. You can also perform Null checks, using null as a value, for example, user.department -eq null.

upvoted 1 times

  **Download100** 3 months, 2 weeks ago


When specifying a value within an expression, it's important to use the correct syntax to avoid errors.
The user.department supported value is 'string'
Property names are case sensitive
Regex and string operations aren't case sensitive.
<https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership#supported-values>
upvoted 1 times

  **Download100** 3 months, 2 weeks ago

The user.department supported value is 'string'
<https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership#properties-of-type-string>
upvoted 1 times

  **Download100** 3 months, 2 weeks ago

Correct Answers:
User1: Group1 only
User2: Group1 and Group2 only
upvoted 2 times

  **learn254** 7 months ago

User 1 - Group 1
User 2 - Group 1

Users do not need a Microsoft 365 license to join a Microsoft security group. Security groups in Azure Active Directory (Azure AD) are primarily used to manage access to resources like applications, file shares, and other non-Microsoft 365 services.

Key Points:
Microsoft Security Groups: These are used to control access to various resources, including applications, virtual machines, or SharePoint sites. Membership in these groups does not require a Microsoft 365 license.

Microsoft 365 Groups: In contrast, Microsoft 365 groups (which are different from security groups) are tied to services like Exchange, SharePoint, Teams, and other Microsoft 365 services. To fully utilize the benefits of a Microsoft 365 group (like access to Teams or SharePoint), a Microsoft 365 license is typically required.
upvoted 3 times

  **usmanov** 8 months ago

Given answers are correct and straight forward, the only argument is that user2 does not have office 365 license which is fine because a user can be added to m365 group without license, they will just have no access to specific features like like planner, group's sharepoint
upvoted 1 times

  **[Removed]** 8 months ago



correct

only "dynamic user" Membership Type can add users automatically to it



User1 meets the requirements only of the rules in Group1
User2 meets the requirements of the rules in both Group1 & Group2
upvoted 3 times

  **Bobip** 8 months, 2 weeks ago

I don't think User2 can be member of Group2!
The department "Marketing" is not excluded by the rule, but User2 does not have an Office 365 license. Given that Group2 is a Microsoft 365 group, it would typically only include users who have such a license. Therefore, User2 should not be a member of Group2.
What do you think?!
upvoted 1 times

  **mojo86** 8 months, 4 weeks ago

A user must have a Microsoft 365 license assigned to them in order to be added to a Microsoft 365 group. The license is necessary for access to group features like email, SharePoint, and Teams. Without a license, the user won't be able to use the group's services.
upvoted 1 times

  **op22233** 1 year ago



Correct answer.
User 1: Group 1& 3
The Microsoft 365 assigned to him makes him a dynamic joined member of group 3
User 2: Group 1 & 2
upvoted 5 times



  **LovelyGroovey** 1 year ago



What is the meaning of 'Not applicable' under the Membership rule? Does it mean there is no rule? Or there is no membership?
upvoted 1 times

  **yeti21** 1 year ago



Groups with Assigned Membership don't have a Membership Rule. Because someone has to assign groups manually to the users.
upvoted 2 times



  **GlixRox** 11 months, 1 week ago
Was wondering this, thank you!
upvoted 1 times

  **tashakori** 1 year, 1 month ago
Given answer is correct
upvoted 1 times

  **SkyZeroZx** 1 year, 4 months ago
My opinion answer is

user 1 : Group 1 and 3
Group 3 because it have keyword "configured" in question and "Office 365 assigned" on table
User 2 : Group 1 and 2
upvoted 3 times



  **SgtDumitru** 1 year, 5 months ago
User1: Group1 only because Group3 does not auto-get this user and Group 2 block his department;
User2: Group 1 & Group 2. Group 3 does not auto-get this user.
upvoted 3 times



  **ggogel** 1 year, 5 months ago
This question is weird and misleading. You need to have enough Azure AD Premium P1 licenses for the dynamic group membership feature. While most Office 365 (now Microsoft 365) plans contain this license, just saying "Office 365" is too unspecific.



If we assume that User 1 has the Azure AD Premium P1 license and User 2 does not. Further, we assume that there are no other users in the tenant, who could have this license. Then User 1 would be a member of Group 1 and User 2 would be a member of no group. This is because User 2 would not be able to use the dynamically assigned membership due to a lack of licenses.

Additionally, both users COULD be a member of Group 3, but this is not specified in the question.

This question simply does not give all the required information to be able to answer this with 100% certainty.
upvoted 1 times

  **JWS80** 1 year, 9 months ago
The question is Of which groups are User1 and User2 members? I think both of these should be Group 1 only
upvoted 1 times

  **PMiao** 1 year, 11 months ago
If it's case-insensitive, then the answer is correct, otherwise the answer should be:
User 1: Group 2
User 2: Group 2
upvoted 1 times

  **azhoarder** 1 year, 8 months ago
Strings and regex are not case sensitive
<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#supported-values>
upvoted 1 times

HOTSPOT -

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

You need to modify the JobTitle and UsageLocation attributes for the users.

For which users can you modify the attributes from Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

JobTitle:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

UsageLocation:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Answer Area

Correct Answer:

JobTitle:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

UsageLocation:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Box 1: User1 and User3 only -

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory.

Box 2: User1, User2, and User3 -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal>


 **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

Box 1:User1 and User3 only
You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory.

Box 2: User1, User2, and User3
Usage location is an Azure property that can only be modified from Azure AD (for all users including Windows Server AD users synced via Azure AD Connect).

upvoted 340 times

 **Ivanvazovv** 1 month, 3 weeks ago

The answer is correct, but Usage Location can be automatically enumerated if you have Hybrid Exchange configuration and have the necessary on-premises attributes of the user account.

upvoted 1 times

  **LovelyGroovey** 1 year, 2 months ago

The correct answer for modifying the UsageLocation attribute from Azure AD is User1 only. Here's why:

User1:

User1 has their attributes sourced directly from Azure AD.

Therefore, their UsageLocation attribute can be modified in Azure AD.

User2:

User2's attributes are sourced from Windows Server Active Directory.

The UsageLocation attribute cannot be modified directly in Azure AD for User2.

User3:

User3's attributes are sourced from a Microsoft account.

The UsageLocation attribute cannot be modified directly in Azure AD for User3.

upvoted 5 times

  **TechThameem** 11 months, 1 week ago

Usage location can be modified for all users (Cloud only account and Onprem Directory synchronized account, Purpose of the UsageLocation attribute is License cost calculation, based on the country which we have selected, the billing amount has been calculated, I have done this usage location selection task 1000+ times in the user account onboarding process.

upvoted 4 times

  **Mozbius_** 3 years, 3 months ago

Thank you for the clarification. I am shocked to see how little I know. I swear after following Microsoft's course I feel like the goal wasn't really to prepare me for the exam at all.

upvoted 99 times

  **abhmalal** 3 years, 1 month ago

microsoft's course is shit

upvoted 86 times

  **NadirM_18** 3 years, 1 month ago

Same here. I know a lot less than I thought I knew apparently. On the positive side, rather find that out now, than when sitting for the exam.

upvoted 14 times

  **homersimpson** 2 years, 10 months ago

You make really good points. I spent 2 entire weekends going thru the MS course and stopped before the last module, I was exhausted. I'm learning a lot more by going thru these questions here.

upvoted 12 times

  **Asymptote** 2 years, 6 months ago

They are the genius know and good at what they are using, but definitely not good at teaching and misunderstood what is the difference between training and documentary.

upvoted 5 times

  **CommanderBigMac** 2 years, 2 months ago

Microsoft states you need x-amount of job experience before writing the exam to 'validate' your experience. Microsoft exams are not designed to give you a qualification in the traditional sense, but companies still expect is as such.

upvoted 9 times

  **zman_83** 2 years, 7 months ago

Damn your GOOD!, please keep up your work. The community need you for sure!!!)

upvoted 18 times

  **hakanbaba** Highly Voted  4 years, 5 months ago

I've checked on my AAD, answer is correct

upvoted 53 times

  **Somewhatbusy** 4 years, 4 months ago

Yes its correct. 100% agreed



upvoted 6 times

  **Kiano** 4 years ago

I have also checked but I can see that you can change both job title and usagelacation for all type of identities. even the ones that have been synchronized from on-prem AD.



Maybe this is an update since you published your comment, but anyways I think both answers should be User1, 2 and 3.



upvoted 7 times



  **Kiano** 3 years, 11 months ago

The answer is actually right. Although both usagelocation and jobtitle can directly be updated in Azure AD for all type of users, jobtitle can probably be overwritten by the synchronization process, although usagelocation is more an Azure AD type of attribute. But the question is tricky. it asks: "For which users can you modify the attributes from Azure AD? ". Both can b updated directly in Azure AD, although Jobtitle could be overwritten by the sync.




upvoted 9 times



  **Mozbius_** 3 years, 3 months ago
Thank you for the info.
upvoted 1 times



  **Shnash** 2 years, 5 months ago
It also depends on the settings on AD connect (Uni-direction or Bi-Direction) The Job Title Field is disabled (Grayed Out) for the accounts synced through AD Connect from Windows AD Service if AD Connect is configured to sync data from On-Premises AD to Azure AD only then we can't edit it. but for the same account usage location is editable. (Tested in Production Environment).
upvoted 1 times



  **chandiochan** Most Recent 2 months, 2 weeks ago
JobTitle: User1 and User3 only
UsageLocation: User1 and User3 only

User1 and User3 are fully managed in Azure AD, so their attributes can be changed directly.
User2 is synchronized from on-premises Active Directory, so the attributes must be modified on-premises and synced to Azure AD.



1. User1 (Cloud-Only in Entra ID) 
JobTitle: Can be modified directly in Entra ID via GUI or Microsoft Graph API.
UsageLocation: Can also be modified in Entra ID.
Why? User1 is a native Entra ID user with no dependency on an on-premises directory.
2. User2 (On-Prem AD Sync via Entra Connect) 
JobTitle: Cannot be modified in Entra ID because it is synced from on-prem Active Directory.
UsageLocation: Cannot be modified in Entra ID for the same reason.
Why? On-prem users are read-only in Entra ID. Changes must be made on-premises in Active Directory and synced via Entra Connect.
3. User3 (Guest from Microsoft Account) 
JobTitle: Can be modified directly in Entra ID.
UsageLocation: Can be modified directly in Entra ID.
Why? Guest users exist in Entra ID as separate objects and can have certain attributes modified, unlike on-prem synced users.
upvoted 1 times



  **[Removed]** 8 months ago
correct
upvoted 3 times



  **mojo86** 8 months, 4 weeks ago
For users whose source of authority is Windows Server Active Directory, you must use Windows Server Active Directory to update their identity, contact info, or job info. After making updates, you must wait for the next synchronization cycle to complete before the changes take effect. However, you can update their attributes directly in the Microsoft Entra admin center if you are updating Microsoft Entra ID attributes, such as Usage Location.
upvoted 2 times



  **LovelyGroovey** 1 year, 2 months ago
This is why I hate AZ-104 questions. Microsoft needs to audit these answers.



The correct answers are User1 only for both JobTitle and UsageLocation. For example, The correct answer for modifying the JobTitle attribute from Azure AD is User1 only. This is because User2 and User3 have their attributes sourced from different places: User2 from Windows Server Active Directory and User3 from a Microsoft account. Only User1's attributes can be directly modified in Azure AD. Therefore, the answer is not User1 and User3 only; it is User1 only.
upvoted 5 times

  **LovelyGroovey** 1 year, 2 months ago
Box 2's answer is User2 only. User1 and User3 are guests and cannot modify their UsageLocation attribute from Azure AD. Only User2 is a member with on-premises sync enabled, which allows them to change their UsageLocation attribute from Azure AD. the reference you provided is not correct for this scenario. The reference above explains how to modify the UsageLocation attribute for a user from the Azure portal, but it does not mention anything about the UserType or the On-premises sync status of the user. These factors affect whether you can modify the attribute from Azure AD or not.
upvoted 1 times

  **Amir1909** 1 year, 2 months ago
Correct
upvoted 1 times

  **Babustest** 1 year, 7 months ago
I spent two months in on-line courses including Microsoft Az-104 training. Most of the questions I see here are not at all covered in those trainings.
upvoted 4 times

  **Dankho** 6 months, 2 weeks ago
Welcome to Microsoft testing, courses are just one small piece of the learning experience.
upvoted 1 times

  **Mehedi007** 1 year, 9 months ago
User1 and User3 only
User1, User2, and User3

"You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory. After you complete your update, you must wait for the next synchronization cycle to complete before you'll see the

changes."

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-manage-user-profile-info#profile-categories>

upvoted 2 times

  **bsaksham** 2 years, 1 month ago

I dont know why you guys are vouching for User1 and User3 only, question is asking for

For which users can you modify the attributes from Azure AD?

and the reason they are giving You must use Windows Server Active Directory, this is not what the question is asking..

i will go with User 1 only

upvoted 5 times

  **bsaksham** 2 years, 1 month ago

Sorry my bad, answers are correct from ET

upvoted 3 times

  **Nitestorm** 2 years, 1 month ago

I got a modified form of this question on the March 2023 exam, specifically instead of indicating the "source" in the last column, the chart simply specified that User 2 was synced to on-premises and User 1 and 3 were not.

upvoted 3 times

  **cankayahmet** 2 years, 1 month ago

so what was the answer?

upvoted 1 times

  **Vivek88** 2 years, 2 months ago

On-premises: Accounts synced from Windows Server Active Directory include other values not applicable to Azure AD accounts.

Note

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory. After you complete your update, you must wait for the next synchronization cycle to complete before you'll see the changes.

upvoted 1 times

  **gauravit43** 2 years, 3 months ago

Correct Answer. Tested in Lab

Box 1: User1 and User3

Box 3 : User1,User2 and User3



upvoted 5 times

  **NaoVaz** 2 years, 7 months ago

JobTitle = User1 and User3 only

UsageLocation = User1, User2 and User3

upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Correct Answer:

Box 1:User1 and User3 only

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory.

Box 2: User1, User2, and User3

Usage location is an Azure property that can only be modified from Azure AD (for all users including Windows Server AD users synced via Azure AD Connect).

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal>

upvoted 3 times

  **RougePotatoe** 2 years, 3 months ago

Why on earth are you copy and pasting someone else's opinion?

upvoted 5 times

  **HorseradishWalrus** 2 years, 8 months ago

WHY on earth should I know this to pass this exam? This detail is soo unimportant. Whether you know it or not does not tell anything about your qualification. Yet too many questions are like this...

upvoted 9 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Network Contributor role at the subscription level to Admin1.



Does this meet the goal?


- A. Yes
- B. No

Correct Answer: A

Community vote distribution

A (56%)B (44%)

-   **mlantonis**

Highly Voted 

 3 years, 11 months ago

Correct Answer: A - Yes

Your account must have any one of the following Azure roles at the subscription scope: Owner, Contributor, Reader, or Network Contributor. Network Contributor role - Lets you manage networks, but not access to them.

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.



Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>



<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements>



<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 140 times
-   **twambala** 3 years, 8 months ago



how can yu

upvoted 6 times
-   **twambala** 3 years, 8 months ago



how can one manage something if he does not have access to it


upvoted 2 times
-   **rsharma007** 3 years, 7 months ago

they are two different permissions- a NC role can manage the resources, but he/she can't grant access to those resources to anyone else. That can be done by roles with 'access' permissions such as 'owner'

upvoted 7 times
-   **Mozbius_** 3 years, 3 months ago



Thank you for clarifying! Much appreciated.


upvoted 1 times
-   **RithuNethra**

Highly Voted 

 4 years, 5 months ago

correct answer

upvoted 22 times
-   **tars1212**



Most Recent 

 1 month ago

Selected Answer: B

To enable Traffic Analytics, Admin1 needs permissions to manage Network Watcher and Log Analytics, which are required for Traffic Analytics.

The Network Contributor role grants permissions to manage network resources (e.g., virtual networks, load balancers, network security groups) but does not provide access to Log Analytics workspaces, which are necessary for Traffic Analytics.

upvoted 1 times
-   **lumax007** 2 months ago

Selected Answer: A

To use Traffic analytics, you must assign one of the following Azure built-in roles to your account:

Deployment model Role
Resource Manager Owner
Contributor

Network contributor 1 and Monitoring contributor

1 Network contributor doesn't cover Microsoft.Operationallnsights/workspaces/* actions.

If none of the preceding built-in roles are assigned to your account, assign a custom role that supports the actions listed in Flow logs and Traffic analytics permissions.

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics?tabs=Americas>


upvoted 1 times

  **BUDSENA** 2 months ago

Selected Answer: B

You need monitor contributor and network contributor.

upvoted 2 times

  **Jakub4444** 3 months ago

Selected Answer: B

No, this does not meet the goal.


The Network Contributor role allows managing network resources (such as virtual networks, network interfaces, and network security groups), but it does not provide the required permissions to enable Traffic Analytics.

To enable Traffic Analytics, the user must have the Reader or Contributor role at the subscription level to access traffic data and must also have the Log Analytics Contributor role on the Log Analytics workspace where the traffic analytics data is stored.

Correct Solution:

Assign the Log Analytics Contributor role to Admin1 on the Log Analytics workspace used for Traffic Analytics.

upvoted 3 times

  **Bambi0074** 3 months, 3 weeks ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics?tabs=Americas#prerequisites>

Tested in Lab, you need "Network contributor" and "Monitoring contributor"

upvoted 3 times

  **ozansenturk** 3 months, 3 weeks ago

Selected Answer: B

Network contributor and Monitoring contributor

* Network contributor doesn't cover Microsoft.Operationallnsights/workspaces/* actions.

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics?tabs=Americas#prerequisites>

upvoted 3 times

  **ozansenturk** 3 months, 3 weeks ago

rectify my answer: just to enable the built in role network contributor will be sufficient. the answer is A

upvoted 1 times

  **58b2872** 4 months, 1 week ago

Selected Answer: A

assigning the Network Contributor role to the user at the appropriate level (e.g., subscription or resource group) will provide sufficient permissions to enable and configure Traffic Analytics.

upvoted 1 times

  **RajeshwaranM** 4 months, 1 week ago

Selected Answer: B

Answer from ChatGPT :

Why "Network Contributor" is Insufficient?

While the Network Contributor role allows managing NSGs, it does not include permissions to enable diagnostics or configure Log Analytics settings.

By assigning the Contributor role or combining the above permissions in a custom role, you can accomplish this task. Let me know if you need further clarification or examples!

upvoted 1 times

  **Miniappa** 4 months, 2 weeks ago

Selected Answer: A



A is correct as per recent Microsoft documentation <https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites>

upvoted 1 times

  **srini77923** 4 months, 1 week ago

it should have both network and monitoring contributor role so the answers is B

upvoted 1 times

  **RVivek** 5 months, 4 weeks ago

Selected Answer: B

Monitoring contributor role is also required, along with Network Contributor
<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites>
<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#key-components>
upvoted 2 times

  **dirkxi** 7 months ago

Network Watcher can be applied in various scenarios to ensure network integrity and performance: Enabling Traffic Analytics: Assigning roles such as Owner, Contributor, or Network Contributor at the subscription level to enable traffic analytics. A is indeed correct!
upvoted 1 times

  **Exilic** 7 months, 2 weeks ago

Selected Answer: A

ChatGPT

B. No

Assigning the Network Contributor role to Admin1 at the subscription level does not meet the goal of enabling Traffic Analytics for the Azure subscription. The Network Contributor role provides permissions to manage network resources, such as virtual networks and network interfaces, but it does not grant the necessary permissions to enable Traffic Analytics.

To enable Traffic Analytics for an Azure subscription, you need to assign the Log Analytics Contributor or the Network Watcher Contributor role to Admin1 at the subscription level. These roles provide the necessary permissions to configure and enable Traffic Analytics.
upvoted 5 times

  **blackwhites** 7 months, 2 weeks ago

Answer A

es, this meets the goal. The Network Contributor role at the subscription level allows users to manage network resources, including enabling Traffic Analytics.

Here are the steps on how to assign the Network Contributor role to Admin1:

Go to the Azure portal.
In the left navigation pane, select Roles and subscriptions.
In the Subscriptions tab, select the subscription that you want to assign the role to.
In the Roles tab, select Add role assignment.
In the Select a role dialog box, select Network Contributor.
In the Select users or groups dialog box, enter the name of the user or group that you want to assign the role to.
Select the Select button.
In the Review + assign dialog box, review the role assignment, and then select the Assign button.

Once you have assigned the Network Contributor role to Admin1, they will be able to enable Traffic Analytics for the Azure subscription.
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: A

A is correct

upvoted 1 times

  **[Removed]** 7 months, 3 weeks ago

Owner & Network Contributor can enable Traffic Analytics
upvoted 1 times

  **Matsane** 1 year ago

A is the correct answer
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Owner role at the subscription level to Admin1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Community vote distribution

A (81%)B (19%)

- mlantonis

Highly Voted

3 years, 11 months ago

Correct Answer: A

Your account must have any one of the following Azure roles at the subscription scope: Owner, Contributor, Reader, or Network Contributor. Network Contributor role - Lets you manage networks, but not access to them.

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 73 times
- Rockysekhon

1 year, 5 months ago

mlantonis i read the question to enable not to view only etc.

upvoted 1 times
- RithuNethra

Highly Voted

4 years, 5 months ago

correct answer

upvoted 13 times
- nnamacha

Most Recent

1 month, 3 weeks ago

Selected Answer: B

The owner can enable but is it the "required" role if we take into account least privilege principle

upvoted 1 times
- RMS1223

4 months ago

Selected Answer: A

Respuesta Correcta

upvoted 1 times
- [Removed]

7 months, 3 weeks ago

Selected Answer: A

A is correct

Owner & Network Contributor can enable Traffic Analytics


upvoted 2 times
- [Removed]

8 months ago


Selected Answer: A

A is correct


upvoted 1 times

-  **3c5adce** 12 months ago

Answer B - The key word that indicates that the answer B is correct is "enable." The goal is to ensure that an Azure AD user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription. This implies that the user needs permissions to configure or activate Traffic Analytics, not just view or read its data. Therefore, simply assigning the Reader role, which provides read-only access, does not fulfill the requirement to enable Traffic Analytics.

upvoted 2 times
-  **tashakori** 1 year, 1 month ago


Yes is right

upvoted 1 times
-  **kond** 1 year, 2 months ago


Copilot: No, assigning the Owner role to Admin1 does not meet the goal of enabling Traffic Analytics for an Azure subscription. The Owner role provides full control over the entire subscription, including resources and access management. However, it is not specific to enabling or configuring Traffic Analytics.

To achieve the goal, you should assign a role that specifically grants permissions related to Traffic Analytics, such as the Log Analytics Contributor role. This role allows users to manage and configure Log Analytics workspaces, which includes enabling features like Traffic Analytics.

Therefore, consider assigning the Log Analytics Contributor role to Admin1 to meet the goal effectively.


upvoted 1 times
-  **ELearn** 9 months, 3 weeks ago

Copilot now: Yes, assigning the Owner role at the subscription level to Admin1 does meet the goal. The Owner role has full access to all resources including the right to delegate access to others. This means they can enable and configure Traffic Analytics for the subscription.

upvoted 2 times
-  **learnboy123** 1 year, 4 months ago

Selected Answer: B


<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

upvoted 1 times
-  **EwoutBI** 1 year, 3 months ago

Doesn't that link confirm answer A?


One of the following Azure built-in roles needs to be assigned to your account:

Owner


upvoted 1 times
-  **Mehedi007** 1 year, 9 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites>
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>


upvoted 2 times
-  **Mehedi007** 1 year, 9 months ago

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner>

upvoted 1 times
-  **[Removed]** 1 year, 10 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>
Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.


upvoted 3 times
-  **Athul07** 1 year, 11 months ago

A. Yes


Assigning the Owner role at the subscription level to Admin1 meets the goal of enabling Traffic Analytics for an Azure subscription.

The Owner role has full access to all resources within the subscription, including the ability to enable Traffic Analytics. By assigning the Owner role to Admin1 at the subscription level, Admin1 will have the necessary permissions and control to enable and configure Traffic Analytics for the Azure subscription.

Therefore, the provided solution meets the goal.

upvoted 2 times
-  **habbey** 2 years ago

Yes. A is correct. Owner have full access to resources.


upvoted 1 times
-  **kklohit** 2 years, 2 months ago

Selected Answer: B

No, assigning the Network Contributor role at the subscription level to Admin1 does not meet the goal of enabling Traffic Analytics. The Network Contributor role provides the ability to manage network resources, but it does not include the necessary permissions to configure Traffic Analytics. To enable Traffic Analytics, Admin1 needs to be assigned the Network Contributor role on the resource group where the virtual network that is

being monitored by Traffic Analytics is located, and also needs to have read permissions to the storage account where the Traffic Analytics data is stored.

upvoted 3 times

  **Durden871** 2 years, 1 month ago

Great answer, but you voted on the wrong question.
Solution: You assign the Owner role at the subscription level to Admin1.
upvoted 1 times

  **ignorica** 1 year, 6 months ago

still even for the former question if you look in the docs:
<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>
network contributor at subscription level is still OK (it does require adding this as extra/custom: 1 Network contributor doesn't cover Microsoft.Operationallnsights/workspaces/* actions.)
upvoted 1 times

  **KennethLZK** 2 years, 4 months ago

Selected Answer: A

Correct
upvoted 2 times

  **MayurSingh** 2 years, 4 months ago

Selected Answer: A

A is 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. You need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Reader role at the subscription level to Admin1.

Does this meet the goal?



- A. Yes
- B. No


Correct Answer: B

Community vote distribution

B (81%)

A (19%)

-   **asmodeus**



Highly Voted 

 4 years, 5 months ago



Traffic Analytics requires the following prerequisites:

A Network Watcher enabled subscription.
Network Security Group (NSG) flow logs enabled for the NSGs you want to monitor.
An Azure Storage account, to store raw flow logs.
An Azure Log Analytics workspace, with read and write access.
Your account must meet one of the following to enable traffic analytics:



Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

upvoted 101 times
-   **knowakuk** 4 months, 3 weeks ago



<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements>

upvoted 1 times
-   **visave** 4 years, 5 months ago



As per your description the answer is A. could you please paste the source of the information.

upvoted 2 times
-   **visave** 4 years, 5 months ago

got it.
<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq#:~:text=Your%20account%20must%20meet%20one,%2C%20reader%2C%20or%20network%20contributor.>

upvoted 7 times
-   **MountainW** 4 years, 1 month ago

The key is to enable, not to use. The article is about to use. The answer is not correct.



upvoted 12 times
-   **JayBee65** 3 years, 11 months ago

The requirements above state..

Your account must meet one of the following to ***enable**** traffic analytics:



Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, ***reader***, or network contributor.

So it is correct

upvoted 10 times
-   **Testyboy15** 2 years, 10 months ago

Article must have been amended as the word enable does not appear any longer. Under Prerequisites it says "Before you use traffic analytics...."

So answer is and always has been NO

upvoted 3 times
-   **Chang401** 2 years, 7 months ago

agree we can enable TA. use the below link for answer.
<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq#what-are-the-prerequisites-to-use-traffic-analytics->

upvoted 3 times

  **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer: A - Yes

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor. Reader role - View all resources, but does not allow you to make any changes. Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>



upvoted 98 times

  **hercu** 3 years, 10 months ago

I think the answer is correct as it's assumed that the prerequisites to use traffic analytics are already met. Referring to:
<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq#what-are-the-prerequisites-to-use-traffic-analytics->

As a result, as stated just few lines below, all following roles: Owner, Contributor, Reader, or Network Contributor are sufficient to enable Traffic Analytics.

upvoted 3 times

  **xupiter** 3 years, 10 months ago

"Reader role - View all resources, but does not allow you to make any changes."

So that means this role doesn't allow you to enable traffic analytics.
So it cannot be "Yes".

upvoted 23 times

  **Mozbius_** 3 years, 3 months ago

Yet it is "Yes". You can blame Microsoft for the confusion.
<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>
upvoted 8 times

  **GoldenDisciple2** 1 year, 8 months ago

According to Microsoft, the sky is up, but the answer is down. To Microsoft, the ocean is wet but the answer is dry, the desert is dry but on the exam you must select wet or you'll get it wrong...

According to Microsoft, the air in space is breathable... Let me explain. The earth has breathable air and the earth is in space, therefor, the air in space is breathable...

upvoted 10 times

  **shahidsayyed** 1 year, 6 months ago

You should try standup comedy as an alternative career. Got into wrong profession.
upvoted 5 times

  **ozansenturk** Most Recent 3 months, 3 weeks ago

Selected Answer: B

To use Traffic analytics, you must assign one of the following Azure built-in roles to your account:

Deployment model Role
Resource Manager Owner
Contributor
Network contributor 1 and Monitoring contributor
1 Network contributor doesn't cover Microsoft.Operationallnsights/workspaces/* actions.

If none of the preceding built-in roles are assigned to your account, assign a custom role that supports the actions listed in Flow logs and Traffic analytics permissions.

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics?tabs=Americas#prerequisites>

upvoted 2 times

  **danlo** 4 months, 3 weeks ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites>

upvoted 2 times

  **JeremyChainsaw** 7 months, 2 weeks ago

Per MS: Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, or network contributor.

Here's the confusion: a custom role can have reader roles to enable it.
If your account isn't assigned to one of the previously listed roles, it must be assigned to a custom role that is assigned the following actions, at the subscription level.



Microsoft.Network/applicationGateways/read
Microsoft.Network/connections/read
Microsoft.Network/loadBalancers/read
Microsoft.Network/localNetworkGateways/read
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/publicIPAddresses/read
Microsoft.Network/routeTables/read
Microsoft.Network/virtualNetworkGateways/read
Microsoft.Network/virtualNetworks/read

So, if the question were talking about custom roles, then perhaps it'd be A yes, but as it is regarding to built-in roles, this is NO.

Source:
<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>
upvoted 4 times

  **[Removed]** 8 months ago

Selected Answer: B
im going with B
upvoted 1 times

  **mojo86** 8 months, 4 weeks ago

Subscription Reader Role:
Permissions: The Subscription Reader role has read-only access to the Azure resources within a subscription.
Capability: It allows users to view resources, settings, and data but does not grant permissions to make any changes, including enabling or configuring features like Traffic Analytics.
To enable Traffic Analytics, you would need a role with write permissions on the relevant network resources, such as Owner, Contributor, Network Contributor, or a custom role with the necessary permissions.
upvoted 3 times

  **Matsane** 10 months ago

No, assigning the Reader role to Admin1 does not meet the goal.

The Reader role only provides read-only access to resources and does not grant the necessary permissions to enable Traffic Analytics.


To enable Traffic Analytics, Admin1 requires the Network Contributor role or a higher role like the Contributor or Owner role, which grants the necessary permissions to configure and manage network resources, including Traffic Analytics.

You should assign the Network Contributor role (or a higher role) at the subscription level to Admin1 to meet the goal.
upvoted 3 times

  **amurp35** 10 months, 1 week ago

Selected Answer: B
Reader role is not enough:

One of the following Azure built-in roles needs to be assigned to your account:
Deployment model Role
Resource Manager Owner
Contributor
Network contributor 1 and Monitoring contributor 2
upvoted 5 times

  **3ba6d0b** 10 months, 3 weeks ago

Selected Answer: B
Assigning the Reader role at the subscription level to Admin1 does not meet the goal. The Reader role provides read-only access to Azure resources, which allows viewing information but not configuring or enabling features like Traffic Analytics. To enable Traffic Analytics, Admin1 would need more permissions, typically provided by roles such as Network Contributor or Contributor. These roles allow configuring network resources and settings necessary to enable Traffic Analytics.
upvoted 4 times

  **frvr** 11 months ago

Selected Answer: B
<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites~:text=Deployment%20model-,Role,-Resource%20Manager>
upvoted 2 times



  **SofiaLorean** 11 months, 1 week ago

Selected Answer: B
B. No

Assigning the Reader role at the subscription level to Admin1 does not meet the goal of enabling Traffic Analytics for an Azure subscription. The Reader role has permissions to view resources but does not allow for any write operations, which are required to enable Traffic Analytics. To enable



Traffic Analytics, Admin1 would need to be assigned a role that has write permissions, such as the Owner, Contributor, or a custom role with specific permissions for Traffic Analytics

upvoted 4 times

  **3c5adce** 11 months, 4 weeks ago

No. Access but not enable.



upvoted 1 times

  **SinopsysHK** 12 months ago

Hello, seems that there was a typo in Azure documentation and Reader (read only, cannot make any change) cannot enable Traffic Analytics: cf <https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites> "One of the following Azure built-in roles needs to be assigned to your account: Owner, Contributor, Network contributor,and Monitoring contributor"



Hence answer is B.

upvoted 2 times

  **3c5adce** 12 months ago

NO - to enable Traffic Analytics for an Azure subscription, Admin1 should be assigned the Network Watcher Contributor or Owner, Contributor, User Access Administrator, Security Administrator

upvoted 1 times

  **pverma20** 1 year ago

Correct Answer - No (Confirmed, check below documentation) If you enable Traffic Analytics for sure, it require some write access to capture and write the logs. We need to be Logical.

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

Prerequisites

Traffic analytics requires the following prerequisites:

A Network Watcher enabled subscription. For more information, see Enable or disable Azure Network Watcher.

NSG flow logs enabled for the network security groups you want to monitor or VNet flow logs enabled for the virtual network you want to monitor.

For more information, see Create a flow log or Enable VNet flow logs.

An Azure Log Analytics workspace with read and write access. For more information, see Create a Log Analytics workspace.

One of the following Azure built-in roles needs to be assigned to your account:

Expand table

Deployment model

Role



Resource Manager

Owner

Contributor

Network contributor 1 and Monitoring contributor 2

upvoted 2 times

  **Annie_5** 1 year ago

Selected Answer: B

It seems reader role cannot enable traffic analytics. It can view it.

upvoted 4 times



You have an Azure subscription that contains a user named User1.
You need to ensure that User1 can deploy virtual machines and manage virtual networks. The solution must use the principle of least privilege.
Which role-based access control (RBAC) role should you assign to User1?


- A. Owner
- B. Virtual Machine Contributor
- C. Contributor
- D. Virtual Machine Administrator Login

Correct Answer: C



Community vote distribution



C (92%)8%



-   **wooyourdaddy**



Highly Voted 



 4 years, 5 months ago



Should the answer be C. Contributor? Answer B, only allows the managing of the VM's and not the Virtual Networks as stated in the question.
upvoted 240 times
-   **brakonda** 3 years, 7 months ago



Admin given answer in description is B but if yo read description carefully it says B can only manage VM and not the network
upvoted 6 times
-   **alessioferrario** 4 years, 2 months ago



I agree
upvoted 1 times
-   **Miles19** 4 years, 1 month ago



You are right, definitely, we need to assign a role of contributor, as the virtual machine contributor isn't enough - can't even manage the virtual networks to which the VM is attached to. See details: <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>
upvoted 2 times
-   **ciscogeek** 4 years, 1 month ago



Whatever Manage means by Microsoft standards, as per the doc they say, VM Contributor can manage.
Virtual Machine Contributor Lets you "manage" virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
I would go for B.
upvoted 3 times
-   **Gadzee** 3 years, 3 months ago


I would go for B taking into account that they say "least privilege"
upvoted 5 times
-   **Broniac** 3 years, 1 month ago

yes but, with B you can only achieve to manage VMs not Vnets which is also mentioned.
upvoted 10 times
-   **Deputy7** 3 years, 2 months ago

Bro, It is User1 can deploy virtual machines and manage virtual networks. So, Definitely C.
upvoted 2 times
-   **brico** 3 years, 10 months ago

Can't be B. As you mentioned in your response, "and not the virtual network...". C is the correct answer.
upvoted 8 times
-   **Hari2017** 3 years, 2 months ago

Answer is C because though the question says least privilege it should meet both the conditions of managing VMs & VNets.
upvoted 7 times
-   **mlantonis**

Highly Voted 

 3 years, 11 months ago

Correct Answer: C

Only Owner and Contributor can perform the actions, but we need to follow the least privilege principal, so Contributor.
A: Owner- Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
B: Virtual Machine Contributor - Create and manage virtual machines, manage disks and disk snapshots, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you to assign roles in

Azure RBAC.
C: Contributor - Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.
D: Virtual Machine Administrator Login - View Virtual Machines in the portal and login as administrator.

Reference:
<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>
upvoted 151 times

  **faseeh** Most Recent 1 month ago

Selected Answer: C

You want User1 to:

Deploy virtual machines

Manage virtual networks

But only give the minimum required permissions (least privilege)

☒ Contributor Role
Allows creating and managing all types of Azure resources, including virtual machines and virtual networks

Does NOT allow managing access (i.e., assigning roles)

Fits the principle of least privilege for the tasks mentioned

☒ Why the other options are incorrect:
A. Owner

Too much access – includes full permissions plus the ability to manage RBAC (assign roles), which violates least privilege

B. Virtual Machine Contributor



Only allows management of virtual machines

Does not grant permissions for virtual networks, so this doesn't meet the requirement

D. Virtual Machine Administrator Login

Only allows login to virtual machines with administrative privileges

Does not allow deploying or managing VMs or networks
upvoted 1 times

  **Odc4dd8** 3 months, 2 weeks ago

Selected Answer: B

Virtual Machine Contributor (Option B):

Permissions:


Create and manage virtual machines.

Manage virtual networks (e.g., create, update, delete virtual networks and subnets).

Manage network interfaces and disks.

Limitations:

Does not allow User1 to manage other Azure resources (e.g., storage accounts, databases).
upvoted 1 times

  **JustinYoo** 4 months, 3 weeks ago

Selected Answer: C

Virtual Machine Contributor: This role only allows the user to manage VMs but not virtual networks, so it would not provide the ability to manage virtual networks.
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: C

C is corerct
upvoted 2 times

  **brandon4sam** 1 year, 2 months ago

Question is tricky, but it states "Least privilege" So answer C is correct
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

C is correct

upvoted 1 times

  **stanislaus450** 1 year, 2 months ago

The correct answer is B. Virtual Machine Contributor¹.

The Virtual Machine Contributor role allows a user to create and manage virtual machines, manage disks, install and run software, reset the password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions¹. However, this role does not grant management access to the virtual network or storage account the virtual machines are connected to¹.

For managing virtual networks, User1 would also need the Network Contributor role¹. This role lets you manage all networking resources, but not access to them¹.

upvoted 1 times

  **stanislaus450** 1 year, 2 months ago

Please note that the Owner role (option A) grants full access to manage all resources, including the ability to assign roles in Azure RBAC¹, which might be more than what's needed if you're following the principle of least privilege. The Contributor role (option C) grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC¹, which might also be more than what's needed. The Virtual Machine Administrator Login role (option D) allows you to view virtual machines in the portal and login as administrator¹, but it does not allow you to deploy virtual machines or manage virtual networks

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

Selected Answer: C

Contributor

upvoted 1 times

  **TSKARAN** 1 year, 5 months ago

Selected Answer: C

Virtual Machine Contributor > B: Wrong Answer.

Create and manage virtual machines, manage disks, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you to assign roles in Azure RBAC.

Correct answer > C. Contributor

upvoted 2 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: C

'Contributor': because both vm and vnet need to be managed.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#contributor>

upvoted 2 times



  **[Removed]** 1 year, 10 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries

upvoted 1 times

  **Athul07** 1 year, 11 months ago

C. Contributor

To ensure that User1 can deploy virtual machines and manage virtual networks with the principle of least privilege, you should assign the Contributor role to User1.



The Contributor role provides permissions to create and manage Azure resources but does not grant excessive privileges like the Owner role. By assigning the Contributor role, User1 will have the necessary permissions to deploy virtual machines and manage virtual networks without having unrestricted access to other resources or the subscription management.

The Virtual Machine Contributor role is more limited and focuses specifically on managing virtual machines. It does not include permissions to manage virtual networks, so it is not the most appropriate choice for this scenario.

The Virtual Machine Administrator Login role is specific to Windows Virtual Desktop and grants permissions to manage the administrative accounts for virtual machines in a virtual desktop infrastructure.

Therefore, the best option in this scenario is to assign the Contributor role to User1.

upvoted 1 times

  **emptyH** 1 year, 11 months ago

Keyword here is & Networks. Only the contributor role can manage the VM's and the Networks.

upvoted 2 times

  **hz78** 2 years ago

B. Virtual Machine Contributor.

To meet the requirement of allowing User1 to deploy virtual machines and manage virtual networks with the principle of least privilege, the Virtual Machine Contributor role should be assigned to User1. This role allows User1 to manage virtual machines, but only those virtual machines for

which they have been granted access. Additionally, this role provides permissions to manage the virtual network resources required to support the virtual machines.

Assigning the Owner or Contributor role to User1 would provide more permissions than necessary, and therefore, does not follow the principle of least privilege. The Virtual Machine Administrator Login role does not provide the necessary permissions to deploy virtual machines or manage virtual networks.

upvoted 2 times

  **Kishore_Ahmed** 2 years, 3 months ago

Answer is C. Because having user1 has role of "VirtualMachineContributor", User1 can Create and manage virtual machines, manage disks, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. But we cannot create VM as this role as dosen't having write access to

Microsoft.Network/virtualNetworks

Microsoft.Network/publicIPAddresses

Microsoft.Network/networkSecurityGroups

which stops VM creation.

upvoted 1 times

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains three global administrators named Admin1, Admin2, and Admin3. The tenant is associated to an Azure subscription. Access control for the subscription is configured as shown in the Access control exhibit. (Click the Access Control tab.)

+

Add

≡

Edit columns

↺

Refresh

🗑

Remove

♥

Got feedback?

Check access

Role assignments

Deny assignments

Classic administrators

Roles

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name ⓘ

Type ⓘ

All

Scope ⓘ

All scopes

Group by ⓘ

Role


Role ⓘ

Owner

☒ Select all

☒ Owner

1 items (1 Users)

<input type="checkbox"/>	NAME	TYPE	ROLE	SCOPE
	OWNER			
	<div>Admin3</div> <div>Admin3@Cont...</div>	User	<div>Owner ⓘ</div>	This resource

You sign in to the Azure portal as Admin1 and configure the tenant as shown in the Tenant exhibit. (Click the Tenant tab.)

Save

Discard

Directory properties

Name ⓘ

✓

Country or region

Slovenia

Location


EU Model Clause compliant datacenters

Notification language

English

▼

Directory ID



Technical contact

✓

Global privacy contact

✓

Privacy statement URL

✓

Access management for Azure resources

Admin1@Cont190525outlook.onmicrosoft.com (Admin1@Cont190525outlook.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

Yes

No

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin3 can add Admin 2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can add Admin 2 as an owner of the subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input checked="" type="radio"/>

mlantonis Highly Voted 3 years, 11 months ago

Correct Answer:

Azure (RBAC) and Azure AD roles are independent. AD roles do not grant access to resources and Azure roles do not grant access to Azure AD. However, a Global Administrator in AD can elevate access to all subscriptions and will be User Access Administrator in Azure root scope.

All 3 users are GA (AD) and Admin3 is owner of the subscription (RBAC). Admin1 has elevated access, so he is also User Access Admin (RBAC). To assign a user the owner role at the Subscription scope, you require permissions, such as User Access Admin or Owner.

Box 1: Yes
Admin1 has elevated access, so he is User Access Admin. This is valid.

Box 2: Yes
Admi3 is Owner of the Subscription. This is valid.

Box 3: No
Admin2 is just a GA in Azure AD scope. He doesn't have permission in the Subscription.

upvoted 549 times

Dankho 6 months, 2 weeks ago

Wrong on Box1: A Global Administrator in Azure does not automatically have User Access Administrator privileges in Azure RBAC, but they can elevate their access to effectively gain those permissions by enabling the "Access management for Azure resources" setting in the Azure portal, essentially granting them the User Access Administrator role across all subscriptions within the tenant; allowing them to manage user access to Azure resources.

upvoted 3 times

Shri0024 4 months, 1 week ago

2nd Screenshot in question clearly indicate the admin1 has manage access to all subscription in tenant. As per first screenshot admin1 is not owner, however if he still able to manage access then this implies that admin1 has user access admin role on subscription. So Box1 is yes.

upvoted 2 times

schvantz 3 years ago

crystal clear
upvoted 5 times

Takloy 3 years, 6 months ago

Unless configure the elevated access for Admin 2 right? making admin2 user access administrator.
upvoted 2 times

kastanov 2 years, 9 months ago

Global Administrators can create resource groups in the subscription. How you work like this in your?

upvoted 1 times

  **ashish2201** Highly Voted 3 years, 11 months ago

Answer is correct, tested in Lab

1. No : Admin1 is a Global Administrator at Tenant which does not give it permission on subscription therefore cannot assign Owner Roles
2. Yes : Admin 3 is Global Administrator + Owner of Subscription therefore can assign Owner role to other user.
3. NO : Admin2 is Global Administrator for Tenant and do not have any rights on Subscription therefore cannot create resources in it.

upvoted 63 times

  **ashish2201** 3 years, 11 months ago

Kindly ignore my previous comment, below is the correct one

1. Yes : Admin1 is a Global Administrator at Tenant which does not give it permission on subscription but as per exhibit it has taken control to manage access to all Azure subscriptions therefore it now has access to manage subscription therefore can assign role to other users.
2. Yes : Admin 3 is Global Administrator + Owner of Subscription therefore can assign Owner role to other user.
3. NO : Admin2 is Global Administrator for Tenant and do not have any rights on Subscription therefore cannot create resources in it.

upvoted 116 times

  **Praveen66** 3 years, 8 months ago

Even if your a global administrator at the Tenant level you can grant the access of owner to any other user to in tenant for the subscription.

Simple example is the default account through which you have registered is global admin, if you have created another user account you can very well assign a owner role to him for a sub

upvoted 2 times

  **Bikth** Most Recent 2 months, 3 weeks ago

Answer:

| Statements | Yes | No |

| Admin1 can add Admin2 as an owner of the subscription. | ☐ | **√** |

| Admin3 can add Admin2 as an owner of the subscription. | **√** | ☐ |

| Admin4 can create a resource group in the subscription. | ☐ | **√** |

Explanation:

- **Admin3** has the **Owner** role at the subscription scope, granting full permissions to manage access (including adding other owners).
- **Admin1**, despite being a Global Administrator, lacks explicit RBAC roles (e.g., Owner, User Access Administrator) on the subscription, so they cannot modify role assignments.
- **Admin4** is not listed in the RBAC assignments and has no permissions to create resource groups (requires Contributor/Owner role).

upvoted 1 times

  **Bravo_Dravel** 3 months, 1 week ago

Box 1: Yes Admin1 is configured to manage access to all Azure subscriptions and management groups in the directory, they can add another user as the Owner of an Azure subscription associated with the tenant

B. Yes

Box 3: No

upvoted 1 times

  **Toxictwins** 6 months, 1 week ago

Correct answers :



Box 1 = YES

Box 2 = YES

Box 3 = YES , as a Global Admin, you can elavate access, and give your account Subscription Owner permissions (tested successful in my own tenant).

See MS article "Elevate access to manage all Azure subscriptions and management groups" (<https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin?tabs=azure-portal>)

upvoted 1 times

  **feralberti** 6 months, 2 weeks ago

question 1 is indeed a Yes, User Access Administrator: Manage user access to Azure resources, Assign roles in Azure RBAC, Assign themselves or others the Owner role.

source: <https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

upvoted 1 times

  **james1890** 7 months, 2 weeks ago

By default, Azure roles and Azure AD roles do not span Azure and Azure AD. However, if a Global Administrator elevates their access by choosing the Access management for Azure resources switch in the Azure portal, the Global Administrator will be granted the User Access Administrator role (an Azure role) on all subscriptions for a particular tenant. The User Access Administrator role enables the user to grant other users access to Azure resources. This switch can be helpful to regain access to a subscription. For more information, see Elevate access to manage all Azure subscriptions and management groups.

Several Azure AD roles span Azure AD and Microsoft 365, such as the Global Administrator and User Administrator roles. For example, if you are a member of the Global Administrator role, you have global administrator capabilities in Azure AD and Microsoft 365, such as making changes to Microsoft Exchange and Microsoft SharePoint. However, by default, the Global Administrator doesn't have access to Azure resources.

Box 1: YES

Box 2: YES



Box 3: NO

upvoted 3 times

  **Lazylinux** 7 months, 2 weeks ago

Guys i was convinced NYN and only Bill Gates would have convinced me otherwise!!!! until i read those two links below i than realized it is YYN for sure
So answer is YYN
Also as point admin2 can assigned themselves the user admin by click YES to the Access management for Azure resources
Below is snippet but i encourage you read all
When you set the toggle to Yes, you are assigned the User Access Administrator role in Azure RBAC at root scope (/). This grants you permission to assign roles in all Azure subscriptions and management groups associated with this Azure AD directory. This toggle is only available to users who are assigned the Global Administrator role in Azure AD.
When you set the toggle to No, the User Access Administrator role in Azure RBAC is removed from your user account. You can no longer assign roles in all Azure subscriptions and management groups that are associated with this Azure AD directory. You can view and manage only the Azure subscriptions and management groups to which you have been granted access.
will continue in reply as txt too large

upvoted 2 times

  **Lazylinux** 2 years, 10 months ago
further info below

Note:

If you're using Privileged Identity Management, deactivating your role assignment does not change the Access management for Azure resources toggle to No. To maintain least privileged access, we recommend that you set this toggle to No before you deactivate your role assignment.

Click Save to save your setting.

This setting is not a global property and applies only to the currently signed in user. You can't elevate access for all members of the Global Administrator role.

More info here: <https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin#how-does-elevated-access-work>

upvoted 1 times

  **[Removed]** 8 months ago
wrong

Yes

Yes

No

upvoted 3 times

  **Makoporosh** 10 months ago

The answer is NYN: Global Administrators in Azure AD have the highest level of access in the Azure Active Directory, allowing them to manage users, groups, and other directory-related functions. However, this role does not automatically grant them access to manage Azure subscriptions and resources within those subscriptions.

upvoted 1 times

  **[Removed]** 10 months, 3 weeks ago

Admin1 can add Admin 2 as an owner of the subscription.

Yes: Admin1 is a global administrator, and based on the tenant settings, global administrators can manage access to all Azure subscriptions and management groups in this directory.

Admin3 can add Admin 2 as an owner of the subscription.

Yes: Admin3 is already assigned the "Owner" role for the subscription. An owner has full access, including the ability to assign roles to other users.

Admin2 can create a resource group in the subscription.

Yes: Admin2 is a global administrator. Global administrators have the highest level of permissions in Azure AD and can manage all aspects of the directory and subscription.

upvoted 2 times

  **SofiaLorean** 11 months, 3 weeks ago

Answer should be : Yes Yes No

upvoted 2 times

  **3c5adce** 11 months, 4 weeks ago

I believe the more recent and tested answer which is YYN

upvoted 2 times

  **3c5adce** 12 months ago

Answer is YYN

upvoted 2 times

  **Nateramj** 1 year ago



My thought here is

Box1:Admin1 even with Global admin permissions, User Administrator refers to the 365 admin console, and not Azure resources. They would need RBAC control to the subscription in the form of User Access Admin/Owner to add themselves to be able to add RBAC controls for others-NO is correct

Box 2:Admin 3 is an Owner of the subscription, subsequently meaning the ability to add RBAC controls for other Admins-YES is the correct Answer

Box 3: whilst Admin 2 is a GA they do not possess the correct RBAC role for the subscription resource meaning they cannot hand out permissions- Correct answer is NO



upvoted 1 times

  **_gio_** 1 year, 1 month ago

YES YES NO

Admin3 can elevate his permissions but in this question only Admin 1 has elevated his permissions

upvoted 1 times

  **tashakori** 1 year, 1 month ago

No no no

upvoted 1 times

You have an Azure subscription named Subscription1 that contains an Azure virtual machine named VM1. VM1 is in a resource group named RG1. VM1 runs services that will be used to deploy resources to RG1.

You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1.

What should you do first?



- A. From the Azure portal, modify the Managed Identity settings of VM1
- B. From the Azure portal, modify the Access control (IAM) settings of RG1
- C. From the Azure portal, modify the Access control (IAM) settings of VM1
- D. From the Azure portal, modify the Policies settings of RG1


Correct Answer: A

Community vote distribution

A (87%)

13%

-   **mlantonis**



Highly Voted 

 3 years, 11 months ago



Correct Answer: A

Managed identities for Azure resources provides Azure services with an automatically managed identity in Azure Active Directory. You can use this identity to authenticate to any service that supports Azure AD authentication, without having credentials in your code. You can enable and disable the system-assigned managed identity for VM using the Azure portal.



RBAC manages who has access to Azure resources, what areas they have access to and what they can do with those resources. Examples of Role Based Access Control (RBAC) include: Allowing an app to access all resources in a resource group Policies on the other hand focus on resource properties during deployment and for already existing resources. As an example, a policy can be issued to ensure users can only deploy DS series VMs within a specified resource

upvoted 267 times
-   **itgg11** 2 years, 9 months ago



A is a correct answer. Just tested in the lab and first you need to create a managed identity

upvoted 5 times
-   **Kalzonee3611** 1 year, 7 months ago

he is goat

upvoted 3 times
-   **Dankho** 6 months, 2 weeks ago



we really gotta bring that word here. When I think of goat I think of Jordan, Ali, Gretsky, not freakin' mlantonis, c'mon now!

upvoted 3 times
-   **kilowd** 2 years, 11 months ago



Answer A: What is a managed identity in Azure?

Image result for managed identity vs Access Control(IAM) azure



Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication

upvoted 2 times
-   **zman_83** 2 years, 7 months ago



Trust in Superman(mlantonis)!!!

upvoted 24 times
-   **BaldFury401** 2 years, 7 months ago



mlantonis is a savage

upvoted 6 times
-   **AzureG0d** 2 years, 6 months ago

i promise he is LOL

upvoted 4 times
-   **supershysherlock** 2 years, 6 months ago

What ho, jolly good show that man!

upvoted 4 times
-   **ment0s** 1 year, 8 months ago

Right-O good chap, no faffing about, tally-ho!

upvoted 2 times

🗲️ 👤 **fedztedz** Highly Voted 👍 4 years, 3 months ago

Answer is correct "A" Modify Managed Identities.

upvoted 55 times

🗲️ 👤 **RVivek** Most Recent ⌚ 5 months, 4 weeks ago

Selected Answer: A

Answer is A. Both A and B are the required steps. However the question states What should you do first. By default VM does not have Managed Identity assigned. Hence first you should modify that setting, then step B

upvoted 3 times

🗲️ 👤 **[Removed]** 8 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗲️ 👤 **mojo86** 8 months, 4 weeks ago

'A' is the correct answer. The first thing you should do is enable the system-assigned managed identity for VM1. This managed identity will then be used to authenticate and manage resources in RG1. After enabling the identity, you need to assign the appropriate role to it at the resource group level to grant it the necessary permissions.

upvoted 1 times

🗲️ 👤 **3ba6d0b** 10 months, 3 weeks ago

Selected Answer: A

To ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1, you should first enable a managed identity for VM1. This can be done by modifying the Managed Identity settings of VM1 from the Azure portal. Once the managed identity is enabled, you can assign the necessary role to this identity in the Access control (IAM) settings of RG1 to grant it the required permissions.

upvoted 1 times

🗲️ 👤 **3c5adce** 11 months, 4 weeks ago

A. From the Azure portal, modify the Managed Identity settings of VM1

This is the correct first step. You should enable a managed identity for VM1. Managed identities are Azure AD objects that provide Azure services with an identity within Azure AD. By enabling a managed identity, VM1 can authenticate to Azure services that support Azure AD authentication, like Azure Resource Manager, for managing resources.

upvoted 1 times

🗲️ 👤 **3c5adce** 12 months ago

A. From the Azure portal, modify the Managed Identity settings of VM1

upvoted 1 times

🗲️ 👤 **stanislaus450** 1 year, 2 months ago

Selected Answer: A

To enable a service running on VM1 to manage resources in RG1 using VM1's identity, you should first configure the Managed Identity settings for VM1. Managed identities for Azure resources provide automatically managed identities for Azure services, allowing them to authenticate to services that support Microsoft Azure authentication without requiring credentials in your code12.

Therefore, the correct answer is A. From the Azure portal, modify the Managed Identity settings of VM1.

upvoted 2 times

🗲️ 👤 **sismer** 1 year, 4 months ago

Selected Answer: B

The question is clearly saying that the VM has already a MI. You just need to assign the RBAC to the MI. So the answer is B.

upvoted 2 times

🗲️ 👤 **18c2076** 1 year, 1 month ago

Comprehend the question better next time before blasting your thoughts. Its just implying that it NEEDS TO BE ABLE TO USE the Managed Identity. Without having created/enabled it, YOU CANT USE IT. Correct answer: A !

upvoted 1 times

🗲️ 👤 **BillDilena** 1 year, 8 months ago

Selected Answer: A

By default, resources system managed identity status is Off. FIRST we need to turn it ON

upvoted 4 times

🗲️ 👤 **oopspruu** 1 year, 8 months ago

Selected Answer: A

Pay attention to the question. It asks what should you do FIRST.

You'd do A first, and then B. Once you have enabled Managed Identity for this VM, you can then give it access using IAM.

upvoted 6 times

🗲️ 👤 **NavigatiOn** 1 year, 9 months ago



A. From the Azure portal, modify the Managed Identity settings of VM1.

Explanation:

Managed identities for Azure resources is a feature of Azure Active Directory (Azure AD). Each of the Azure resources has an identity in Azure AD that you can use to authenticate to any service that supports Azure AD authentication, without any credentials stored in your code.

Managed identities eliminate the need for developers having to manage credentials by providing an identity for the Azure resource in Azure AD and using it to obtain Azure Active Directory (Azure AD) tokens.

upvoted 1 times

  **Athul07** 1 year, 11 months ago

A. From the Azure portal, modify the Managed Identity settings of VM1

To ensure that a service running on VM1 can manage the resources in RG1 using the identity of VM1, you should first modify the Managed Identity settings of VM1.

Managed Identity allows Azure resources, such as virtual machines, to obtain an identity that can be used to authenticate and authorize against other Azure resources. By enabling Managed Identity for VM1, you can grant the necessary permissions to the service running on VM1 to manage resources in RG1 without exposing any sensitive credentials.

upvoted 2 times

  **Exilic** 1 year, 12 months ago

Selected Answer: A

OpenAI



"A. From the Azure portal, modify the Managed Identity settings of VM1

To allow a service running on a virtual machine to manage resources in an Azure resource group, you can use a managed identity for the virtual machine. A managed identity is an Azure Active Directory (Azure AD) object that can be used to authenticate to services that support Azure AD authentication, including Azure Resource Manager. By using a managed identity, you can avoid the need to store credentials for a service account on the virtual machine.

To enable a managed identity for a virtual machine, you can modify the Managed Identity settings of the virtual machine from the Azure portal or using Azure PowerShell or Azure CLI. Once the managed identity is enabled, you can grant the identity access to the resource group by assigning it a role or permissions in the Access control (IAM) settings of the resource group.

Therefore, the correct option is A. From the Azure portal, modify the Managed Identity settings of VM1."

upvoted 2 times

  **Chris76** 2 years ago

Selected Answer: A

A & B are needed to achieve the goal. But the question asks which one needs to be done FIRST. Hence its A, aka ensuring you have a management identity assigned to the VM. And only then configure what access that managed identity has from within the IAM of the RG

upvoted 4 times

  **lokii9980** 2 years, 1 month ago

Once the Managed Identity for VM1 is enabled, you can grant the necessary permissions to the service running on VM1 to manage the resources in RG1 by using the identity of VM1. This can be done by modifying the Access control (IAM) settings of RG1 or the specific resources within RG1 as needed, and adding the Managed Identity of VM1 with the appropriate role-based access control (RBAC) role.

upvoted 4 times

You have an Azure subscription that contains a resource group named TestRG.
You use TestRG to validate an Azure deployment.
TestRG contains the following resources:

Name	Type	Description
VM1	Virtual Machine	VM1 is running and configured to back up to Vault1 daily
Vault1	Recovery Services Vault	Vault1 includes all backups of VM1
VNET1	Virtual Network	VNET1 has a resource lock of type Delete

You need to delete TestRG.
What should you do first?

- A. Modify the backup configurations of VM1 and modify the resource lock type of VNET1
- B. Remove the resource lock from VNET1 and delete all data in Vault1
- C. Turn off VM1 and remove the resource lock from VNET1
- D. Turn off VM1 and delete all data in Vault1



Correct Answer: B


Community vote distribution

B (67%)

A (22%)

9%

  **mlantonis**

Highly Voted 

 3 years, 11 months ago

Correct Answer: B

When you delete a resource group, all of its resources are also deleted. Deleting a resource group deletes all of its template deployments and currently stored operations.

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

You can't delete a vault that contains backup data. Once backup data is deleted, it will go into the soft deleted state.

So you have to remove the lock on order to delete the VNET and delete the backups in order to delete the vault.



Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/delete-resource-group?tabs=azure-powershell>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>



<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault#before-you-start>

upvoted 307 times

  **eternaldiarrhea** 1 month, 2 weeks ago



This man is a beast. You can take my daughter, but nourish my nuts first

upvoted 1 times

  **Gyanshukla** 3 years, 8 months ago



correct

upvoted 2 times

  **monus** 3 years, 7 months ago

backup can be taken even if vm is powered off. so, I think the answer is A.



upvoted 11 times

  **AubinBakana** 3 years, 8 months ago

No, this is wrong. one of the reasons why resource groups were designed is to facilitate the deletion of resources in Dev environments. You delete the RG and all its components are gone.

C is the answer.

upvoted 1 times

  **AubinBakana** 3 years, 8 months ago

sorry, I meant Dev/Test environment. Think CI/CD.

upvoted 1 times

  **zr79** 3 years, 2 months ago

Microsoft decided on an exception for recovery vaults. it's weird but you can not delete your RG before deleting your vaults

upvoted 9 times

  **Dips88** Highly Voted 4 years ago

Answer should be B. A recovery service vault can not deleted unless all its backups are deleted permanently. And along with that definitely resource lock has to be removed on vnet

upvoted 127 times

  **poplovic** 3 years, 10 months ago

Tried in the lab, a lot of steps to remove the vault.

<https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal>

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-security-feature-cloud#permanently-deleting-soft-deleted-backup-items>

upvoted 1 times

  **rawrkadia** 3 years, 9 months ago

Disagree. The more I think about this, the less "delete all data" makes sense as step one. Step one is to modify the VM's backup configuration, but A doesn't make sense either.

I actually think they're correct. Easiest first step is to shut stuff off (not strictly needed) and remove the resource lock. Then disable soft-delete if on, remove the backup configuration for VM1 and any backups, then you can turn down the RG.

upvoted 4 times

  **mmNYC** 3 years, 3 months ago

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault?tabs=portal>

vault manuall deleted because it stays there 14 days.. B , is corect unswer, if it was sql you need to shutdown sql instances for backup

upvoted 2 times

  **mmtechsolutionsinc** 3 years, 2 months ago

true but q is what is first, vm off, delete off, then go to recovery service emty it, then remove RG

upvoted 3 times

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

Selected Answer: B

Resource Locks: You must remove any resource locks from VNET1 to allow the deletion of the resource group1.

Vault Data: Deleting all data in Vault1 ensures that there are no dependencies preventing the deletion of the resource group

upvoted 1 times


  **58b2872** 4 months, 1 week ago

Selected Answer: B

The resource lock of type Delete on VNET1 will prevent the deletion of the virtual network and, consequently, the resource group, so you must first remove the resource lock on VNET1. Later, Vault1 contains backups of VM1. Before you can delete the recovery vault, you need to delete all data (backups) inside it.

Azure Recovery Services Vaults require the deletion of backup data before the vault itself can be deleted.

upvoted 2 times

  **Mazinger** 7 months, 2 weeks ago

Selected Answer: B

B. Remove the resource lock from VNET1 and delete all data in Vault1.

Before you can delete TestRG, you must remove any dependencies that are associated with the resources in TestRG. In this scenario, VNET1 has a resource lock of type delete, which means it cannot be deleted until the resource lock is removed. Additionally, Vault1 contains backups of VM1, so you must delete all the data in Vault1 before deleting TestRG.

To do this, you can follow these steps:

1. Navigate to the VNET1 resource in the Azure portal.
2. Under Settings, select Locks.
3. Select the delete lock for VNET1 and then click Delete.
4. Navigate to the Vault1 resource in the Azure portal.
5. Delete all the backup data associated with VM1.
6. After all backup data has been deleted, delete Vault1.
7. Once VNET1 and Vault1 are deleted, you can delete TestRG.

By removing the resource lock from VNET1 and deleting all data in Vault1, you ensure that all dependencies associated with TestRG have been removed before deleting the resource group.


upvoted 7 times

  **[Removed]** 8 months ago

Selected Answer: B

it's B

upvoted 1 times

  **CheMetto** 9 months, 1 week ago

Selected Answer: B

C and D is wrong, you don't need to turn off VM.

Both A and B are not correct but B is more correct than A, let me explain:

One of the first thing to do is to remove the resource lock, which is done only from B. A doesn't Remove the resource lock but edit it. You can edit a resource lock and switch between delete and read-only (read-only is you can't delete, and you can't modify, delete has only delete lock, you can modify the resource). So This is where A is wrong.

To delete a backup, you can't go in the vault and delete it, before do that, you need to go to stop backup, then you can delete all backup, so that's why B is incorrect, is missing 1 step. This step is not mentioned in A too, it says modify backup configuration. Backup configuration mean how many time i took the backup, retain, snapshot etc, but it doesn't stop the backup, you need to do that from backup item.

upvoted 6 times

  **Charumathi** 10 months, 4 weeks ago

B is the correct answer,

1. Remove VM Backup from Recovery Services Vault
Stop Backup: First, stop the backup for the VM in the Recovery Services vault.



Navigate to the Recovery Services vault.
Go to "Backup items".
Select the VM.
Click "Stop backup".
Choose the option to "Retain data" or "Delete backup data". If you choose to retain data, you must delete it later from the backup data.
Delete Backup Data (if chosen earlier):

In the Recovery Services vault, go to "Backup items".
Select the VM.
Click "Delete backup data".

2. Remove the Delete Lock on vNet
Navigate to the vNet that has the delete lock.
Go to "Locks" under the "Settings" section.
Select the delete lock and remove it.

3. Delete the Resource Group
Navigate to the Resource Group containing the VM, Recovery Services vault, and vNet.
Click "Delete Resource Group".
Confirm the deletion by typing the resource group name when prompted.

upvoted 2 times

  **3c5adce** 11 months, 4 weeks ago


B. Remove the resource lock from VNET1 and delete all data in Vault1 is the most direct and comprehensive approach to prepare the resource group for deletion, assuming you manage data deletion carefully to prevent unwanted loss. Removing resource locks is necessary to allow deletion, and clearing Vault1 ensures there are no leftover dependencies that could halt the process. Thus, removing the resource lock is the critical first step, which is covered in this option.

upvoted 1 times

  **3c5adce** 12 months ago

B. Remove the resource lock from VNET1 and delete all data in Vault1


upvoted 1 times

  **_gio_** 1 year, 1 month ago

Selected Answer: C

C or D.
Before deleting resource group, you must first solve this problem:
- you can't delete a virtual network with subnets that are still in use by a virtual machine.
- you can't delete recovery service vault with backedup data inside

upvoted 2 times

  **Cg007** 1 year, 1 month ago

Selected Answer: C

C. Turn off VM1 and remove the resource lock from VNET1

Before deleting the resource group TestRG, it's essential to ensure that all resources within it are in a state that allows for their deletion. Turning off VM1 and removing any resource locks from VNET1 would prepare the resources for deletion without causing any data loss or leaving resources in a locked state.

upvoted 2 times

  **jecampos2** 1 year, 2 months ago

I would say the correct ans is C, but you could also think the B is OK. The question is.
Once we execute the delete resource group action it will automatically turn off the VM1?
If yes, then the ans should be B.
Please advise

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

B is correct

upvoted 1 times

  **HdiaOwner** 1 year, 2 months ago

Answer should be B

upvoted 1 times

  **MYR55** 1 year, 4 months ago

3 steps which has to be done before we can delete the resource group

-> Stop the back up of VM

-> Delete all locks on resources of rg

-> Empty the vault

based on this, B seems to be the best option.

upvoted 2 times

  **MentalTree** 1 year, 4 months ago

Correct Answer: C

Question is what should you DO FIRST:

-First you turn off the VM and remove the resource lock

-Once VM is off you can modify the back config

-Once backup config is remove you can remove backups from vault

-Once vault is empty you can remove the TestRG.

Key point being that of the choices, C which includes turning off the VM HAS to be done first before anything else can be done.

upvoted 3 times

  **MentalTree** 1 year, 4 months ago

Ignore what I said about backup config xD

The VM has to be off so that it is not using the subnet associated with the vnet: "you can't delete a virtual network with subnets that are still in use by a virtual machine"

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/delete-resource-group?tabs=azure-powershell#required-access-and-deletion-failures>

upvoted 2 times



You have an Azure DNS zone named adatum.com.
You need to delegate a subdomain named research.adatum.com to a different DNS server in Azure.
What should you do?


- A. Create an NS record named research in the adatum.com zone.
- B. Create a PTR record named research in the adatum.com zone.
- C. Modify the SOA record of adatum.com.
- D. Create an A record named *.research in the adatum.com zone.

Correct Answer: A

Community vote distribution

A (100%)

-   **mlantonis**

Highly Voted 



 3 years, 11 months ago

Correct Answer: A



An NS record or (name server record) tells recursive name servers which name servers are authoritative for a zone. You can have as many NS records as you would like in your zone file. The benefit of having multiple NS records is the redundancy of your DNS service.

You need to create a name server (NS) record for the zone.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain>
upvoted 242 times
-   **suriyaswamy** 3 years, 8 months ago



Nice Explanation. Many Thanks


upvoted 2 times
-   **Tom34** 3 years, 3 months ago

Answer A correct.

It should be "Create or edit an NS record .."


Because this record is already created after DNS zone creation.

upvoted 6 times
-   **chaitu1990**



Highly Voted 


 4 years, 3 months ago

All the best for your Exam guys:))

upvoted 174 times
-   **omw2wealth** 3 years, 7 months ago

Thank you i guess



upvoted 11 times
-   **[Removed]**

Most Recent 



 8 months ago

Selected Answer: A

A is corerct

upvoted 2 times
-   **tashakori** 1 year, 1 month ago



A is right

upvoted 2 times
-   **Athul07** 1 year, 11 months ago

A. Create an NS record named research in the adatum.com zone.

To delegate a subdomain named research.adatum.com to a different DNS server in Azure, you should create an NS (Name Server) record named "research" in the adatum.com zone.

The NS record is used to delegate authority for a subdomain to a different set of name servers. By creating an NS record named "research" in the adatum.com zone and specifying the name server(s) for the subdomain, you can delegate the management of the research.adatum.com subdomain to the specified DNS server(s) in Azure.

upvoted 4 times
-   **djgodzilla** 2 years, 1 month ago

Selected Answer: A

to cut the crap watch this video to understand really what an NS record is !👉

<https://www.youtube.com/watch?v=WyDQHrDad8&t=2s>

upvoted 5 times

🗋️ 👤 **Mazinger** 2 years, 2 months ago

Selected Answer: A

A. Create an NS record named research in the adatum.com zone.

To delegate a subdomain named research.adatum.com to a different DNS server in Azure, you need to create an NS (name server) record in the adatum.com DNS zone that specifies the name of the DNS server that will handle the subdomain.

To do this, you can follow these steps:

1. In the Azure portal, navigate to the adatum.com DNS zone.
2. Under Settings, select NS records.
3. Click Add NS record to add a new NS record.
4. In the Record name field, enter "research".
5. In the FQDN of name server field, enter the FQDN of the DNS server that will handle the research.adatum.com subdomain.
6. Click Add to create the NS record.

Once the NS record is created, any DNS queries for research.adatum.com will be forwarded to the DNS server specified in the NS record.

upvoted 1 times

🗋️ 👤 **[Removed]** 2 years, 3 months ago

I'm not seeing any DNS questions on the recent test

upvoted 1 times

🗋️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: A

A) " Create an NS record named research in the adatum.com zone."

Reference: <https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain#create-an-ns-record>

upvoted 1 times

🗋️ 👤 **EmnCours** 2 years, 8 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

🗋️ 👤 **Lazylinux** 2 years, 10 months ago

Selected Answer: A

A is correct

upvoted 1 times

🗋️ 👤 **manalshowaei** 2 years, 10 months ago

Selected Answer: A

A. Create an NS record named research in the adatum.com zone.

upvoted 1 times

🗋️ 👤 **Chrys941** 3 years ago

According to The Documentation please read the answer is correct

<https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain>

upvoted 1 times

🗋️ 👤 **WS_21** 3 years, 2 months ago

Selected Answer: A

<https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain>

upvoted 2 times

🗋️ 👤 **EleChie** 3 years, 2 months ago

FYI:

A record - The record that holds the IP address of a domain.

AAAA record - The record that contains the IPv6 address for a domain (as opposed to A records, which list the IPv4 address).

CNAME record - Forwards one domain or subdomain to another domain, does NOT provide an IP address.

MX record - Directs mail to an email server. Learn more about the MX record.

TXT record - Lets an admin store text notes in the record. These records are often used for email security.

NS record - Stores the name server for a DNS entry.

SOA record - Stores admin information about a domain.

SRV record - Specifies a port for specific services.

PTR record - Provides a domain name in reverse-lookups.

upvoted 25 times

🗋️ 👤 **GodfreyMbizo** 3 years, 7 months ago

I have just started yesterday,i have exam i 2 days time,i dont know if i will master everything

upvoted 2 times

🗋️ 👤 **ShikshaGarg** 3 years, 9 months ago

Thanks a lot ExamTopics for the questions and also this discussion panel, helps a lot to understand different ways a question can be solved. All the best everyone!! :)

upvoted 2 times

DRAG DROP -

You have an Azure Active Directory (Azure AD) tenant that has the contoso.onmicrosoft.com domain name.

You have a domain name of contoso.com registered at a third-party registrar.

You need to ensure that you can create Azure AD users that have names containing a suffix of @contoso.com.

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

Select and Place:

Actions		Answer Area
Add a record to the public contoso.com DNS zone		
Add an Azure AD tenant		
Configure company branding	➤	⬆
Create an Azure DNS zone	⬅	⬇
Add a custom name		
Verify the domain		

Correct Answer:

Actions		Answer Area
		Add a custom name
Add an Azure AD tenant		Add a record to the public contoso.com DNS zone
Configure company branding	➤	Verify the domain
Create an Azure DNS zone	⬅	

1. Add the custom domain name to your directory
2. Add a DNS entry for the domain name at the domain name registrar
3. Verify the custom domain name in Azure AD

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>

 **mumu_myk** Highly Voted 3 years, 5 months ago


I bought a domain just to test this. The answer is correct. Please like me.
upvoted 1407 times

 **andted98** 3 weeks ago

Sensational!
upvoted 1 times

 **junaidd001** 1 year, 7 months ago

inspiring
upvoted 13 times

 **hehuo** 2 years, 2 months ago

i attach the answer:
1. Add the custom domain name to your directory



- 2. Add a DNS entry for the domain name at the domain name registrar
- 3. Verify the custom domain name in Azure AD

upvoted 22 times

  **fene** Highly Voted 4 years ago

As I'm a smart guy I can confirm this to be the proper answer

upvoted 163 times

  **xheo** 3 years, 1 month ago



I like your confidence :)

upvoted 6 times

  **maki999** 1 year, 3 months ago

me too :)

upvoted 3 times

  **rolling_potato_** 3 years, 2 months ago

Seems legit

upvoted 22 times



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

Correct.

Steps are:

- 1. Add a custom domain: Add the contoso.com domain to your Azure AD tenant.
- 2. Add a record to the public contoso.com DNS zone: Update your DNS settings at the third-party registrar to include the necessary records for domain verification.
- 3. Verify the domain: Verify the contoso.com domain in Azure AD.

upvoted 2 times

  **RVivek** 5 months, 3 weeks ago

- 1. Add the custom domain name to your directory
 - 2. Add a DNS entry for the domain name at the domain name registrar
 - 3. Verify the custom domain name in Azure AD
- <https://learn.microsoft.com/en-us/entra/fundamentals/add-custom-domain>

upvoted 2 times

  **mcdet** 6 months ago


this is the right answer

upvoted 1 times

  **[Removed]** 8 months ago

correct

upvoted 2 times

  **23169fd** 10 months, 3 weeks ago

Add a custom name: Register the contoso.com domain in your Azure AD tenant.
Add a record to the public contoso.com DNS zone: Add the necessary DNS records at the domain registrar to verify the domain.
Verify the domain: Complete the verification process in Azure AD to confirm ownership of the contoso.com domain.

upvoted 5 times

  **MCLC2021** 1 year ago

- 1- Create an Azure DNS Zone.
 - 2- Add a record to the public contoso.com DNS zone.
 - 3- Verify the domani.
- Tutorial: Host your domain in Azure DNS (<https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>)
<https://learn.microsoft.com/es-es/training/modules/configure-azure-dns/>

upvoted 5 times

  **etrop** 9 months ago

I guess the answer is correct, but it says "Add a custom name", I feel like someone uneducated wrote this question, couldn't they have written "Add a custom domain" just like in the portal interface. Why is it so hard to just get some simple english accurate on the exam. I mean "Adding a custom name" is not the same thing as "Adding a custom domain name". There is actually a way to add a custom Name to your AD under Properties and name, so if we were being 100% accurate here that "Adding a custom name" is not the correct step. So many questions are like this, its almost as if they were written poorly to try to trip you up.

upvoted 1 times

  **tashakori** 1 year, 1 month ago

Given answer is correct

upvoted 1 times

  **897dd59** 1 year, 7 months ago

The answer is correct. but as we are all known. It's MS, learning doc vs documentation vs exam are all different. nothing in common. About the exam alone. my experiences with the drag/drop is about to read the question carefully. Some of them require something like: bla..blah ... Make sure the steps are in correct order => then should care about the steps we drag/drop to correct with what we will do in the real envi

upvoted 3 times

  **USNOOZEYULOSEY** 1 year, 9 months ago

For some CSI, it would be nice if the "custom name" was updated to "add custom domain name" for brevity.

upvoted 2 times

  **sardonique** 1 year, 7 months ago

It was purposefully called custom name to trick you into choosing "Create an Azure DNS Zone"

upvoted 2 times

  **NavigatiOn** 1 year, 9 months ago

Here are the steps we need to perform in sequence:

> > Add a custom name: add a custom domain name to Azure AD from the "Custom domain names" page in the Azure portal. When we add a custom domain name, Azure AD gives us the information we need to create DNS records at the domain name registrar.

> > Add a record to the public contoso.com DNS zone: we need to add a DNS record at our domain name registrar to verify that we own the domain. This record is typically a TXT or MX record for domain verification.

> > Verify the domain: After we've added the DNS record at the domain name registrar, then we can go back to the Azure portal to verify the domain. Azure AD checks if the DNS record exists and if it does, the domain is verified.

upvoted 24 times

  **Iolek997** 1 year, 11 months ago

1. Add the custom domain name to your directory:

In the Azure portal, navigate to the Azure Active Directory blade.

Select "Custom domain names" and click on the "+ Add custom domain" button.

Enter the domain name "contoso.com" and follow the prompts to add the domain.

2. Add a DNS entry for the domain name at the domain name registrar:

Sign in to the domain name registrar where you registered the domain name (e.g., the third-party registrar for contoso.com).

Add a DNS entry for the custom domain, such as a CNAME or TXT record, as instructed by Azure AD.

This step verifies your ownership of the domain.

3. Verify the custom domain name in Azure AD:

In the Azure portal, go back to the Azure Active Directory blade and select "Custom domain names."

Select the custom domain name (e.g., contoso.com) and click on the "Verify" button.


Azure AD will check the DNS records to ensure they match, and once verified, the domain will be marked as verified.

upvoted 16 times

  **binhdortmund** 1 year, 9 months ago

very clear for me! LIKE

upvoted 1 times

  **etanvandan7** 1 year, 11 months ago

Since a custom domain has already been created and registered at third party, next should be

1. Verify the domain

2. Create an Azure DNS zone

3. Add a record to the public contoso.com DNS zone

upvoted 1 times

  **gauravit43** 2 years, 3 months ago



Given answer is correct -:

1 - add an entry in "custom domain names" (You will see TXT and MX column, make a note of it)

2 - Go to public domain provider (let say godaddy.com) and make 2 entries there (TXT and MX)

3- Verify on the Azure portal

upvoted 4 times

  **rupayan87** 2 years, 5 months ago

options seems terrible here

1 add a custom name - should be domain name

2. add a record to public DNS zone - we only add the MX/TXT record at the third party site as long as the name servers are third party managed.

3. verify the domain - this seems redundant. adding the MX record to third party registrar site is what Azure needs to verify the domain.

upvoted 13 times

  **matejka** 2 years, 6 months ago

Both first two options can be swapped without any issues. So the answer is unclear. But as per <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#add-your-custom-domain-name-to-azure-ad> it is a good idea to provide this answer at the exam:

Add a custom name

Add a record to the DNS zone

Verify the domain

upvoted 2 times

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.
You need to view the error events from a table named Event.
Which query should you run in Workspace1?

- A. Get-Event Event | where {\$_.EventType == "error"}
- B. Event | search "error"
- C. select * from Event where EventType == "error"
- D. search in (Event) * | where EventType != "error"

Correct Answer: B

Community vote distribution

B (91%)

9%

- NaoVaz**

Highly Voted

2 years, 7 months ago

Selected Answer: B

B) 'Event | search "error"'

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial>
upvoted 13 times
- AnKiLa**

2 years, 3 months ago

Agree. Found another reference too:
<https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuredatexplorer>
upvoted 2 times
- Bravo_Dravel**

Highly Voted

3 months, 1 week ago

Selected Answer: B

Other correct versions of this question:
1. search in (Event) "error"
2. Event | search "error"
3. Event | where EventType == "error"
upvoted 6 times
- [Removed]**

Most Recent

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times
- 3c5adce**

12 months ago

C. select * from Event where EventType == "error" This query selects all columns (*) from the "Event" table where the EventType column is equal to "error". It effectively filters the rows in the "Event" table to only those where the EventType is "error", which is what you need to view the error events.
The reason why it's not B. Event | search "error" is that this query selects all records from the "Event" table and then filters them for the string "error". While this query might work in some contexts, it doesn't directly filter based on the EventType column being "error". It searches for the string "error" within all columns.
upvoted 3 times
- MCLC2021**

1 year ago

Selected Answer: B

Repeated question Topic2.Question22

Correct answer B
upvoted 3 times
- Amir1909**

1 year, 2 months ago

B is correct
upvoted 1 times
- Oryx360**

1 year, 8 months ago

Selected Answer: C



The correct query to view error events from a table named "Event" in Azure Log Analytics workspace is:

C. select * from Event where EventType == "error"



This query will retrieve all the records from the "Event" table where the EventType is equal to "error," allowing you to view only the error events.
upvoted 3 times

  **EwoutBI** 1 year, 3 months ago

That's not valid KQL, try it with this sample code
let MyInMemoryTable = datatable(EventType: string, EventMessage: string, EventTime: datetime)
[
"error", "Something bad occurred in the application.", datetime(2024-01-09T13:00:00),
"warning", "A warning was logged by the application, be careful of error", datetime(2024-01-09T14:00:00),
"info", "Informational message from the application.", datetime(2024-01-09T15:00:00),
"error", "Oh noes occurred in the application.", datetime(2024-01-09T16:00:00)
];
SELECT * FROM (MyInMemoryTable) where EventType == "error"
upvoted 1 times

  **XtraWest** 1 year, 10 months ago

Event
| where SeverityLevel == "Error"
Correct Answer: B
upvoted 1 times



  **Athul07** 1 year, 11 months ago

C. select * from Event where EventType == "error"



To view the error events from a table named Event in the Azure Log Analytics workspace named Workspace1, you should run the query:
select * from Event where EventType == "error"

This query selects all the columns (*) from the Event table where the EventType is equal to "error". It will retrieve all the error events from the Event table in Workspace1.



The other options provided are not valid for querying data in Azure Log Analytics. They do not use the correct syntax or functions for querying data in Log Analytics.
upvoted 1 times

  **sedex** 1 year, 9 months ago


select * from Event where EventType == "error" is an example of SQL (Structured Query Language) whereas Log Analytics uses KQL (Kusto Query Language). The correct answer is B
upvoted 5 times

  **gauravit43** 2 years, 3 months ago



B - Tested in lab (Event | search "error")
upvoted 2 times

  **virgilpza** 2 years, 8 months ago



Selected Answer: B
Correct Answer: B
upvoted 2 times

  **KSoul** 2 years, 8 months ago

Selected Answer: B
Event | search "error"
upvoted 2 times

  **libran** 2 years, 8 months ago

Selected Answer: B
Correct Answer: B
upvoted 2 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B
Correct Answer: B
upvoted 2 times

You have a registered DNS domain named contoso.com.
You create a public Azure DNS zone named contoso.com.
You need to ensure that records created in the contoso.com zone are resolvable from the internet.
What should you do?

- A. Create NS records in contoso.com.
- B. Modify the SOA record in the DNS domain registrar.
- C. Create the SOA record in contoso.com.
- D. Modify the NS records in the DNS domain registrar.

Correct Answer: D

Community vote distribution

D (100%)

- Eltooth**

Highly Voted

3 years, 6 months ago

Correct answer - D. Registrar “owns” the tld and will have their NS registered against the domain by default. By changing the registrar NS records to point to your Azure DNS NS records you take ownership into your Azure DNS.

upvoted 58 times
- js_indore**

Highly Voted

3 years, 7 months ago

D. Modify the NS records in the DNS domain registrar.

upvoted 18 times
- [Removed]**

Most Recent

8 months ago

Selected Answer: D

D is corerct

upvoted 2 times
- CheMetto**

9 months, 1 week ago

Selected Answer: D

D is right. After you add a Custom domain name on azure, if you need to make it searchable online, you need to modify the NS record on the registrar. On the Azure DNS page, azure will give you 4 DNS server with his properly name. You need to go on the registrar and add those 4 NS record to make it work in azure.

upvoted 4 times
- 23169fd**

10 months, 3 weeks ago

Selected Answer: D

Update NS record to point to the Azure DNS nameservers. This direct internet traffic to use Azure DNS for resolving records in the contoso.com zone.

upvoted 1 times
- tashakori**

1 year, 1 month ago

D is right

upvoted 1 times
- tashakori**

1 year, 1 month ago

D is right

upvoted 1 times
- Lowe6**

1 year, 4 months ago

also in the question they ask for u to ensure the records already created so A and C becomes wrong immediately

upvoted 2 times
- Athul07**



1 year, 11 months ago

D. Modify the NS records in the DNS domain registrar.

To ensure that records created in the contoso.com zone are resolvable from the internet, you need to modify the NS (Name Server) records in the DNS domain registrar.

When you create a public Azure DNS zone named contoso.com, Azure assigns a set of NS records for that zone. These NS records specify the name servers responsible for handling DNS queries for the contoso.com domain. To make the records in the Azure DNS zone resolvable from the internet, you need to update the NS records at the DNS domain registrar to point to the name servers provided by Azure.

upvoted 5 times

  **djgodzilla** 2 years, 1 month ago

Selected Answer: D

watch this video to understand really what an NS record is !👉
<https://www.youtube.com/watch?v=WyDQhIRDad8&t=2s>
upvoted 12 times

  **Mazinger** 2 years, 2 months ago

Selected Answer: D

D. Modify the NS records in the DNS domain registrar.
To ensure that records created in the Azure DNS zone named contoso.com are resolvable from the internet, you need to delegate the domain to the Azure DNS name servers. To do this, you need to modify the NS (Name Server) records at the DNS domain registrar for contoso.com to point to the Azure DNS name servers. This will allow the authoritative DNS server for contoso.com to be hosted in Azure and answer queries for the contoso.com zone.
Option A is not the correct answer, because creating NS records in the contoso.com zone will not delegate the domain to the Azure DNS name servers. Option B is also not the correct answer, because modifying the SOA (Start of Authority) record in the DNS domain registrar will not delegate the domain to the Azure DNS name servers either. Option C is also not necessary, because Azure DNS automatically creates an SOA record for each zone, and it cannot be modified.
upvoted 8 times

  **[Removed]** 2 years, 3 months ago

Not seeing DNS questions in the 2 tests I took
upvoted 5 times

  **Marge_Simpson** 2 years, 3 months ago

Neither have I
upvoted 2 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: D

D) "Modify the NS records in the DNS domain registrar."

Reference: <https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns#delegate-the-domain>
upvoted 5 times

  **petestudies** 2 years, 8 months ago

Selected Answer: D

this is pretty easy, D
upvoted 2 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: D



Answer is D

Delegate the domain
Once the DNS zone gets created and you have the name servers, you'll need to update the parent domain with the Azure DNS name servers. Each registrar has its own DNS management tools to change the name server records for a domain.

In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers.

When you delegate a domain to Azure DNS, you must use the name servers that Azure DNS provides. Use all four name servers, regardless of the name of your domain. Domain delegation doesn't require a name server to use the same top-level domain as your domain.

<https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>
upvoted 10 times

  **WS_21** 3 years, 2 months ago

Selected Answer: D

<https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>
upvoted 2 times

  **edengoforit** 3 years, 2 months ago

Answer is D and here is some information helpful
You can use Azure DNS to host your DNS domain and manage your DNS records. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

Suppose you buy the domain contoso.net from a domain name registrar and then create a zone with the name contoso.net in Azure DNS. Since you're the owner of the domain, your registrar offers you the option to configure the name server (NS) records for your domain. The registrar stores the NS records in the .NET parent zone. Internet users around the world are then directed to your domain in your Azure DNS zone when they try to resolve DNS records in contoso.net.
upvoted 13 times

HOTSPOT -

You have an Azure subscription that contains a storage account named storage1. The subscription is linked to an Azure Active Directory (Azure AD) tenant named contoso.com that syncs to an on-premises Active Directory domain. The domain contains the security principals shown in the following table.

Name	Type
User1	User
Computer1	Computer

In Azure AD, you create a user named User2.

The storage1 account contains a file share named share1 and has the following configurations.

```
"kind": "StorageV2",
"properties": {
  "azureFilesIdentityBasedAuthentication": {
    "directoryServiceOptions": "AD",
    "activeDirectoryProperties": {
      "domainName": "Contoso.com",
      "netBiosDomainName": "Contoso.com",
      "forestName": "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	Yes	No
You can assign the Storage File Data SMB Share Contributor role to User1 for share1.	<input type="radio"/>	<input type="radio"/>
You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.	<input type="radio"/>	<input type="radio"/>
You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
You can assign the Storage File Data SMB Share Contributor role to User1 for share1.	<input checked="" type="radio"/>	<input type="radio"/>
You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.	<input type="radio"/>	<input checked="" type="radio"/>
You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azure-portal>

- ech

Highly Voted

3 years, 7 months ago

Yo cannot give share-level priviledges to a computer object. Ans is correct.

upvoted 47 times
- ExamWolf

1 year, 5 months ago

You can if you add the computer object to a group first :)

upvoted 1 times
- nir977

3 years, 4 months ago

Y-N-N because user2 is cloud-only user created in AAD and does not have netbios and other chars defined in storage

upvoted 26 times
- allyQ

2 years, 2 months ago

I have created an AAD user (not snyched from the WinDC) and can give it the Storage file data SMB Elev. Contributor role.

upvoted 10 times
- ubiquituz

1 year, 4 months ago

this is the correct answer....only hybrid identities (on-prem synched to ms entra can be assigned share-level rbac roles. cloud only (ms entra/AAD users) can not be assigned... as well as computer accounts too, however computer can use the default share level permission

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azure-portal>



upvoted 2 times

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

Y-N-Y - I've tested this in my lab and was able to add a AzureAD account in a Hybrid environment. So please ignore if someone states Y-N-N.
upvoted 27 times

  **Oramahi3** Most Recent  1 month, 2 weeks ago



I say YNN because, it doesn't mention that user 2 has been synced, therefore, the object of the user is still not replicated, they should at least say DeltaSync was applied on the DC, so Vague question
upvoted 1 times

  **Abhisk127** 3 months, 2 weeks ago

What is correct answer finally ? does anyone had this question appeared in Exam recently?
upvoted 3 times

  **Announcement** 5 months, 2 weeks ago



<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions?tabs=azure-portal#azure-rbac-roles-for-azure-files>
upvoted 1 times

  **RVivek** 5 months, 3 weeks ago

User1 is created in ADDS but synced to Entra AD so Yes.
Computer account cannot be assigned RBAC in Azure AD service . <https://imgur.com/a/dt8hwHO>
user 2 is created in Azure AD can be assigned RBAC .
Hence answer is Y N Y
upvoted 3 times

  **[Removed]** 8 months ago

correct
upvoted 4 times

  **mojo86** 8 months, 4 weeks ago



The answer given is correct. Because computer accounts don't have an identity in Microsoft Entra ID, you can't configure Azure role-based access control (RBAC) for them. However, computer accounts can access a file share by using a default share-level permission.
upvoted 4 times

  **tashakori** 1 year, 1 month ago


Yes
No
No
upvoted 2 times

  **Amir1909** 1 year, 2 months ago

Yes
No
No
upvoted 1 times

  **vsvoid** 1 year, 3 months ago

Y -N -N,
Hybrid user will work
Computer and cloud users will not work
upvoted 2 times

  **31c21da** 1 year, 3 months ago

The key to whether you can assign user2 depends on whether user2 is a cloud-only identity. Initially, yes, as the user is created in Azure AD. However, the question also mentions an Azure AD 'contoso.com' syncs to an on-premises AD. Once user2 is synced, they become a hybrid identity. So, the crucial point here is what the question is aiming to test. If the question is testing whether a user created in Azure AD is initially a cloud-only identity, the answer will be 'N'. If it is testing whether the user will be synced, the answer is 'Y'. Since we don't know the intent of the question, we cannot definitively say whether the answer is N or Y...
upvoted 7 times

  **ggogel** 1 year, 3 months ago

This is not how this works. You can't sync users from AAD to AD. Users need to be created in AD to become a hybrid identity. If they are re-created in AAD they are considered cloud-only. So the user is completely unknown to the AD and therefore can't access that share.
upvoted 4 times

  **GoldBear** 1 year, 4 months ago

Does this question represent the level of knowledge that you need to memorize to perform the role of System Admin? Seems to have too much details to remember, on the job you would run tests on these items to verify if it meets the requirement.
upvoted 5 times

  **897dd59** 1 year, 7 months ago

should be Y-N-Y
1/ you cannot assign for object: computer
2/ user2 is a cloud user => can fully managed on cloud
upvoted 1 times

  **AMEHAR** 1 year, 8 months ago

Y -N -N

upvoted 4 times



  **GoldenDisciple2** 1 year, 8 months ago

Microsoft clearly states the user must have a hybrid identity therefor the 3rd one is a NO.

"If you intend to use a specific Azure AD user or group to access Azure file share resources, that identity must be a hybrid identity that exists in both on-premises AD DS and Azure AD."

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azure-portal#:~:text=If%20you%20intend%20to%20use%20a%20specific%20Azure%20AD%20user%20or%20group%20to%20access%20Azure%20file%20share%20resources%2C%20that%20identity%20must%20be%20a%20hybrid%20identity%20that%20exists%20in%20both%20on%2Dpremises%20AD%20DS%20and%20Azure%20AD.>



upvoted 4 times

  **Andy_S** 1 year, 11 months ago

Y-N-N

In JSON we can see parameter "directoryServiceOptions" has a value "AD" which means File Share is enabled for authentication to users having SESSION TICKET (Kerberos) issued by LOCAL Domain Controller. It means that this file share can be accessed from computers JOINED to AD (OnPrem) and by Users created in OnPrem AD AND Synced to AAD (for RBAC).

upvoted 5 times

  **Andy_S** 1 year, 11 months ago

Ref:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview>

<https://learn.microsoft.com/en-us/azure/templates/microsoft.storage/2021-04-01/storageaccounts?pivots=deployment-language-bicep>

<https://www.linkedin.com/pulse/configuring-active-directory-authentication-over-smb-azure-skerritt/>

upvoted 3 times

HOTSPOT -

You have an Azure subscription named Subscription1 that contains a virtual network VNet1.
You add the users in the following table.

User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which user can perform each configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Add a subnet to VNet1:

User1 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

Assign a user the Reader role to VNet1:

User1 only

User2 only

User3 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Correct Answer:

Answer Area

Add a subnet to VNet1:

User1 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

Assign a user the Reader role to VNet1:

User1 only

User2 only

User3 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Box 1: User1 and User3 only.

User1: The Owner Role lets you manage everything, including access to resources.

User3: The Network Contributor role lets you manage networks, including creating subnets.

Box 2: User1 only.

The Security Admin role: In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles> <https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork>

Correct.
Security admin can't add subnets.
Only owner can assign roles.
upvoted 85 times

🗲️ 👤 **NaoVaz** Highly Voted 👍 2 years, 7 months ago

- 1) Add a subnet to VNET1 = "User1 and User3 only"
- 2) Assign a user the Reader role to VNET1 = "User1 only"

Explanation:

User1 - The Owner Role lets you manage everything, including access to resources.

User3 - The Network Contributor role lets you manage networks, including creating subnets.

User2 - The Security Admin role can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.

upvoted 74 times

🗲️ 👤 **JL2000** Most Recent ⌚ 3 weeks, 1 day ago

Appeared in today's exam

- 1) User 1 and User 3
- 2) User 1 only

upvoted 1 times

🗲️ 👤 **netloony** 1 month, 1 week ago

MS Documentation: You can apply tags to your Azure resources, resource groups, and subscriptions but not to management groups.

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources>

upvoted 1 times

🗲️ 👤 **lumax007** 1 month, 1 week ago

Box 1 - User1 and User3 only

Box 2 - User1 only

upvoted 1 times

🗲️ 👤 **[Removed]** 8 months ago

correct

upvoted 4 times

🗲️ 👤 **Amir1909** 1 year, 2 months ago

Correct

upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 8 months ago

It's 1 & 3 for both answers as both can manage the network and grant access to the vnet.

upvoted 1 times

🗲️ 👤 **KingHalik** 1 year, 6 months ago

But Contributors can't assign roles no?

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 5 times

🗲️ 👤 **THELegendofArangaer** 1 year, 10 months ago

1.User1 and User3

2. User1 only because security admin can't add security roles

upvoted 2 times

🗲️ 👤 **Rams_84z06n** 2 years, 1 month ago

What we are looking for here is Microsoft.Authorization/* permission actions for role assignment. Only Owner role has that among the given choices. Given answer is correct.

upvoted 2 times

🗲️ 👤 **TheB** 2 years, 3 months ago

The provided answer is correct.

upvoted 2 times

🗲️ 👤 **EmnCours** 2 years, 8 months ago

Add a subnet to VNet1: User1 and User3 Only

Assign a user the Reader role to VNet1: User1 Only

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 5 times

🗲️ 👤 **WS_21** 3 years, 2 months ago

Add a subnet to VNet1: User1 and User3 Only

Assign a user the Reader role to VNet1: User1 Only

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 5 times

  **Azure_daemon** 3 years, 2 months ago

the answer is correct, only owner can assign reader role and owner and contributor can add subnet

upvoted 1 times

  **subhuman** 3 years, 5 months ago

Answer is Correct

Owner : Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

Security Administrator Can read security information and reports, and manage configuration in Azure AD and Office 365 (That means he cant assign roles in Azure RBAC)

Network contributor : Lets you manage networks, but not access to them.

upvoted 8 times

HOTSPOT -

You have the Azure resources shown on the following exhibit.



You plan to track resource usage and prevent the deletion of resources.

To which resources can you apply locks and tags? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Locks:

	▼
RG1 and VM1 only	
Sub1 and RG1 only	
Sub1, RG1, and VM1 only	
MG1, Sub1, RG1, and VM1 only	
Tenant Root Group, MG1, Sub1, RG1, and VM1	

Tags:

	▼
RG1 and VM1 only	
Sub1 and RG1 only	
Sub1, RG1, and VM1 only	
MG1, Sub1, RG1, and VM1 only	
Tenant Root Group, MG1, Sub1, RG1, and VM1	

Answer Area

Locks:

▼

RG1 and VM1 only

Sub1 and RG1 only

Sub1, RG1, and VM1 only

MG1, Sub1, RG1, and VM1 only

Tenant Root Group, MG1, Sub1, RG1, and VM1

Correct Answer:

Tags:

▼

RG1 and VM1 only

Sub1 and RG1 only

Sub1, RG1, and VM1 only

MG1, Sub1, RG1, and VM1 only

Tenant Root Group, MG1, Sub1, RG1, and VM1

Box 1: Sub1, RG1, and VM1 only -
You can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

Box 2: Sub1, RG1, and VM1 only -
You apply tags to your Azure resources, resource groups, and subscriptions.

Reference:
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json>

- GepeNova

Highly Voted

3 years, 7 months ago

Correct answer.
Only can assign locks and tags to subscriptions, resource groups and resources. Tested in lab
upvoted 116 times
- atspace

2 years, 6 months ago

Tenant parent group also a subscription so answer should be the last choice?
upvoted 1 times
- xRiot007

1 year, 11 months ago

The tenant parent group is an MG, not a Sub.
upvoted 3 times
- Omar_Aladdin

Highly Voted

3 years, 7 months ago

Answer is correct, both Tags and Locks are available to Subscriptions, Resource Groups, and Resources..

See FIRST Paragraph in both Refs
Ref Locks:
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>
Ref Tags:
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json>
upvoted 35 times
- Chuong0810

Most Recent

6 months, 1 week ago

Locks: Tenant Root Group, MG1, Sub1, RG1, and VM1:
Explanation: Locks can be applied at all resource levels to prevent accidental deletion or modification.

Tags: Tenant Root Group, MG1, Sub1, RG1, and VM1:
Explanation: Tags can be applied to all resource levels to track and manage resource usage effectively.
From Copilot.
upvoted 2 times
- Ivanvazovv

1 month, 3 weeks ago

Each time I see "Copilot", I know the answer will be incorrect because AI simply invents information that is not true. Such as this case.
upvoted 1 times
- zeuge

4 months, 3 weeks ago

Stop using Copilot, ChatGPT, etc. This answer is nonsense. Referenz-Tags: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json> "Tag usage and recommendations

You can apply tags to your Azure resources, resource groups, and subscriptions, but not to management groups."

upvoted 5 times

🗳️ 👤 **[Removed]** 8 months ago

correct

upvoted 3 times

🗳️ 👤 **Charumathi** 10 months, 3 weeks ago

Correct Answer,

Locks: Sub1, RG1 and VM1 only

Tags: Sub1, RG1 and VM1 only

Here is the explanation and reference,

Locks: you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>

Tags: You can apply tags to your Azure resources, resource groups, and subscriptions.

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources>

upvoted 4 times

🗳️ 👤 **3c5adce** 11 months, 4 weeks ago

ChatGPT4:

- Correct Answer for Locks might be best as "Sub1, RG1, and VM1 only" if you want to protect specific resources and the subscription itself.
- Correct Answer for Tags is correctly "Tenant Root Group, MG1, Sub1, RG1, and VM1" as tags need to be applied at each level you want them to be accounted for.

upvoted 1 times

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

Given answer is correct

upvoted 1 times

🗳️ 👤 **Rams_84z06n** 2 years, 1 month ago

tested it. Given answer is correct

upvoted 3 times

🗳️ 👤 **zellck** 2 years, 3 months ago

1. Sub1, RG1, and VM1 only

2. Sub1, RG1, and VM1 only

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources>

Tags are metadata elements that you apply to your Azure resources. They're key-value pairs that help you identify resources based on settings that are relevant to your organization. If you want to track the deployment environment for your resources, add a key named Environment. To identify the resources deployed to production, give them a value of Production. Fully formed, the key-value pair becomes, Environment = Production.

You can apply tags to your Azure resources, resource groups, and subscriptions.

upvoted 4 times

🗳️ 👤 **majerly** 2 years, 7 months ago

Today in exam

1) Locks: "Sub1, RG1, and VM1 only"

2) Tags: "Sub1, RG1, and VM1 only"

upvoted 13 times

🗳️ 👤 **NaoVaz** 2 years, 7 months ago

1) Locks: "Sub1, RG1, and VM1 only"

2) Tags: "Sub1, RG1, and VM1 only"

Locks and tags can only be assigned to Subscriptions, Resource Groups or Resources.

upvoted 4 times

🗳️ 👤 **libran** 2 years, 8 months ago

Correct Answer -

Locks: Sub1, RG1, and VM1 only

Tags: Sub1, RG1, and VM1 only

upvoted 1 times

🗳️ 👤 **EmnCours** 2 years, 8 months ago

Locks: Sub1, RG1, and VM1 only

Tags: Sub1, RG1, and VM1 only

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>



<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json>

upvoted 3 times

  **rolling_potato_** 3 years, 2 months ago

Something like this came up in the exam March 4 2022. The difference was that you had to indicate which objects could be applied to the policy and which could be excluded from it.

upvoted 1 times

  **zr79** 3 years, 2 months ago

Tags are not inherited from the parent unlike the locks

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json#inherit-tags>

upvoted 1 times

  **WS_21** 3 years, 2 months ago

Locks: Sub1, RG1, and VM1 only

Tags: Sub1, RG1, and VM1 only

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json>

upvoted 1 times

  **Azure_daemon** 3 years, 2 months ago

both answers are correct, you can only assign tags and locks to Subscriptions, Resource groups and resources

upvoted 1 times



You have an Azure Active Directory (Azure AD) tenant.
You plan to delete multiple users by using Bulk delete in the Azure Active Directory admin center.
You need to create and upload a file for the bulk delete.
Which user attributes should you include in the file?


- A. The user principal name and usage location of each user only
- B. The user principal name of each user only
- C. The display name of each user only
- D. The display name and usage location of each user only
- E. The display name and user principal name of each user only

Correct Answer: B

Community vote distribution

B (100%)



-   **Mazinger**


Highly Voted 

 7 months, 2 weeks ago

Selected Answer: B

To perform a bulk delete of users in Azure Active Directory, you need to create and upload a CSV file that contains the list of users to be deleted. The file should include the user principal name (UPN) of each user only. Therefore, the answer is B. The user principal name of each user only. When you use the bulk delete feature in the Azure Active Directory admin center, you need to specify the UPN for each user that you want to delete. The UPN is a unique identifier for each user in Azure AD and is the primary way that Azure AD identifies and manages user accounts. Including additional attributes like the display name or usage location is not required for the bulk delete operation, as the UPN is the only mandatory attribute for the user account. However, you may include additional attributes in the CSV file if you want to keep track of the metadata associated with each user account.

upvoted 30 times
-   **NaoVaz**



Highly Voted 


 2 years, 7 months ago

Selected Answer: B

B) "The user principal name of each user only "

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete#csv-template-structure>



upvoted 11 times
-   **Flip46**

Most Recent 

 2 months, 1 week ago



Selected Answer: B

location Home > Standardmap | Users > Bulk operations > Bulk delete.
Create a csv file with User name [userPrincipalName] Required

upvoted 1 times
-   **minura** 7 months, 1 week ago



Selected Answer: B

The UPN is the unique identifier for each user within the directory and is necessary to specify the correct users for deletion. When performing a bulk delete operation in Azure AD, the system requires only the user principal name (UPN) to identify the users you want to delete.

upvoted 1 times
-   **[Removed]** 8 months ago



Selected Answer: B

B is corerct

upvoted 1 times
-   **3c5adce** 12 months ago

B. The user principal name of each user only.

The user principal name (UPN) uniquely identifies each user in Azure AD. It is commonly used as the primary identifier for user-related operations, including deletion. When performing a bulk delete, including the UPN of each user is essential for accurately identifying and deleting the intended users.

upvoted 1 times
-   **Amir1909** 1 year, 2 months ago

B is correct

upvoted 1 times

- ric2020

1 year, 3 months ago

I ran a test for this and the result is:
1. NO: RG1 will have tag2:it policy at the subscription level, it is not applied to resource groups, only to the subscription resources.
2. NOT: tag3:value1 and tag4:value4
3. NO: tag3:value2 only since it is excluded
upvoted 1 times
- AK4U_111

2 years, 2 months ago

If they were all that easy
upvoted 1 times
- zellck

2 years, 3 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete#to-bulk-delete-users

The only required value is User principal name.

upvoted 2 times
- brein33

2 years, 3 months ago

B is the correct answer
upvoted 1 times
- majerly

2 years, 7 months ago

today in exam is B
upvoted 7 times
- jesusalex1s

2 years, 7 months ago

answer B. only user principal name of each user only

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete#csv-template-structure

upvoted 1 times
- qwerty100

2 years, 8 months ago

Selected Answer: B

The rows in a downloaded CSV template are as follows:
Version number: The first row containing the version number must be included in the upload CSV.
Column headings: User name [userPrincipalName] Required. Older versions of the template might vary.
Examples row: We have included in the template an example of an acceptable value. Example: chris@contoso.com You must remove the example row and replace it with your own entries.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete

upvoted 2 times
- DeltaSM

2 years, 8 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times
- libran

2 years, 8 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times
- EmnCours

2 years, 8 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

HOTSPOT -

You have an Azure subscription named Sub1 that contains the Azure resources shown in the following table.

Name	Type
RG1	Resource group
storage1	Storage account
VNET1	Virtual network

You assign an Azure policy that has the following settings:

- ⇒ Scope: Sub1
- ⇒ Exclusions: Sub1/RG1/VNET1
- ⇒ Policy definition: Append a tag and its value to resources
- ⇒ Policy enforcement: Enabled
- ⇒ Tag name: Tag4
- ⇒ Tag value: value4

You assign tags to the resources as shown in the following table.

Resource	Tag
Sub1	Tag1:subscription
RG1	Tag2:IT
storage1	Tag3:value1
VNET1	Tag3:value2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
RG1 has the Tag2 : IT tag assigned only	<input type="radio"/>	<input type="radio"/>
Storage1 has the Tag1 : subscription, Tag2 : IT, Tag3 : value1, and Tag4 : value4 tags assigned.	<input type="radio"/>	<input type="radio"/>
VNET1 has the Tag2 : IT and Tag3 : value2 tags assigned only	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
RG1 has the Tag2 : IT tag assigned only	<input type="radio"/>	<input checked="" type="radio"/>
Storage1 has the Tag1 : subscription, Tag2 : IT, Tag3 : value1, and Tag4 : value4 tags assigned.	<input type="radio"/>	<input checked="" type="radio"/>
VNET1 has the Tag2 : IT and Tag3 : value2 tags assigned only	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -
The Azure Policy will add Tag4 to RG1.

Box 2: No -

Tags applied to the resource group or subscription aren't inherited by the resources although you can enable inheritance with Azure Policy.

Storage1 has Tag3:

Value1 and the Azure Policy will add Tag4.

Box 3: No -

Tags applied to the resource group or subscription aren't inherited by the resources so VNET1 does not have Tag2.

VNET1 has Tag3:value2. VNET1 is excluded from the Azure Policy so Tag4 will not be added to VNET1.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json>

  **Lionred**  3 years, 4 months ago

N, N, N

1st No: Azure policy was created before the RG1 was assigned tag, which means when RG1 was manually assigned tag Tag2:IT, the policy will take action to append Tag4:vaule4 to RG1. Note that policy action is to "append", that means whatever else tag RG1 is given won't be taken away. As such RG1 will have two tags, Tag2:IT and Tag4:value4

2nd No: Remember tags are not inheritable, whatever tag assigned to RG1 won't be applied to any resources under it. As such the Storage1 should be Tag3:value1 and Tag4:vaule4.

3rd No: vNet1 is excluded from the Azure policy, hence the policy won't do anything to it. As such vNet1 should only have the tag manually assigned: Tag3:value2. PS, I take that "Exclusions: Sub1/RG1/VNET1" does not mean both RG1 & vNet1 are excluded, only vNet1 is excluded, the Sub1/RG1/VNET1 is merely a path to the object that is excluded.

upvoted 232 times

  **DalyMasmoudi** 5 months ago

The Azure Policy is assigned to add the tag Tag4:value4 to resources in a subscription Sub1, except for VNET1. However, the policy does not apply to existing resources because remediation (auto-correction) is not enabled.

So the correct Answer is:

Y: RG1 has the Tag2:IT tag assigned only

Reason: RG1 receives the tag Tag2:IT because it is explicitly assigned in the policy and is not affected by the exclusion.

N: Storage1 has the Tag1:subscription, Tag2:IT, Tag3:value1, and Tag4:value4 tags assigned.

Reason: Although Storage1 has several tags assigned, the policy does not apply to this existing resource because remediation is not enabled.

N: VNET1 has the Tag3:value2 assigned only.

Reason: VNET1 is excluded from the policy, so no tags are assigned to this resource.

upvoted 9 times

  **S3ktar** 3 years, 4 months ago

Not true, if the RG1 exists before the policy is in place, it will not apply the tags. This is even true if you go into the resource to add the tags as mentioned in the question, it will not apply the policy rules just because you are adding a tag. The result of this will be that the resources will only be tagged as not compliant until it is fixed.

Source: I tested it in the portal

upvoted 33 times

  **S3ktar** 3 years, 4 months ago



Correct answer is y-n-n

upvoted 60 times

  **marioZuo** 1 year, 9 months ago


I tested also, but the tag is appended automatically on my side.

upvoted 3 times

  **mufflon** 3 years, 3 months ago

Are you sure? When you are updating the resources with tags according to "You assign tags to the resources as shown in the following table" then , dont you update the resource and the policy activates? A policy adds the by the policy specified tag and value when any resource missing the tag is created or updated, so it vill add Tag4 with value: value4

upvoted 2 times

  **albergd** 3 years, 2 months ago

The trick is not there, the trick is in the policy: "Append a tag and its value to resources" : this policy does not apply to Resource Groups.

You can check here: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

To apply the policy to a RG you need to use "Append a tag and its value to resource groups".



The answer is Y-N-N

upvoted 75 times

  **Abdou001** 2 years, 2 months ago


@Albergd, you convinced me. Thanks !

upvoted 3 times

  **dimsok** 2 years, 3 months ago



Y-N-N, RG1 is exluded



upvoted 24 times



  **happpieee** 6 months, 1 week ago




Y-N-N.
This is correct. RG1 is excluded in the Azure policy (I am guessing the questions is tweaked here and there over time).



And tags does not inherits for the remaining: <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json#inherit-tags>
upvoted 3 times



  **Mshaty** 7 months, 1 week ago
RG1 is not excluded what is excluded Vnet1 which is in RG1
upvoted 4 times



  **Ponpon3185** 2 months ago
Exclusions: Sub1/RG1/VNET1 So RG1 is excluded
upvoted 1 times



  **juniorccs** 2 years, 11 months ago
this is just wron
upvoted 1 times



  **testmobile18** Highly Voted  3 years, 4 months ago
Wouldn't it be Y-N-N?
Y - RG1 is excluded thus retain as it is
N - Storage1 will have Tag3:value1 and Tag4:value4
N - VNET1 is excluded as well so only have Tag3:value2
upvoted 134 times




  **gofto** 3 years, 4 months ago
doubt that this explanation is correct
upvoted 4 times



  **Edward2021** 3 years, 4 months ago
I think the same!!! Y N N
upvoted 10 times

  **olsenOnS** 3 years, 4 months ago
Correct,
Y - RG1 has its own tag, and is excluded from policy
N
N
upvoted 8 times

  **maatksle** 3 years, 4 months ago
Dude, you're wrong. Please refer to Lionred's answer. RG1 has already a tag to it and the policy appends the tag not take away and add. Guys, please upvote his answer.
upvoted 9 times

  **mufflon** 3 years, 3 months ago
First you have the resources specified, they you assign a policy that says Tag name: Tag4 and Tag value: value4.
Then you assign tags to the resources as shown in the table.
When assigning tags to the resources, the resources gets updated and the policy gets activated and adds its tag.
<https://www.examttopics.com/exams/microsoft/az-104/view/9/#>
upvoted 1 times

  **manishk39** Most Recent  3 months, 2 weeks ago
NNN, Appends the specified tag and value when any resource which is missing this tag is created or updated. Does not modify the tags of resources created before this policy was applied until those resources are changed. Does not apply to resource groups.
upvoted 1 times

  **bacana** 6 months ago
YNN
Police only add tags if you set the remediation option. Tags remain the same whether the police apply them or not. Test it out if you don't believe me
upvoted 2 times



  **stcr** 6 months ago
Y, N, N

Append a tag and its value to resources Appends the specified tag and value when any resource which is missing this tag is created or updated. Does not modify the tags of resources created before this policy was applied until those resources are changed. Does not apply to resource groups. New 'modify' effect policies are available that support remediation of tags on existing resources (see <https://aka.ms/modifydoc>).



<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>



So this policy
- never applies to resource groups
- Exclusion: "Optionally select resources to exclude from the policy assignment."



- the resource group is already there
By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.
upvoted 3 times

  **LinuxLewis** 6 months, 1 week ago
NO --- RG1 created > policy with scope Sub1 assigned > path excludes only VNET1 > so RG1 is a resource of Sub1 > tag2+tag4
NO --- storage created > carries tag3 > tag4 policy enforced > other tags are not inherited
NO --- VNET1 is excluded > no tag4 > only tag3 remains



my thoughts...
upvoted 1 times

  **rodrod** 6 months, 1 week ago
how can it be a path and not a list??
a path would be /subscriptions/Sub1/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1
very confusing...
upvoted 1 times

  **feralberti** 6 months, 2 weeks ago
there seems to be alot of confusion on the first options: i believe it to be a N. RG1 is not excluded from the policy and the policy will add Tag4 to the already existing Tag2. The policy ONLY excludes Vnet1
upvoted 1 times

  **[Removed]** 8 months ago
Wrong

Yes
No
No
upvoted 3 times

  **ELearn** 8 months ago
1) RG1 has the Tag2: IT tag assigned only.



Since RG1 is not excluded and the policy applies to all resources in Sub1, the policy will add Tag4: value4 to RG1. So, RG1 will have Tag2: IT and Tag4: value4.
Answer: No

2) storage1 has the Tag1: subscription, Tag2: IT, Tag3: value1, and Tag4: value4 tags assigned.



storage1 is under the Sub1 and not excluded from the policy. Initially, it has Tag3: value1. The policy will append Tag4: value4.
It is not specified that Tag1: subscription or Tag2: IT is applied to storage1. Only the tags mentioned in the table and policy enforcement apply.
Answer: No



3) VNET1 has the Tag2: IT and Tag3: value2 tags assigned only.

VNET1 is specifically excluded from the policy. It already has Tag3: value2 and no other tags from the table or policy are applied.
There is no mention of Tag2: IT being assigned to VNET1.
Answer: No
upvoted 2 times



  **ELearn** 8 months ago
NB: The forward slashes in the exclusion path "Sub1/RG1/VNET1" indicate a hierarchical relationship, not separate exclusions. This format specifies that the exclusion applies to the VNET1 resource located within the RG1 resource group, under the Sub1 subscription.

So, it does not exclude Sub1 or RG1 independently. It only excludes the specific resource VNET1, ensuring that only this virtual network is unaffected by the policy.
upvoted 3 times


  **CheMetto** 9 months, 1 week ago
YNN! Remember: Even if enforce policy might think is enforced for everything, it doesn't mean this way! To apply a tag to pre-existence resource with azure policy, the only way is to do a remediation task, nothing else. The meaning of enforce policy is what azure policy will do. In this case, if you disable enforce policy it will put the resource in "Non compliant state" and send a custom message. If you enable enforce policy, it will force what it has to do, so in this case apply a tag.
upvoted 2 times

  **OpOmOp** 10 months ago
I dont know why subs1 will get tag4.

When you assign the policy you have this warning:
By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned
upvoted 1 times

  **2dc6125** 11 months ago
Y,n,n. IT tag already exists and policy has append action so will not remove the existing tag

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

ChatGPT4 - NNY
upvoted 1 times

  **Wassel_Laouini** 1 year ago

Y-N-N, the policy excluded RG1, meaning it has no tag(the tag4), all good now? then it said you assign a tag1 to RG1, which you can because it has nothing to do with the policy
upvoted 1 times

  **mkhliszf** 1 year, 1 month ago

Two things to notice:
"Sub1/RG1/VNET1" reads as a path not a list, so it only applies to VNET1 and not RG1 and Sub1

The tag does not apply to RG1 because it is a resource group and the policy specifies "Append a tag and its value to resources" so it will only apply to resources, no resource groups.

Therefore, answer is.

Y
N
N

upvoted 5 times


  **promartyr** 1 year, 1 month ago

"Exclusions: Sub1/RG1/VNET1":

IT MEANS : "the virtual network called VNet1 (which is inside Resource Group RG1, and inside Subscription called Sub1) is excluded from the policy"

IT DOES NOT MEAN: "Sub1 _and_ RG1 _and_ VNet1 are excluded from the policy"

upvoted 18 times

  **HichemCFE** 4 months, 1 week ago

yes but the policy :tag append only resource :
y,n,n
upvoted 1 times

  **Aadhithya** 1 year ago

This is the best explanation for the exclusion criteria
upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Traffic Manager Contributor role at the subscription level to Admin1.



Does this meet the goal?


- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (98%)

-   **GoldenFox**

Highly Voted 



 3 years, 4 months ago

Q.36
Assign Network Contributor role at subscription level to Admin1 ☐ Yes



Q.37
Assign Owner role at subscription level to Admin1 ☐ Yes

Q.38
Assign Reader role at subscription level to Admin1 ☐ Yes



Q.52
Assign Traffic Manager Contributor role at subscription level to Admin1 ☐ No

upvoted 262 times
-   **scottytohotty** 8 months, 2 weeks ago



This is the way.

upvoted 3 times
-   **maatksle** 3 years, 4 months ago



Are you sure on Q.38 - reader role can only access not enable traffic analytics

upvoted 16 times
-   **mmtechsolutionsinc** 3 years, 2 months ago

yes,
Your account must meet one of the following to enable traffic analytics:
Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.
Reference:
<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

upvoted 6 times
-   **DarkAngel76** 3 years, 1 month ago



It looks like there's an error in that Microsoft Docs page as per issue published on GitHub at <https://github.com/MicrosoftDocs/azure-docs/issues/77499>.

upvoted 19 times
-   **edd004** 1 year, 10 months ago



Yes agree with @DarkAngel76, They already fixed it. Check it at:
<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

"Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, or network contributor."



So Q.38 ans is NO!

upvoted 15 times
-   **flyingcolours87** 1 year, 10 months ago

This link is now updated. The reader role is not in the list anymore.
Ref: <https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

upvoted 7 times
-   **ABhi101** 3 years, 3 months ago

GoldenFox is correct

upvoted 5 times
-   **jackAttew_1** 3 years, 4 months ago

So answer is No. Read this => <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#traffic-manager-contributor>
upvoted 6 times

  **Marski** Highly Voted 3 years, 3 months ago


Clever cheat question by MS. You need to know. Got to know. These are traps. I dont like these anyway.
upvoted 27 times

  **4f45fce** Most Recent 2 weeks, 4 days ago

Selected Answer: B

No, this solution does not meet the goal. To enable Traffic Analytics for an Azure subscription, Admin1 requires the Network Contributor role at the subscription level—not the Traffic Manager Contributor role. The Network Contributor role provides the necessary permissions to manage network resources, including enabling Traffic Analytics.

upvoted 1 times

  **Jakub4444** 2 months, 3 weeks ago

Selected Answer: B

No, assigning the Traffic Manager Contributor role at the subscription level does not meet the goal.

The Traffic Manager Contributor role allows managing Azure Traffic Manager, which is used for DNS-based traffic routing. However, it does not provide the necessary permissions for enabling Traffic Analytics.

upvoted 3 times

  **allinict_111** 5 months, 1 week ago

Network Contributor: Required for enabling Traffic Analytics.

Traffic Manager Contributor: Manages Traffic Manager profiles and configurations, but not specific to Traffic Analytics.

upvoted 1 times

  **dilopezat** 5 months, 2 weeks ago

Selected Answer: B



To enable Traffic Analytics for an Azure subscription, you need to have one of the following Azure built-in roles assigned to your account:

Owner
Contributor
Network contributor
Monitoring contributor

https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics?wt.mc_id=knwlserapi_inproduct_azportal#prerequisites

https://learn.microsoft.com/en-us/azure/network-watcher/required-rbac-permissions?wt.mc_id=knwlserapi_inproduct_azportal#traffic-analytics

upvoted 4 times

  **RVivek** 5 months, 3 weeks ago

Selected Answer: B

To enable Traffic manager one of there three RBAC reuired 1 Owner 2. Contributor 3. Network contributor 1 and Monitoring contributor 2

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites>

upvoted 3 times

  **ricardona** 7 months, 2 weeks ago


No, assigning the Traffic Manager Contributor role to Admin1 at the subscription level will not meet the goal of enabling Traffic Analytics for the Azure subscription.

The Traffic Manager Contributor role only grants permissions to manage Traffic Manager profiles, endpoints, and traffic routing methods, but it does not provide the necessary permissions to enable Traffic Analytics for the Azure subscription.

To enable Traffic Analytics for an Azure subscription, you need to assign the Log Analytics Contributor role to the Azure AD user named Admin1. The Log Analytics Contributor role allows the user to manage Log Analytics workspaces, which is required to enable Traffic Analytics for the Azure subscription.

Therefore, assigning the Traffic Manager Contributor role to Admin1 will not meet the goal of enabling Traffic Analytics for the Azure subscription.

upvoted 2 times

  **ricardona** 7 months, 2 weeks ago

Selected Answer: B

No, assigning the Traffic Manager Contributor role to Admin1 at the subscription level will not meet the goal of enabling Traffic Analytics for the Azure subscription.

The Traffic Manager Contributor role only grants permissions to manage Traffic Manager profiles, endpoints, and traffic routing methods, but it does not provide the necessary permissions to enable Traffic Analytics for the Azure subscription.

To enable Traffic Analytics for an Azure subscription, you need to assign the Log Analytics Contributor role to the Azure AD user named Admin1. The Log Analytics Contributor role allows the user to manage Log Analytics workspaces, which is required to enable Traffic Analytics for the Azure subscription.

Therefore, assigning the Traffic Manager Contributor role to Admin1 will not meet the goal of enabling Traffic Analytics for the Azure subscription.

upvoted 12 times

🗳️ 👤 **esawormjr** 7 months, 2 weeks ago

No, assigning the "Traffic Manager Contributor" role to the user "Admin1" will not meet the goal of enabling Traffic Analytics for the Azure subscription. The "Traffic Manager Contributor" role is related to Azure Traffic Manager, which is a DNS-based traffic load balancer used to distribute traffic across multiple Azure services or endpoints in different data centers.

For enabling Traffic Analytics, you need to assign the appropriate role related to Azure Monitor and Log Analytics, not Traffic Manager. To achieve the goal, you should assign the "Log Analytics Contributor" or "Contributor" role at the subscription level to the user "Admin1". These roles grant permissions to manage and configure resources related to Azure Monitor, including Traffic Analytics.

Remember to always follow the principle of least privilege and only assign the necessary permissions to users based on their roles and responsibilities.

upvoted 14 times

🗳️ 👤 **[Removed]** 8 months ago

Selected Answer: B

B is corerct

upvoted 1 times

🗳️ 👤 **[Removed]** 7 months, 4 weeks ago

Owner & Network Contributor can enable Traffic Analytics

upvoted 1 times

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

Selected Answer: B

The Traffic Manager Contributor role does not provide the necessary permissions to enable Traffic Analytics for an Azure subscription. To enable Traffic Analytics, you need permissions to configure and access the logs and data associated with network traffic.

Required Role:

Network Contributor or a custom role with permissions to configure Traffic Analytics and access diagnostic settings is typically needed for managing Traffic Analytics configurations.

Explanation:

Traffic Manager Contributor Role: This role allows users to manage Traffic Manager profiles and endpoints but does not grant access to configure Traffic Analytics or manage diagnostic settings.

Correct Answer: B. No

upvoted 2 times

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

No is right

upvoted 1 times

🗳️ 👤 **LPaul** 1 year, 7 months ago

Please read carefully "Traffic Manager " Contributor nothing to do with "Traffic Analytics" , is 2 different service .

upvoted 4 times

🗳️ 👤 **Souban07** 1 year, 10 months ago

Selected Answer: B

The Traffic Manager Contributor role is specifically for managing Traffic Manager profiles and does not provide the necessary permissions to enable Traffic Analytics. Enabling Traffic Analytics requires the Network Contributor or higher role at the subscription level.

upvoted 3 times

🗳️ 👤 **zellck** 2 years, 3 months ago

Selected Answer: B

B is the answer.

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements>

One of the following Azure built-in roles needs to be assigned to your account:

- Owner
- Contributor
- Reader
- Network Contributor

upvoted 4 times

🗳️ 👤 **iDrewax** 1 year, 11 months ago

wrong, Reader Role is not correct. The rest is.

upvoted 3 times

🗳️ 👤 **naxer82** 2 years, 6 months ago

Hello here it says that the correct answer is NO. But in the

Question #33 Subject 2 says YES and in Question #49 Subject 2 says NO. Looking back, it's the same question. I'm a bit confused.

upvoted 2 times

🗳️ 👤 **rodolfodc** 2 years ago

If you read again Question #33 Subject 2, it says:
Solution: You assign the Network Contributor role at the subscription level to Admin1.

Current question says "Traffic Manager Contributor" as the Role (answer is NO), and the other one "Network Contributor" (in this case this role meets the criteria, answer is YES).

upvoted 1 times

You have three offices and an Azure subscription that contains an Azure Active Directory (Azure AD) tenant. You need to grant user management permissions to a local administrator in each office. What should you use?

- A. Azure AD roles
- B. administrative units
- C. access packages in Azure AD entitlement management
- D. Azure roles

Correct Answer: B

Community vote distribution

B (91%)

9%

- HananS**

Highly Voted

3 years, 4 months ago

The answer is correct
Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.
upvoted 53 times
- magichappens**

3 years, 1 month ago

Although I agree with your explanation the question is not really stating that administrative units are required as there is no statement about the local office administrators and weather they need to administer all users or should only administer the users of their respective office.
upvoted 18 times
- NaoVaz**

Highly Voted

2 years, 7 months ago

Selected Answer: B

B) "administrative units"

"It can be useful to restrict administrative scope by using administrative units in organizations that are made up of independent divisions of any kind."- <https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units#deployment-scenario>
upvoted 17 times

Ivanvazovv

Most Recent

1 month, 3 weeks ago

Selected Answer: A

"You need to grant user management permissions to a local administrator in each office"
Why are administrative units needed here? Why not simply assign an Entra role to one guy from each office?
upvoted 1 times

[Removed]

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times

JananiToo

1 year, 2 months ago

Why some YouTube videos say azure AD roles?
upvoted 2 times

af68218

1 year, 1 month ago

The wording of the question, "what should you choose," is equivalent to "what is the best answer?" AD roles would work, but they wouldn't be the best answer, given that the question mentions having local administrators, which could be grouped together for practicality. The youtube video, like me, probably missed that.
upvoted 3 times

Amir1909

1 year, 2 months ago

B is correct
upvoted 1 times

Rednevi

1 year, 7 months ago

Selected Answer: B

B. Administrative units

Administrative units in Azure AD allow you to organize and delegate administrative tasks to specific administrative units. You can assign specific permissions and roles to administrators based on these units. This approach allows local administrators to have control over users and resources within their respective offices without having full global permissions. It's a more granular and decentralized approach to user management.

Azure AD roles (Option A) typically deal with assigning permissions at a broader level, and they might not provide the necessary granularity for managing users within specific offices.

Access packages in Azure AD entitlement management (Option C) are used for granting access to resources and applications rather than delegating user management tasks.

Azure roles (Option D) are primarily focused on managing permissions for Azure resources and services, not user management within Azure AD.

So, the most suitable choice for delegating user management permissions to local administrators in different offices is "B. Administrative units."
upvoted 9 times

  **grimrodd** 1 year, 8 months ago

Selected Answer: A

I think A because, the question does not state that each local administrator should be restricted to only administer the users in their office, so assigning the role 'User Administrator' would be the solution to this question would it not?

upvoted 3 times

  **urbanmonk** 1 year, 7 months ago

Do not overthink these questions. The phrase "... Local administrator in each office" gave the answer away for Administrative Unit.



upvoted 3 times

  **kamalpur** 1 year, 9 months ago

answer is correct

<https://youtu.be/XNqSQOYtcPQ>

upvoted 1 times

  **Chris76** 2 years ago

Selected Answer: B

"You need to grant user management permissions to a local administrator in each office"

vs

"You need to grant *LOCAL* user management permissions to a local administrator in each office"

IMHO the latter is a stronger case for Administrative Units. But the mere fact of mentioning "Local administrator in each office", implies an already in place setup of Administrative Units. Location/Division - based admin is use case for Administrative Units.

upvoted 4 times

  **lokii9980** 2 years, 1 month ago

B. Administrative units would be the best option to grant user management permissions to a local administrator in each office.

Administrative units are a feature in Azure AD that allow you to delegate administrative privileges to specific groups of users or administrators. By creating an administrative unit for each office, you can grant the local administrator in each office the necessary permissions to manage users and groups within their own office, without giving them access to the entire Azure AD tenant.

Azure AD roles and Azure roles are used to grant permissions to perform specific tasks within Azure services, but they are not specifically designed for user management within Azure AD.

Access packages in Azure AD entitlement management are used to manage access to specific resources and applications within an organization, but they are not specifically designed for delegating administrative privileges.

upvoted 3 times

  **Mazinger** 2 years, 2 months ago

Selected Answer: B

To grant user management permissions to a local administrator in each office, you should use Azure AD administrative units.

Administrative units are a feature in Azure AD that allow you to delegate administrative permissions to specific groups of users or administrators.

You can create an administrative unit for each office and then assign a local administrator to manage the users and groups within that unit.

Azure AD roles, Azure roles, and access packages in Azure AD entitlement management are also used to grant permissions to users and groups, but they are not designed specifically for delegating administrative permissions to specific groups of users or administrators based on their location or organizational structure. Therefore, they are not the best option for granting user management permissions to local administrators in each office.

So, the correct answer is B. administrative units.

upvoted 5 times

  **allyQ** 2 years, 2 months ago

True, But the scenario says:



You need to grant user management permissions to a local administrator in each office.

Not....

You need to grant 'local' user management permissions to a local administrator in each office.

The answer assumes a scope that the question does not actually specify.

upvoted 5 times

  **Chris76** 2 years ago

Finally somebody sane with attention to details

upvoted 2 times

  **zellck** 2 years, 3 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

An administrative unit is an Azure AD resource that can be a container for other Azure AD resources. An administrative unit can contain only users, groups, or devices.

Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.

upvoted 3 times

  **brein33** 2 years, 3 months ago

Administrative units is correct

upvoted 1 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B 

Reference:



<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

upvoted 3 times

  **Azure_daemon** 3 years, 2 months ago

It's very obvious, Administrative Unit is the answer

upvoted 2 times

  **edengoforit** 3 years, 2 months ago

Answer is Administrative unit

If you go to portal.azure.com -> Azure Active Directory -> Roles and Administrators from the left pane, you will be able to see multiple built in role called 'User Administrator'. If you click that role, you are able to assign, update or delete the user to the role

upvoted 3 times



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev. You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group. Solution: On Dev, you assign the Logic App Contributor role to the Developers group. Does this meet the goal?


- A. Yes
- B. No

Correct Answer: A

Community vote distribution

A (58%)B (42%)

-  **MrMacro**



Highly Voted 

 3 years, 4 months ago



Answer "Yes" is correct. Logic App Contributor role will allow you to create Logic Apps.

See here: <https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app?tabs=azure-portal>



"Your Azure subscription requires Contributor permissions for the resource group that contains that logic app resource. If you create a logic app resource, you automatically have Contributor access."

upvoted 67 times
-  **youngjanpawel** 3 months, 3 weeks ago



Logic App Contributor - Lets you manage logic app, but not access to them
Logic App Operator - Lets you read, enable and disable logic app
Description from access control (IAM)

upvoted 3 times
-  **2d153f5** 5 months, 3 weeks ago



Contributor is needed.

upvoted 2 times
-  **itguy2** 3 years, 1 month ago



ANSWER: B
Contributor and Logic App Contributor are different...from your link
Logic App Contributor: Lets you manage logic apps, but you can't change access to them.
Logic App Operator: Lets you read, enable, and disable logic apps, but you can't edit or update them.
Contributor: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

upvoted 21 times
-  **sca88** 5 months, 3 weeks ago



The question talk about create Logic App. So Logic App Contributor Role it's enough


upvoted 4 times
-  **klasbeatz** 2 years, 7 months ago

Microsoft doesn't say it directly on site so I thought the same they almost present as of Contributor and Logic app contributor are different

upvoted 1 times
-  **MeysamBayani** 2 years, 3 months ago



in dev resource group you can create a logic app. when you try create logic app in this RG change plane type to consumption

upvoted 2 times
-  **Emre_jm**

Highly Voted 

 2 years, 6 months ago

Tested today, gave "Logic App Contributor" role to a user account. During Logic App creation phase got error under RG selection: "You cannot perform this action without all the following permissions (Microsoft.Storage/storageAccounts/write, Microsoft.Web/ServerFarms/write, Microsoft.Web/Sites/write"

upvoted 18 times
-  **LuLaCeK** 6 months, 1 week ago

Tested as well, got the same error.

upvoted 3 times

  **Ivanvazovv** Most Recent 1 month, 3 weeks ago

Selected Answer: A

Logic App Contributor gives action "Microsoft.Logic/*" so creating should be possible.



upvoted 1 times

  **BUDSENA** 1 month, 3 weeks ago

Selected Answer: B

You need contributor

upvoted 1 times

  **digitalcoder** 2 months, 1 week ago

Selected Answer: B

No, assigning the Logic App Contributor role to the Developers group does not meet the goal.

The Logic App Contributor role allows users to manage existing logic app workflows, but it does not provide permissions to create new logic apps. To enable the Developers group to create Azure logic apps in the Dev resource group, you would need to assign a role with broader permissions, such as the Contributor role, which grants full access to manage all resources within the resource group, including creating and managing logic apps

upvoted 3 times

  **Jay_D_Lincoln** 3 months ago

Selected Answer: A


The Logic App Contributor role allows users to:

✓ Create, edit, and delete logic apps.

✓ Manage triggers, workflows, and actions.

✗ Cannot assign roles or manage security settings (needs Owner or User Access Administrator role for that).

upvoted 1 times

  **Bambi0074** 3 months, 2 weeks ago

Selected Answer: A

Depends on the hosting option. Tested in Environment.

Consumption: YES

Standard: NO

upvoted 1 times

  **youngjanpawel** 3 months, 3 weeks ago

Logic App Contributor - Lets you manage logic app, but not access to them

Logic App Operator - Lets you read, enable and disable logic app

Description from access control (IAM)

upvoted 1 times

  **dazzle2013** 4 months, 1 week ago

Selected Answer: B

you need to have contributor role to be able to create a new logic app. with logic app contributor, you can only manage the existing ones

upvoted 3 times

  **sca88** 5 months, 3 weeks ago

Selected Answer: A

Logic App Contributor role allow to create Logic App, but not to use it. If you want to allow to use Logic App, you need to assign Logic App Operator role. The question talk about create Logic App, so A should be correct



upvoted 1 times

  **Xpinguser** 6 months, 3 weeks ago

Selected Answer: A

Logic App Contributor role: This role grants the necessary permissions to create, manage, and deploy logic apps within a resource group.

upvoted 1 times

  **jamesf** 6 months, 3 weeks ago

Selected Answer: A

A correct

Logic App Contributor & Contributor can create logical apps

upvoted 1 times

  **[Removed]** 7 months, 3 weeks ago

Selected Answer: A

A is correct

Logic App Contributor & Contributor can create logical apps

upvoted 1 times

  **asaulu** 8 months, 3 weeks ago

Microsoft.Resources/deployments/* Create and manage a deployment ... Means Logic App Contributor can create a logic app
upvoted 1 times

  **Carmen_Ms** 9 months ago

Tested! The answer is A, you can create logic apps but only of the consumption type. So the objective is fulfilled. All those who say the B, you have not tested it correctly.
upvoted 4 times



  **etrop** 9 months ago

Yeah I applied the Logic App Contributor role at the resource group level for a test user, then attempted to create a logic app. As long as the resource provider Microsoft.Web is registered already (For this question we can assume it is) then you can create logic apps of consumption type. If you want to create other types you need a few other perms (Microsoft.Storage/storageAccounts/write, Microsoft.Web/ServerFarms/write, Microsoft.Web/Sites/write)
upvoted 1 times

  **DevopsRock** 9 months ago

Selected Answer: A

Answer is A
upvoted 3 times

  **a6bd45e** 9 months, 2 weeks ago

Selected Answer: B

In Azure, the Logic App Contributor role does not inherently have the permissions to create new logic apps. The Logic App Contributor role allows users to manage logic apps but not create them. Specifically, this role includes permissions to read, write, and delete logic apps, but it lacks the permission required to create new ones, which is part of the broader Logic App Operator role or higher.

To create new logic apps, users generally need either the Logic App Operator role or a custom role with the following specific permission: Microsoft.Logic/workflows/write. This permission is necessary to create logic apps and is included in the Logic App Operator role or higher-level roles like Contributor or Owner.
upvoted 2 times

HOTSPOT -

You have an Azure Load Balancer named LB1.

You assign a user named User1 the roles shown in the following exhibit.

User1 assignments – LB1

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (2) ⓘ

Role	D..	Scope	Group assignment
User Access Administrator	L...	This resource	--
Virtual Machine Contributor	L...	Resource group (inherited)	--

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1 can [answer choice] LB1.

delete

create a NAT rule for

assign access to other users for

User1 can [answer choice] the resource group.

delete a virtual machine from

modify the load balancing rules in

deploy an Azure Kubernetes Service (AKS) cluster to

Correct Answer:

Answer Area

User1 can [answer choice] LB1.

delete

create a NAT rule for

assign access to other users for

User1 can [answer choice] the resource group.

delete a virtual machine from

modify the load balancing rules in

deploy an Azure Kubernetes Service (AKS) cluster to

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor> <https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

- 1) User1 can "assign access to other users for" LB1.
2) User1 can "delete a virtual machine from" the resource group.

The Role assignments say it all.

upvoted 102 times

  **Rogit** Highly Voted  1 year, 9 months ago

Was in test yesterday

upvoted 12 times

  **rteinformatica** 1 year, 9 months ago

A lot of questions came out of here? Would they arrive to approve?

upvoted 1 times

  **behradclid** Most Recent  8 months ago

answer is absolutely correct

upvoted 1 times

  **[Removed]** 8 months ago

correct

upvoted 3 times

  **tashakori** 1 year, 1 month ago

Given answer is right

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

Correct

upvoted 1 times

  **SkyZeroZx** 1 year, 4 months ago

- 1) User1 can "assign access to other users for" LB1.
2) User1 can "delete a virtual machine from" the resource group.



The Role assignments say it all.

upvoted 1 times

  **nmnm22** 1 year, 7 months ago

i wish all questions were as simple as this

upvoted 5 times

  **zellck** 2 years, 3 months ago

1. assign access to other users
2. delete a VM

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>

Lets you manage user access to Azure resources.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>



Create and manage virtual machines, manage disks, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you to assign roles in Azure RBAC.

upvoted 8 times

  **LiamAzure** 2 years, 6 months ago

Its Correct

upvoted 5 times

  **ECNS** 2 years, 7 months ago

Answer is CORRECT

upvoted 5 times

  **EmnCours** 2 years, 8 months ago

Answer is CORRECT

upvoted 4 times

  **vetrivelm** 3 years ago

Both Answer is correct.

Contributer-Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

upvoted 1 times

  **arodman** 3 years ago

Correct

upvoted 2 times

  **Pasmo** 3 years ago

Correct Answer
upvoted 1 times

  **AzureDev777** 3 years ago

Answer is correct
upvoted 1 times

  **epomatti** 3 years ago

Answer provided is correct.
upvoted 1 times

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1. Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users. What should you do?

- A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the Owner role for VNet1.
- C. Assign User1 the Contributor role for VNet1.
- D. Assign User1 the Network Contributor role for VNet1.

Correct Answer: B

Community vote distribution



B (97%)



  **MentalG** Highly Voted 3 years ago
B. Owner correct



Owner = Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Contributor = Grants full access to manage all resources, but does NOT allow you to assign roles in Azure RBAC. (you cannot add users or changes their rights)
User Access Administrator = Lets you manage user access to Azure resources.
Reader = View all resources, but does not allow you to make any changes.
Security Admin = View and update permissions for Security Center. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations.
Network Contributor = Lets you manage networks, but not access to them. (so you can add VNET, subnet, etc)
upvoted 59 times



  **NaoVaz** Highly Voted 2 years, 7 months ago
Selected Answer: B
B) "Assign User1 the Owner role for VNet1."

From the provided options, only the Owner role scoped at the resource level gives the ability to assign other roles to other users.
upvoted 6 times

  **b411470** Most Recent 5 months, 1 week ago
Selected Answer: B
Anything with 'Contributor' in the role cannot do anything with users.
upvoted 2 times

  **[Removed]** 8 months ago
Selected Answer: B
B is corerct
upvoted 1 times

  **Jedi_sg2000** 11 months, 3 weeks ago
<https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced#limitations-and-known-issues>
The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE.
upvoted 1 times

  **3c5adce** 12 months ago
D. Assign User1 the Network Contributor role for VNet1.

Explanation:

Assigning User1 the Network Contributor role for VNet1 would enable them to assign the Reader role for VNet1 to other users. The Network Contributor role grants permissions to manage network resources, including the ability to assign roles within the scope of the virtual network (VNet1). This role aligns with the requirement to allow User1 to assign the Reader role for VNet1 to other users.
upvoted 1 times

  **kijoksip** 1 year, 1 month ago

This is what ChatGPT says:

To ensure that User1 can assign the Reader role for VNet1 to other users, you should assign User1 the "Network Contributor" role for VNet1. This role grants the necessary permissions to manage all aspects of virtual networks, including assigning roles to other users.

So, the correct action is:

D. Assign User1 the Network Contributor role for VNet1.

upvoted 2 times

  **Jay_D_Lincoln** 3 months ago

This is why we should not blindly trust AI as reference.
--- Only owners or User Access Administrators can assign roles to other users. ---
upvoted 1 times

  **Rednevi** 1 year, 7 months ago

Selected Answer: B

the Contributor role in Azure does not have the permission to assign roles to other users or manage access control for other users. The Contributor role can perform actions such as creating, modifying, and deleting resources within the scope of a resource group or subscription, but it cannot manage access control.

To grant the ability to assign roles and manage access control for Azure resources, you would typically need to assign the User Access Administrator or Owner roles to a user or group. These roles have the necessary permissions to manage access control, including the assignment of roles to other users.

upvoted 4 times

  **Codelawdepp** 1 year, 8 months ago

Selected Answer: B

This question comes up so often and is easy to answer: Only owners or User Access Administrators can assign roles to other users
upvoted 5 times



  **Mehedi007** 1 year, 9 months ago

Selected Answer: B

"Grants full access to manage all resources, including the ability to assign roles in Azure RBAC."
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner>
upvoted 1 times

  **[Removed]** 1 year, 10 months ago

within provided solution , the Owner role can assign role for other users
B. Owner is answer
upvoted 1 times



  **Athul07** 1 year, 11 months ago

C. Assign User1 the Contributor role for VNet1.

To ensure that User1 can assign the Reader role for VNet1 to other users, you should assign User1 the Contributor role for VNet1.

The Contributor role grants permissions to manage all resources within a specific scope, including the ability to assign roles to other users. By assigning User1 the Contributor role for VNet1, User1 will have the necessary permissions to assign the Reader role for VNet1 to other users.

Assigning User1 the Owner role for VNet1 (option B) would grant excessive permissions, allowing User1 to make any changes to VNet1 and its resources, which may not be desired.
upvoted 1 times

  **myarali** 2 years, 2 months ago

Selected Answer: B

B. Owner correct



Owner: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
User Access Administrator: Lets you manage user access to Azure resources.

Contributor: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

Reader: View all resources, but does not allow you to make any changes.

Network Contributor: Lets you manage networks, but not access to them.

upvoted 2 times

  **zellck** 2 years, 3 months ago

Selected Answer: B

B is the answer.

upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B

upvoted 2 times

  **vetrivelm** 3 years ago

Answer B is correct. Owner Has full access to all resources including the right to delegate access to others.
upvoted 2 times

  **sjb666** 3 years ago

Selected Answer: B

Answer is B. Contributor can't grant access to others
upvoted 1 times

HOTSPOT -

You configure the custom role shown in the following exhibit.

```
{
  "properties": {
    "roleName": "role1",
    "description": "",
    "roleType": "true",
    "assignableScopes": [
      "/subscriptions/3d6209d5-c714-4440-9556e-d6342086c2d7/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Compute/availabilitySets/*",
          "Microsoft.Compute/locations/*",
          "Microsoft.Compute/virtualMachines/*",
          "Microsoft.Compute/virtualMachineScaleSets/*",
          "Microsoft.Compute/disks/write",
          "Microsoft.Compute/disks/read",
          "Microsoft.Compute/disks/delete",
          "Microsoft.Network/locations/*",
          "Microsoft.Network/networkInterfaces/*",
          "Microsoft.Network/networkSecurityGroups/join/action",
          "Microsoft.Network/networkSecurityGroups/read",
          "Microsoft.Network/publicIPAddresses/join/action",
          "Microsoft.Network/publicIPAddresses/read",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

To ensure that users can sign in to virtual machines that are assigned role1, modify the [answer choice] section

▼

actions

roletype

notActions

dataActions

notDataActions

assignableScopes

To ensure that role1 can be assigned only to a resource group named RG1, modify the [answer choice] section

▼

actions

roletype

notActions

dataActions

notDataActions

assignableScopes

Answer Area

To ensure that users can sign in to virtual machines that are assigned role1, modify the [answer choice] section

▼

actions

roletype

notActions

dataActions

notDataActions

assignableScopes

Correct Answer:

To ensure that role1 can be assigned only to a resource group named RG1, modify the [answer choice] section

▼

actions



roletype

notActions



dataActions



notDataActions

assignableScopes

  **pkkalra** Highly Voted 2 years, 8 months ago
the answer is wrong. you are not defining a policy but a custom role.
You need to provide either of the following in DataActions:
Microsoft.Compute/virtualMachines/login/action
Microsoft.Compute/virtualMachines/loginAsAdmin/action

correct answer is dataActions and assignableScopes
upvoted 232 times

  **dnt91** 4 months, 3 weeks ago
First is a dataAction. if you try to clone the built in Virtual Machine User Login role you can see that >
Microsoft.Compute/virtualMachines/login/action
Log in to a virtual machine as a regular user
DataAction
upvoted 1 times

  **duongduong_me** 5 months, 2 weeks ago
The dataActions field in a custom role is used to specify permissions for operations related to data managed by Azure resources, such as accessing blob storage, queues, or tables in an Azure Storage account. This field is not relevant for managing access to log in to a VM.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#dataactions>

upvoted 1 times

  **go4adil** 1 year, 3 months ago

Agreed....Correct Answer is 'dataActions' and 'assignableScopes'

In custom roles, 'roleType' only indicates whether this is a custom role.

It is set to "true" or "CustomRole" for custom roles and set to "false" or "BuiltInRole" for built-in roles. So, modifying 'roleType' for this custom role won't grant users access to log in to virtual machines that are assigned role1

upvoted 9 times

  **C_M_M** Highly Voted 2 years ago

The key to understanding the first option is to understand the Control plane VS Data plane
Action/notAction is the control plane, and DataAction/notDataAction is the data plane.

Logging into a VM is data plane - So it should be defined at the DataAction

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/control-plane-and-data-plane>

upvoted 36 times

  **ajdann** 1 year, 8 months ago


Thank you, this helped me understand the difference

upvoted 3 times

  **dhavalmodi** Most Recent 1 month, 2 weeks ago

Option1: actions, options2: assignableScopes

upvoted 1 times

  **sca88** 5 months, 3 weeks ago

Should be Action and AssignableScope.



" The Microsoft.Compute/virtualMachines/login/action permission is a control plane operation, so it should be included in the Actions array, not the DataActions array. This permission allows users to log in to virtual machines, which is part of managing the VM itself rather than accessing or modifying data within the VM" by Copilot

upvoted 5 times

  **Ivanvazovv** 1 month, 3 weeks ago

Absolutely stop that Copilot bullshit! You are only confusing people here!



upvoted 2 times

  **pstree** 5 months, 3 weeks ago

Stop wasting our time with wrong information from your Copilot. He will not take the exam for you.
Go here and search for Microsoft.Compute/virtualMachines/login/action :

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute>

upvoted 10 times

  **sca88** 5 months, 1 week ago

Thank you for the documentation link! So the correct Answer will be DataAction.

upvoted 3 times

  **Chuong0810** 6 months, 1 week ago

Ensuring Users Can Sign In to Virtual Machines: Adding Microsoft.Compute/virtualMachines/login/action in the actions section

Assigning role1 Only to RG1: Editing /subscriptions/{subscriptionId}/resourceGroups/RG1 in the assignableScopes section

The DataActions section in a role definition specifies permissions to perform actions on data within your resources (like Azure Storage or Cosmos DB...)

upvoted 1 times

  **Soudenho** 6 months, 1 week ago



To log in to a virtual machine (VM), you typically need to configure actions in a custom role. Specifically, for logging into a VM using Azure, you need to ensure the role includes the necessary actions for accessing the VM, such as:

Microsoft.Compute/virtualMachines/login/action: This action allows users to log in to the VM.

Microsoft.Compute/virtualMachines/read: This action allows users to read the VM properties.



Data actions are generally used for accessing data within Azure resources, such as reading or writing data in a storage account, and are not typically required for logging into a VM.

upvoted 1 times

  **Dankho** 6 months, 2 weeks ago

all the AIs (ChatGPT, Google's whatever it's called) say actions

upvoted 1 times

  **Dankho** 6 months, 2 weeks ago

I take it back, if you look at the reference below, you will see that every time an example includes "/login/action" it's shown in the dataActions section.



Reference: <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute>

upvoted 1 times



  **Stunomatic** 6 months, 2 weeks ago

```
{
  "Name": "Custom VM Login Role",
  "IsCustom": true,
  "Description": "Allows users to log in to assigned virtual machines",
  "Actions": [
    "Microsoft.Compute/virtualMachines/login/action",
    "Microsoft.Compute/virtualMachines/read"
  ],
  "NotActions": [],
  "AssignableScopes": [
    "/subscriptions/<subscription-id>"
  ]
}
```

upvoted 2 times

  **0378d43** 6 months, 3 weeks ago

Data Actions and assignableScopes
upvoted 3 times

  **komlaragnar** 6 months, 4 weeks ago

To ensure that users can sign in to virtual machines (VMs) when assigned a custom role in Azure, the RBAC JSON template needs to include the appropriate actions that grant access to the VM's management and sign-in capabilities.

Key properties to modify in the custom role definition JSON:
Actions:

To allow users to sign in to the VM, you need to add the following permissions in the Actions property:
"Microsoft.Compute/virtualMachines/login/action": Grants permission to log in to virtual machines.
"Microsoft.Compute/virtualMachines/read": Allows read access to the virtual machine's configuration.
"Microsoft.Network/networkInterfaces/read": Provides read access to network interface configurations (necessary for understanding network settings related to the VM).
upvoted 1 times



  **[Removed]** 7 months, 4 weeks ago



WRONG



dataActions
assignableScopes
upvoted 3 times



  **behradclid** 8 months ago



first one is dataActions.
proof is in here:
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute>
upvoted 1 times



  **Dankho** 6 months, 2 weeks ago
every single example is in the actions section not dataActions, are you high?
upvoted 1 times

  **divzrajshekar123** 9 months, 1 week ago
ANSWER IS dataactions and Assignable Scope
upvoted 2 times

  **ajay01avhad** 9 months, 1 week ago
For the first requirement: actions
For the second requirement: assignableScopes
upvoted 2 times

  **Josh219** 4 months, 3 weeks ago
Correct Answer:
Box1 = dataActions
Microsoft.Compute/virtualMachines/login/action
Box2 = assignableScopes
upvoted 1 times


  **23169fd** 10 months, 3 weeks ago
tested: Actions and Assignable Scope
"Microsoft.Compute/virtualMachines/login/action"
upvoted 4 times

  **Highgate** 8 months, 3 weeks ago
MSLearn says Microsoft.Compute/virtualMachines/login/action is a dataAction
"DataActions"

Microsoft.Compute/virtualMachines/login/action Log in to a virtual machine as a regular user"
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute#virtual-machine-user-login>
upvoted 1 times

  **76d5e04** 11 months ago

It is very time consuming and causing confusion to decide which is correct answer as the examtopic has not assured their answer is 100% correct.
Also for some questions mostly voted % is missing so not able to judge the correct answer.
I have exam scheduled by end of June, please teach me how to arrive at the correct answer
upvoted 2 times

  **23169fd** 11 months, 1 week ago

Correct answer: Actions and Assignable Scope.
"Microsoft.Compute/virtualMachines/login/action"
upvoted 2 times



You have an Azure subscription that contains a storage account named storage1. The storage1 account contains a file share named share1. The subscription is linked to a hybrid Azure Active Directory (Azure AD) tenant that contains a security group named Group1. You need to grant Group1 the Storage File Data SMB Share Elevated Contributor role for share1. What should you do first?


- A. Enable Active Directory Domain Service (AD DS) authentication for storage1.
- B. Grant share-level permissions by using File Explorer.
- C. Mount share1 by using File Explorer.
- D. Create a private endpoint.

Correct Answer: A

Community vote distribution

A (100%)

-   **NaoVaz**



Highly Voted 

 2 years, 1 month ago

Selected Answer: A

A) " Enable Active Directory Domain Service (AD DS) authentication for storage1. "

Reference: <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable?tabs=azure-portal#overview-of-the-workflow>



upvoted 22 times
-   **Asta2001** 1 year, 10 months ago

>A) " Enable Active Directory Domain Service



The link you provided says:


"Enable AZURE Active Directory Domain Service..."

Does it matter?

upvoted 2 times
-   **ggogel** 11 months, 1 week ago

No, because it is now called "Microsoft Entra Domain Services".

upvoted 5 times
-   **Athul07**

Highly Voted 

 1 year, 5 months ago



A. Enable Active Directory Domain Service (AD DS) authentication for storage1.


To grant the Group1 the Storage File Data SMB Share Elevated Contributor role for share1, you need to enable Active Directory Domain Service (AD DS) authentication for the storage account.

By enabling AD DS authentication, you allow Azure AD security groups to be used for granting access control to file shares in the storage account. This enables you to assign roles, such as the Storage File Data SMB Share Elevated Contributor role, to the security group Group1 for the specific file share share1.

Once AD DS authentication is enabled and the security group is assigned the appropriate role, Group1 will have the necessary permissions to access and manage the file share.



Therefore, enabling Active Directory Domain Service (AD DS) authentication for storage1 is the first step you should take to grant Group1 the Storage File Data SMB Share Elevated Contributor role for share1.

upvoted 19 times
-   **Amir1909**

Most Recent 

 7 months, 2 weeks ago

A is correct

upvoted 1 times
-   **Mehedi007** 1 year, 3 months ago

Selected Answer: A

Answer: Enable Active Directory Domain Service (AD DS) authentication for storage1.

"1. Enable Azure AD DS authentication over SMB for your storage account to register the storage account with the associated Azure AD DS deployment.



2. Assign share-level permissions to an Azure AD identity (a user, group, or service principal)."

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-domain-services-enable?tabs=azure-portal#overview-of-the->

workflow

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-domain-services-enable?tabs=azure-portal#assign-share-level-permissions>

upvoted 2 times

  **zelck** 1 year, 9 months ago

Selected Answer: A

A is the answer.



<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable?tabs=azure-portal#assign-share-level-permissions>

Most users should assign share-level permissions to specific Azure AD users or groups, and then configure Windows ACLs for granular access control at the directory and file level. However, alternatively you can set a default share-level permission to allow contributor, elevated contributor, or reader access to all authenticated identities.

We have introduced three Azure built-in roles for granting share-level permissions to users and groups:

- Storage File Data SMB Share Elevated Contributor allows read, write, delete, and modify Windows ACLs in Azure file shares over SMB.

upvoted 3 times

  **zelck** 1 year, 9 months ago

Before you can assign the Storage File Data SMB Share Elevated Contributor role to Group1, you need to enable AD DS authentication for storage1, which allows you to use Azure AD security groups to manage access to the file share. Once you have enabled AD DS authentication, you can then assign the appropriate role to the security group.

upvoted 2 times

  **AndreaStack** 1 year, 9 months ago

A) . Enable Active Directory Domain Service (AD DS) authentication for storage1.

Reference: learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable

upvoted 2 times

  **Mat_m0381** 2 years, 1 month ago



A is Correct

upvoted 3 times

  **RichardBill** 2 years, 2 months ago

Correct



upvoted 1 times

  **libran** 2 years, 2 months ago

Selected Answer: A

A is the right answer

upvoted 3 times

  **EmnCours** 2 years, 2 months ago

Selected Answer: A

Note: The Storage File Data SMB Share Elevated Contributor allows read, write, delete and modify NTFS permissions in Azure Storage file shares over SMB.

upvoted 2 times

You have 15 Azure subscriptions.

You have an Azure Active Directory (Azure AD) tenant that contains a security group named Group1.

You plan to purchase additional Azure subscription.

You need to ensure that Group1 can manage role assignments for the existing subscriptions and the planned subscriptions. The solution must meet the following requirements:

- ☞ Use the principle of least privilege.
- ☞ Minimize administrative effort.

What should you do?

- A. Assign Group1 the Owner role for the root management group.
- B. Assign Group1 the User Access Administrator role for the root management group.
- C. Create a new management group and assign Group1 the User Access Administrator role for the group.
- D. Create a new management group and assign Group1 the Owner role for the group.

Correct Answer: B

Community vote distribution

B (84%)

Other

- NaoVaz

Highly Voted

2 years, 7 months ago

Selected Answer: B

B) " Assign Group1 the User Access Administrator role for the root management group."

To be able to assign licenses to all current and future subscriptions, while minimizing the administrative effort, one should apply the role to the Root Management Group.

And because we should use the principle of least privilege we should chose the User Access Administrator role instead of the Owner one.

upvoted 49 times

XristophD

2 years, 5 months ago

Elevation is needed first, but in general this is the right answer and the most effective following the principle of least-privileged-access and will also be valid on newly added Subscriptions.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>

upvoted 7 times

P123123

Highly Voted

2 years, 4 months ago

B or C depending on which requirement you're prioritizing.

- B if you're minimizing the administrative effort

- C if you're following principle of least privilege

upvoted 12 times

lykeman26

6 months, 3 weeks ago

It says for the planned and existing subscriptions. So it has to be the root tenant MG

upvoted 2 times

AnonFox

2 years ago

^ This. So I don't understand which is the correct one. Realistically wouldn't you always do C for a better structured system?

upvoted 2 times

damnboy

9 months ago

From the point of view of "least privilege" it would be recommended, of course, BUT if you create a management group ... you have to move the subscriptions to it, and option C says nothing about moving the subscriptions to this new management group, so group1 would be able to manage access in 0 subscriptions.

upvoted 1 times

Jay_D_Lincoln

Most Recent

3 months ago

Selected Answer: B

C is incorrect because...

- it did not mention anything about move existing subscription to the new mgt group

- even if it would tell to move existing subs, the action would MAXIMIZE administrative task(which does not meet second requirement)

upvoted 1 times

[Removed]

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times

  **GreenTick** 10 months, 3 weeks ago

A. to manage subscriptions required Owner role,
<https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/add-change-subscription-administrator>
upvoted 1 times

  **3c5adce** 11 months, 3 weeks ago

ChatGPT4:
Option B focuses on assigning the User Access Administrator role at the root management group level. This role specifically allows members to manage user access to Azure resources, which includes managing role assignments. Assigning this role at the root management group level ensures that the permissions apply across all existing and future subscriptions under that root. This approach adheres to the principle of least privilege by providing only the necessary permissions to manage access without broader management permissions that come with the Owner role.
upvoted 2 times

  **Amir1909** 1 year, 2 months ago

B is correct
upvoted 1 times



  **LetsGetThisCert** 1 year, 6 months ago

Selected Answer: B

The answer is B you are providing access administrator to the Root Manangment group per Microsoft's documentation

"All subscriptions and management groups fold up into one root management group within the directory.
All resources in the directory fold up to the root management group for global management.
New subscriptions are automatically defaulted to the root management group when created."

<https://learn.microsoft.com/en-us/azure/governance/management-groups/overview>
upvoted 4 times

  **KiwE** 1 year, 9 months ago

I think the key here is " existing subscriptions and the planned [all future] subscriptions"
OpenAI says: "Option C is not the best choice because it requires creating a new management group which is not necessary for the given scenario."
If we were to go the route of C we would need to do considerations for all further added subscriptions (more administrative thought) which we don't need with B and the group is said that it should have the role of all further subscriptions to there's no point to it.
upvoted 4 times

  **Amateur2023** 1 year, 8 months ago

yes; tks for your explain
upvoted 1 times

  **Teroristo** 1 year, 9 months ago

Answer: B
Explanation:
To be able to assign licenses to all current and future subscriptions, while minimizing the administrative effort, one should apply the role to the Root Management Group.
And because we should use the principle of least privilege we should chose the User Access Administrator role instead of the Owner one.
upvoted 1 times

  **[Removed]** 1 year, 10 months ago

Selected Answer: B

The following 2 choices are possible:
A. Assign Group1 the Owner role for the root management group.
B. Assign Group1 the User Access Administrator role for the root management group.
Requested condition is Use the principle of least privilege.
Answer A is eliminated
Answer B: is correct
upvoted 2 times

  **RandomNickname** 1 year, 10 months ago

Selected Answer: B

B: looks correct as per URL below.

Any new/planned subscriptions will fold up into the root management group by default.

See section;
Important facts about the root management group

"All subscriptions and management groups fold up to the one root management group within the directory.
All resources in the directory fold up to the root management group for global management.
New subscriptions are automatically defaulted to the root management group when created."

<https://learn.microsoft.com/en-us/azure/governance/management-groups/overview>

upvoted 3 times

  **Alex1184** 1 year, 11 months ago

Answer should be C. This uses the least-privilege principle - Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group.



upvoted 1 times

  **TestKingTW** 1 year, 11 months ago

Selected Answer: C

Create a new management group and assign Group1 the User Access Administrator role for the group

upvoted 1 times

  **Exilic** 1 year, 12 months ago

Selected Answer: C

OpenAi

"Option C is the correct answer.

Assigning Group1 the Owner role for the root management group (Option A) would give the group unrestricted access to all resources in all subscriptions and management groups under the root management group. This goes against the principle of least privilege and could potentially result in unintended changes or deletions of resources.

Assigning Group1 the User Access Administrator role for the root management group (Option B) would give the group permission to manage user access to Azure resources, but not to manage role assignments for subscriptions and management groups.

Creating a new management group and assigning Group1 the Owner role for the group (Option D) would give the group the same unrestricted access as assigning them the Owner role for the root management group.

Therefore, the best option would be to create a new management group and assign Group1 the User Access Administrator role for the group (Option C). This would allow the group to manage role assignments for all subscriptions and management groups within the new management group without granting them unnecessary permissions."

upvoted 2 times

  **ggogel** 1 year, 5 months ago

It's not C because it does not fulfill the lowest administrative effort. All new subscriptions will be automatically assigned to the root management group but not to this newly created one. So everytime you add a subscription, you would need to assign this management group access to it.

upvoted 3 times

  **AnonFox** 2 years, 2 months ago

Selected Answer: B

B is correct.

upvoted 3 times

  **er101q** 2 years, 2 months ago

While Assigning the User Access Administrator role for the root management group to Group1 will provide Group1 with the ability to manage role assignments for all subscriptions within the root management group, it does not adhere to the principle of least privilege as it grants full administrative access to all Azure resources under the root management group.

It is recommended to create a new management group and assign the User Access Administrator role for that specific group to Group1, in order to meet the requirements of using the principle of least privilege and minimizing administrative effort. while still adhering to the principle of least privilege.

why not B.

upvoted 2 times

  **er101q** 2 years, 2 months ago

C. Create a new management group and assign Group1 the User Access Administrator role for the group.

To meet the requirements of using the principle of least privilege and minimizing administrative effort, it is recommended to create a new management group and assign Group1 the User Access Administrator role for that group. The User Access Administrator role provides the ability to manage role assignments for subscriptions within the management group, without granting full administrative access to all Azure resources. This allows you to provide the necessary permissions to Group1 for managing role assignments for the existing and planned subscriptions, while still adhering to the principle of least privilege.

upvoted 2 times

HOTSPOT -

You have an Azure subscription that contains the hierarchy shown in the following exhibit.



You create an Azure Policy definition named Policy1.

To which Azure resources can you assign Policy1 and which Azure resources can you specify as exclusions from Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can assign Policy1 to:

Subscription1 and RG1 only
ManagementGroup1 and Subscription1 only
Tenant Root Group, ManagementGroup1, and Subscription1 only
Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only
Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

You can exclude Policy1 from:

VM1 only
RG1 and VM1 only
Subscription1, RG1, and VM1 only
ManagementGroup1, Subscription1, RG1, and VM1 only
Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

Correct Answer:

Answer Area

You can assign Policy1 to:

Subscription1 and RG1 only

ManagementGroup1 and Subscription1 only

Tenant Root Group, ManagementGroup1, and Subscription1 only

Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only

Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

You can exclude Policy1 from:

VM1 only

RG1 and VM1 only

Subscription1, RG1, and VM1 only

ManagementGroup1, Subscription1, RG1, and VM1 only

Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

  **Ntinsky**  2 years, 7 months ago

Since the discussion added a lot of confusion cause a lot of people in here just drop random facts without any proof,misleading people, i tested it at an Azure lab.



In the scope field at the "Basics" tab i was able to select "Tenant Root Group" or "Management Group1" with the optional entries of Subscription and Resource group

So ""you can assign policy to Tenant Root Group,ManagementGroup1,Subscription1 and RG1""



As for the second answer about the exclusions, i was able to select all the items in the scope EXCEPT the Tenant Root Group



Therefore the correct answer would be ""ManagementGroup1,Subscription1,RG11 and VM1""

I hope that helps
upvoted 269 times

  **Sanaz90** 9 months, 2 weeks ago

Wrong! Go to a resource like vm and assign a policy from there to vm and you will see the policy assignment is set to resource level and not rg level
upvoted 4 times

  **junkz** 5 months, 4 weeks ago
huh, i learned something new today with this answer.
upvoted 1 times

  **witalis** 5 months, 1 week ago

The question pertains to assigning and excluding Azure Policy definitions. Here's the answer:

You can assign Policy1 to:
Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only
Azure Policies can be assigned at higher levels of hierarchy like the Tenant Root Group, Management Groups, Subscriptions, and Resource Groups.
You can exclude Policy1 from:
Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1
Azure Policies allow exclusions at any scope under the assignment, including specific resources like VMs.
upvoted 1 times

  **XristophD** 2 years, 5 months ago

Since your answer added a lot of confusion, cause you drop random answers:

The Azure Portal only allows to select scopes down to Resource Groups.
That is correct.

BUT: With Azure CLI or Azure PowerShell, a Policy Assignment can be done at a specific resource.

The Azure Portal UI is limited in many ways, so always check the possibilities with Azure CLI or PowerShell, before assuming something is not there or doesn't work.
upvoted 20 times



  **codeScalable** 2 years, 5 months ago



azure policies can be scoped down to individual resources. "Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources."

the second answer is correct
upvoted 12 times



  **RichardBill**  2 years, 8 months ago



Wrong! You can assign a policy to the Root, Management Group, Subscription and Ressource Group BUT NOT A RESSOUCCE ITSELF! Test it in Portal!
2nd part of answer seems to be correct. You can not Exclude the highest scope that you can assign to. I tried it in portal as well and it wont save the exclusion Tenant Root Group
upvoted 38 times



  **Traian** 2 years, 8 months ago
I believe you are wrong. You can assign a policy to a resource :
"An assignment is a policy definition or initiative that has been assigned to a specific scope. This scope could range from a management group to an individual resource."
<https://docs.microsoft.com/en-us/azure/governance/policy/overview>
- check assignments
In my opinion the provided answer is correct
upvoted 25 times



  **RichardBill** 2 years, 7 months ago
So I checked again and the portal doesnt let you do it! Thats what I based my assumption! But via Azure CLI it says that a ressource is a vaild scope for assignment: <https://docs.microsoft.com/en-us/cli/azure/policy/assignment?view=azure-cli-latest#az-policy-assignment-create>



So yeah I think that you are right and my comment is wrong but I can not delete it. But looks like this is just a portal restriction. Sorry for the confusion!
upvoted 37 times



  **meeko86** 2 years, 5 months ago
Valid scopes are management group, subscription, resource group, and resource
<https://learn.microsoft.com/en-us/cli/azure/policy/assignment?view=azure-cli-latest#az-policy-assignment-create>
upvoted 6 times



  **Grande** 2 years, 8 months ago
very correct. in general you cannot exclude the parent of a child already covered by the policy
e.g. if scope was RG1, you cannot exclude Subs1, you can only exclude resources underneath RG1
upvoted 1 times



  **northstar88** 2 years, 8 months ago
Tried in portal as well. You cannot select resources as scope.
upvoted 4 times



  **buzzerboy** 2 years, 4 months ago
I couldnt assign a policy at Tenant Root Management Group. There is no blade for policy.
upvoted 2 times


  **Ivanvazovv** Most Recent 1 month, 3 weeks ago
Just checked:
Go to the VM > Operations > Policies and there you have the options to assign a policy or initiative.
upvoted 1 times

  **nikiv_896** 2 months, 1 week ago
1/ You can assign Policy1 to: Tenant Root Group, Management Group 1, Subscription 1, RG1,VM1
2/ You can exclude Policy1 to: Management Group 1, Subscription 1,RG1,VM1
Refer the link <https://learn.microsoft.com/en-us/azure/governance/policy/overview>
It states this "Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources. The assignment applies to all resources within the Resource Manager scope of that assignment. Subscopes can be excluded"
upvoted 1 times



  **Jay_D_Lincoln** 3 months ago
The answer is correct. You CAN assign a policy to a RESOURCE level using AZURE PORTAL as well. But to do this you have to do it from the resource dashboard or using cli.
go to VM1->Operations->Policies->Assign Policy->Scope->Subscription1/MG1/RG1/VM1
upvoted 2 times

  **vrn1358** 3 months, 3 weeks ago
2025-Jan
Tested in LAB:
you can assign policy to Tenant Root Group,ManagementGroup1,Subscription1 and RG1, VM1
allow exclusions
upvoted 3 times

  **vrn1358** 3 months, 3 weeks ago
Sorry missed Exclusion
2025-Jan
Tested in LAB:
you can assign policy to Tenant Root Group,ManagementGroup1,Subscription1 and RG1, VM1
allow exclusions: Management Group1, Subscription1, RG1, VM1
upvoted 5 times

  **fittech** 7 months ago
!! Please be careful not to share incorrect information! According to Microsoft documentation: "policies can be assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources." !! -

upvoted 4 times

  **[Removed]** 7 months, 3 weeks ago
WRONG



You can assign Policy1 to:
Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only

You can exclude Policy1 from:
ManagementGroup1, Subscription1, RG1, and VM1 only
upvoted 2 times



  **[Removed]** 8 months ago
Wrong



You can assign Policy1 to:
Tenant Root Group, ManagementGroup1, and Subscription1 only



You can exclude Policy1 from:
ManagementGroup1, Subscription1, RG1, and VM1 only
upvoted 1 times



  **[Removed]** 7 months, 3 weeks ago
sorry i misserad it,
You can assign Policy1 to:
Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only



You can exclude Policy1 from:
ManagementGroup1, Subscription1, RG1, and VM1 only
upvoted 1 times



  **Mshaty** 7 months, 3 weeks ago
if you can exclude it doesnt that mean you can assign the policy to the resource ?you cant exclude something that cannot be part of the policy
upvoted 1 times



  **[Removed]** 7 months, 3 weeks ago
you can't assign a policy for a resource on the portal, you can do it only on CLI or PowerShell, which is not mintioned here, so we have to answer this in gerenal.
upvoted 1 times



  **pasangawa** 8 months ago
tested on lab, you can assign policy on vm
upvoted 1 times



  **pet3r** 9 months, 2 weeks ago
Policies can be applied to the resource like VM
<https://learn.microsoft.com/en-us/azure/governance/policy/concepts/recommended-policies>
upvoted 1 times



  **VinodRK** 10 months, 2 weeks ago
You can assign Policy1 to Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only
You can exclude Policy1 from ManagementGroup1, Subscription1, RG1, and VM1 only
upvoted 1 times



  **23169fd** 10 months, 3 weeks ago
given answer is correct.
upvoted 2 times

  **76d5e04** 11 months ago
Feeling tired of reading discussions. examtopics please quality seems ?
upvoted 3 times

  **76d5e04** 11 months ago
In the name of discussion most confusion is created and makes me think is it worth paying \$65 to examtopics. I thought examtopics would be a good material so far out of 90 questions most of them have not been given exact answer
upvoted 3 times

  **nailedIT** 9 months ago
The issue lies on the people and bots using examtopics. I still find it very useful to get access to the questions, but I can never rely exclusively on examtopics answers nor community. Yet, community seems to be sharp on the right answer than examtopics, but is full of bots giving almost random answers without any explanation.
upvoted 2 times

  **Limobakry** 11 months, 3 weeks ago
the key in question is only
upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

You can Assign policy to: Tenant Root Group, ManagementGroup1, Subscription1 and RG1 ONLY"

You can Exclude policy from: ""ManagementGroup1,Subscription1,RG1, and VM1 ONLY""
upvoted 1 times

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

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User2 to create the user accounts.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (92%)

8%

- aaa112

Highly Voted

4 years, 4 months ago

Correct, but the explanation is not. User1 is global admin of contoso.onmicrosoft.com. As he created the new tenant called external.contoso.onmicrosoft.com, he will be the OWNER. Check the scope not just the role, tho.

upvoted 98 times
- mikl

4 years, 2 months ago

Thank you for clarifying

upvoted 2 times
- r3tr0penguin

3 years, 11 months ago

Then if User2 want to create new user on external.contoso.onmicrosoft.com , he can't right ? because User2 is not the one who create tenant external.contoso.onmicrosoft.com that mean User 2 don't be OWNER

upvoted 31 times
- RamanAgarwal

3 years, 11 months ago

Yes because user2 wont have any role or connection with the new tenant unless added by user1 specifically.

upvoted 30 times
- AzureG0d

2 years, 6 months ago

be mindful of the power of a global administrator.

" Because only another global admin can reset a global admin's password, we recommend that you have at least 2 global admins in your organization in case of account lockout. But the global admin has almost unlimited access to your org's settings and most of the data, so we also recommend that you don't have more than 4 global admins because that's a security threat. "

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

upvoted 5 times
- AzureG0d

2 years, 6 months ago

I stand corrected. Only user1 can see and will have access to those.

Administrative independence

If a non-administrative user of organization 'Contoso' creates a test organization 'Test,' then:

By default, the user who creates a organization is added as an external user in that new organization, and assigned the global administrator role in that organization.

The administrators of organization 'Contoso' have no direct administrative privileges to organization 'Test,' unless an administrator of 'Test' specifically grants them these privileges. However, administrators of 'Contoso' can control access to organization 'Test' if they sign in to the user account that created 'Test.'

If you add or remove an Azure AD role for a user in one organization, the change does not affect the roles that the user is assigned in any other Azure AD organization.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-directory-independence#administrative-independence>

upvoted 13 times

🗲️ 👤 **mlantonis** Highly Voted 👍 3 years, 11 months ago

Correct Answer: A - Yes

Only User1 has access to the new Tenant, because User1 created the Tenant and became automatically Global Admin.

upvoted 84 times

🗲️ 👤 **behradclid** 8 months ago

OMG read question carefully, answer is NO

upvoted 2 times

🗲️ 👤 **Spam101198** 2 years, 2 months ago

Question is asking about User 2 not user 1 , hence answer is NO

upvoted 16 times

🗲️ 👤 **EricMaes** 3 years, 7 months ago

Didn't he become owner?

upvoted 3 times

🗲️ 👤 **A_GEE** 2 years, 11 months ago

Yes. User1 becomes the owner and the first user in that Tenant

upvoted 4 times

🗲️ 👤 **FlaShhh** 1 year, 4 months ago

The Azure God mlantonis is wrong for once, is the world ending?

upvoted 11 times

🗲️ 👤 **rodrod** 6 months, 1 week ago

I think earth stopped spinning for a few sec till it realizes the wording of the question has changed. We are all safe.

upvoted 1 times

🗲️ 👤 **58b2872** Most Recent 🕒 4 months ago

Selected Answer: B

Default Behavior When Creating a New Tenant:

When User1 creates a new Azure AD tenant (external.contoso.onmicrosoft.com), User1 becomes the only Global Administrator in that new tenant by default.

No other users, including User2, will have any roles or permissions in the new tenant unless explicitly added by User1.

User2's Role:

While User2 is a Global Administrator in the original tenant (contoso.onmicrosoft.com), that role does not carry over to the newly created tenant (external.contoso.onmicrosoft.com).

Therefore, User2 cannot create user accounts in the new tenant unless User1 explicitly grants User2 permissions (e.g., by assigning User2 the Global Administrator role in the new tenant)

upvoted 1 times

🗲️ 👤 **myarali** 7 months ago

Selected Answer: B

NO

After User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com, User-1 becomes owner and Global Administrator of external.contoso.onmicrosoft.com.

BUT User-2 doesn't have any authorization in new tenant. User-2's Global Administrator Role applies to contoso.onmicrosoft.com NOT for external.contoso.onmicrosoft.com.

SO User-1 can not instruct User2 to create the user accounts.

MAYBE that can be done after User-1 assigns Global Administrator or User Access Administrator Role to User-2.

upvoted 8 times

🗲️ 👤 **shadad** 7 months ago

Selected Answer: B

This was on it and my answer was: B

Only User1. not user2 not user3 not user4 .. there are many version of this question and the right answer is User 1. why? because he is the one who created the tenant so he will be granted the Owner.

upvoted 13 times

🗲️ 👤 **pravin2917** 2 years, 2 months ago

How was your experience bro ?

upvoted 2 times

🗲️ 👤 **Omer87** 7 months, 3 weeks ago

Selected Answer: B

The question asks if User 2 can add users to the new tenant. The answer is "NO" as only user1 is the owner of the new tenant and all the other global admins do not have admin access to the new tenant unless User1 grants them the access.

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B



it's B

upvoted 1 times

  **[Removed]** 7 months, 4 weeks ago

only User1

upvoted 1 times

  **mojo86** 8 months, 4 weeks ago

Answe is No. Tenant Isolation: Azure AD tenants are isolated from each other, meaning that roles and permissions are specific to each tenant. A Global Administrator in one tenant does not have any privileges in another tenant unless they are explicitly granted.

upvoted 1 times

  **ajay01avhad** 9 months, 1 week ago

User2 cannot create user accounts in the new tenant without being granted the necessary permissions by User1. Therefore, instructing User2 to create the user accounts does not meet the goal.

Correct Answer:

B. No

upvoted 1 times

  **ajay01avhad** 9 months, 1 week ago

User Roles and Permissions:

User1: Global Administrator in both the old and the new tenant.

User2: Global Administrator in the original tenant (contoso.onmicrosoft.com), but not automatically in the new tenant (external.contoso.onmicrosoft.com).

User3: User Administrator in the original tenant, but no role in the new tenant.



User4: Owner in the original Azure Subscription, but no role in the new tenant.

Given these roles, only User1 has the necessary permissions by default to create new user accounts in the new tenant (external.contoso.onmicrosoft.com). User2 would need to be assigned appropriate roles in the new tenant by User1 before they can create user accounts.

Conclusion:



Correct Answer: No. Instructing User2 to create user accounts in the new tenant will not meet the goal because User2 does not have the necessary permissions in the new tenant until granted by User1.

upvoted 2 times

  **Op0m0p** 9 months, 4 weeks ago

When you create a new Microsoft Entra tenant, you become the first user of that tenant. As the first user, you're automatically assigned the Global Administrator role. Review your user account by navigating to the Users page.

upvoted 1 times

  **Op0m0p** 9 months, 4 weeks ago

Microsoft Entra ID (formerly Azure Active Directory)



upvoted 1 times

  **LearnerFL** 10 months ago

Selected Answer: B


In Azure, when a new tenant is created, only the user who creates the tenant (in this case, User1) is automatically assigned the Global Administrator role for that tenant. This means that initially, only user1 would have access to the new tenant, external.contoso.onmicrosoft.com.

upvoted 2 times

  **hercule** 10 months, 2 weeks ago

yes and no, according to the least privilege you need a User Administrator hence (B)

upvoted 1 times

  **aflavien** 10 months, 3 weeks ago

Instructing User2 to create user accounts will meet the goal if User2 is granted the necessary permissions in the new tenant (external.contoso.onmicrosoft.com). However, since the problem statement does not mention assigning any roles to User2 in the new tenant, the solution as it stands does not fully meet the goal without additional steps.

Answer: No, it does not meet the goal, as User2 needs to be assigned an appropriate role in the new tenant first.

upvoted 4 times

  **3c5adce** 11 months, 3 weeks ago

ChatGPT4 says YES:

Instructing User2 to create the user accounts in the new Azure Active Directory tenant named external.contoso.onmicrosoft.com does meet the goal. This is because User2 holds the role of "Global administrator" within the Azure Active Directory. A Global administrator has the highest level of administrative privileges across all Azure AD directories and resources, which includes the authority to manage users, assign roles, and create

new user accounts in any directory within the Azure environment. Therefore, User2 is appropriately authorized to create new user accounts in the specified tenant.

upvoted 1 times

  **MCLC2021** 1 year ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

MICROSOFT ENTRA ROLES

Global Administrator:Manage access to all administrative features in Microsoft Entra ID, as well as services that federate to Microsoft Entra ID

Assign administrator roles to others, Reset the password for any user and all other administrators.

User Administrator: Create and manage all aspects of users and groups, Manage support tickets, Monitor service health

Change passwords for users, Helpdesk administrators, and other User Administrators.

upvoted 1 times

  **behradcld** 8 months ago

Read the question carefully for God sake

upvoted 1 times

  **tashakori** 1 year, 1 month ago

No is right

upvoted 2 times

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

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User4 to create the user accounts.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (93%)

7%

- Itkiller

Highly Voted

2 years, 11 months ago

Selected Answer: B

B:No, when you create a new tenant, the creator is the only global admin and owner, he must first give access to others to allow anything.
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant#your-user-account-in-the-new-tenant>
upvoted 32 times
- pranavhalgekar

Highly Voted

2 years, 11 months ago

Tested.
Ans is B. No
Even if User4 is owner of subscription, he was not able to find new tenant created by user1 in Azure Active Directory > Manage Tenant.
upvoted 19 times
- JustinYoo

Most Recent

4 months, 3 weeks ago

Selected Answer: B

User4 is not an owner of the new one, only User1 can do that.
upvoted 1 times
- [Removed]

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times
- [Removed]

7 months, 4 weeks ago

only User1
upvoted 1 times
- MCLC2021

1 year ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>
MICROSOFT ENTRA ROLES
Global Administrator:Manage access to all administrative features in Microsoft Entra ID, as well as services that federate to Microsoft Entra ID
Assign administrator roles to others, Reset the password for any user and all other administrators.
User Administrator: Create and manage all aspects of users and groups, Manage support tickets, Monitor service health
Change passwords for users, Helpdesk administrators, and other User Administrators.
upvoted 2 times
- [Removed]

1 year, 10 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

-Owner

Full access to all resources

Delegate access to others

upvoted 3 times

  **hebbo777** 1 year, 5 months ago

i believe owner have full access in the tenant which associated with its subscription, there is no information about new tenant whether its associated with this subscription or not

upvoted 1 times

  **AK4U_111** 2 years, 2 months ago

how can a tenant such as external.contoso.onmicrosoft.com even be created? i cant find anything on how to do this. when i go to create tenant i can create a new one but not a sub tenant which is a part of the original tenant

upvoted 1 times

  **tomasek88** 2 years, 2 months ago

Selected Answer: B

NO = B --> because User4 has nothing to do with NEW Azure Active Directory tenant named external.contoso.onmicrosoft.com

upvoted 2 times

  **JayLearn2022** 2 years, 2 months ago

There are several version of this question. The following are the valid and invalid solutions that may be presented.

Valid Solution: Meets the Goal

Solution: Solution: You instruct User1 to create the user accounts.


Invalid Solutions: Does not Meet the Goal

-Solution: You instruct User2 to create the user accounts.

-Solution: You instruct User3 to create the user accounts.

-Solution: You instruct User4 to create the user accounts.

upvoted 8 times

  **myarali** 2 years, 2 months ago

Selected Answer: B

- NO



After User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com, User-1 becomes owner and Global Administrator of external.contoso.onmicrosoft.com.

BUT User-4 doesn't have any authorization in new tenant.

SO User-1 can not instruct User4 to create the user accounts.

MAYBE that can be done after User-1 assigns Global Administrator or User Access Administrator Role to User-4.

upvoted 1 times

  **zellck** 2 years, 3 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-overview#scope>

When you assign a role, you specify one of the following types of scope:

- Tenant

- Administrative unit

- Azure AD resource

upvoted 1 times

  **cryptostud** 2 years, 7 months ago

This proves that answer to question 58 is No

upvoted 6 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) "No"

Only the tenant creators receive by default the Owner role inside the tenant and therefore are able to create user accounts.


upvoted 4 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B



Correct Answer: B

upvoted 1 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

  **Fatrat** 2 years, 8 months ago

User 1, who created the new tenancy, will be appointed as Global Administrator. The other 3 users, who belong to the first tenancy, would need to be invited into the new tenancy and given correct permission by User 1.
upvoted 1 times

  **Aypumpin** 2 years, 9 months ago

The answer is B
upvoted 1 times

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

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User3 to create the user accounts.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (83%)

A (17%)

- pgmpp

Highly Voted

2 years, 8 months ago

The answer is No!
I tested this.
1. I created a new Tenant contosgmp.
2. Added 2 users, User1 and User 2 in this tenant and gave them global privileges
3. I logged through User1 and created a new tenant called externalcontosgmp
4. Now when I logged in through User2 and try to switch tenants, the new tenant externalcontosgmp is not available at all for User2. Hence User1 needs to invite User2 first
upvoted 62 times
- ELearn

9 months, 3 weeks ago

Correct answer is: B.NO
Clear explanation: In Azure only a Global Administrator can create a new Azure Active Directory (Azure AD) tenant. In this scenario, User1, who is a Global Administrator, creates a new Azure AD tenant named external.contoso.onmicrosoft.com. However, User3, who is an Owner of an Azure subscription, does not automatically have access to this new tenant. User1, as the one who created the new tenant, would be the only Global Administrator in the new tenant by default.

Therefore, User3 would not be able to create user accounts in the new tenant unless User1 grants them the necessary permissions. So, instructing User3 to create the user accounts in the new tenant would not meet the goal, unless User1 first adds User3 as a User administrator/Global administrator in the new tenant.
upvoted 2 times
- JohnPi

Highly Voted

2 years, 8 months ago

Selected Answer: B

it is another tentant
upvoted 48 times
- allinict_111

Most Recent



5 months, 1 week ago

No, this does not meet the goal. Here's why:
User3, as a User Administrator in Azure AD, has permissions to create and manage users within the scope of an existing Azure AD tenant. However, because the new tenant external.contoso.onmicrosoft.com was just created by User1 (who is a Global Administrator), User3 will not automatically have administrative rights in the new tenant.
To create new user accounts in external.contoso.onmicrosoft.com, you would need to either:
Have User1 (the Global Administrator) create the new user accounts.
Have User1 assign the necessary administrative roles to User3 in the new tenant so that User3 can create user accounts there.
Therefore, simply instructing User3 to create the user accounts will not be sufficient unless they have been explicitly granted the necessary permissions in the new tenant.
upvoted 2 times
- [Removed]

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times

  **[Removed]** 7 months, 4 weeks ago
only User1
upvoted 1 times



  **hercule** 10 months, 2 weeks ago

Selected Answer: A

according to the documentation you need at least a User Administrator hence A is correct. <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-create-delete-users>
upvoted 1 times

  **chucklu** 10 months, 1 week ago

User3's User Administrator role is scoped to the original tenant contoso.onmicrosoft.com and does not extend to the new tenant external.contoso.onmicrosoft.com by default.
upvoted 3 times



  **MCLC2021** 1 year ago

Selected Answer: A



<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>
MICROSOFT ENTRA ROLES
Global Administrator:Manage access to all administrative features in Microsoft Entra ID, as well as services that federate to Microsoft Entra ID
Assign administrator roles to others, Reset the password for any user and all other administrators.
User Administrator: Create and manage all aspects of users and groups, Manage support tickets, Monitor service health
Change passwords for users, Helpdesk administrators, and other User Administrators.
upvoted 1 times

  **TechThameem** 11 months, 1 week ago

You should understand the question properly, User1 (the Global admin) creates a new tenant, that means User1 has created a new domain where User1 only will have access no one other admins will have access in that tenant. So, User 3 cannot create a user account in that new tenant.
upvoted 1 times

  **tashakori** 1 year, 1 month ago

No is right
upvoted 1 times

  **rreghioua** 1 year, 3 months ago

Selected Answer: A
upvoted 1 times

  **VV11_SS22** 1 year, 8 months ago



Correct answer is B
upvoted 1 times

  **NejmeddineBch** 1 year, 9 months ago

Selected Answer: A



<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users>

Add new users or delete existing users from your Azure Active Directory (Azure AD) tenant. To add or delete users, you must be a User Administrator or Global Administrator.
upvoted 2 times

  **[Removed]** 1 year, 10 months ago



Selected Answer: A

<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>
-User Administrator
Create and manage all aspects of users and groups
Manage support tickets
Monitor service health
Change passwords for users, Helpdesk administrators, and other User Administrators
upvoted 3 times

  **[Removed]** 1 year, 10 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>
-User Administrator
Create and manage all aspects of users and groups
Manage support tickets
Monitor service health
Change passwords for users, Helpdesk administrators, and other User Administrators
upvoted 4 times

  **Renss78** 2 years, 1 month ago

Answer is NO, the one who just created the tenant is the only one who can add Users.
But when he assign "user 3" the User Administrator or Global Administrator role then he/she can.

And yes NOT only the Global Adminsitrator can add AD Users.

Source:

""Add new users or delete existing users from your Azure Active Directory (Azure AD) tenant. To add or delete users, you must be a User Administrator or Global Administrator."

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>

upvoted 5 times

  **AK4U_111** 2 years, 2 months ago

how can a tenant such as external.contoso.onmicrosoft.com even be created? i cant find anything on how to do this. when i go to create tenant i can create a new one but not a sub tenant which is a part of the original tenant

upvoted 2 times

  **tomasek88** 2 years, 2 months ago

NO = B --> because User2 OR User3 OR User4 - have nothing to do with NEW Azure Active Directory tenant named external.contoso.onmicrosoft.com

upvoted 1 times

  **JayLearn2022** 2 years, 2 months ago

There are several version of this question. The following are the valid and invalid solutions that may be presented.

Valid Solution: Meets the Goal

Solution: Solution: You instruct User1 to create the user accounts.

Invalid Solutions: Does not Meet the Goal

-Solution: You instruct User2 to create the user accounts.

-Solution: You instruct User3 to create the user accounts.

-Solution: You instruct User4 to create the user accounts.

upvoted 3 times

  **MothePro** 2 years, 1 month ago

what is the difference between user 1 and user2? they are both Global Admin..

upvoted 1 times

  **fateman17** 1 year, 9 months ago

user 1 made the tenant.

upvoted 1 times

  **myarali** 2 years, 2 months ago

NO

After User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com, User-1 becomes owner and Global Administrator of external.contoso.onmicrosoft.com.

BUT User-3 doesn't have any authorization in new tenant. User-3's User Administrator Role applies to contoso.onmicrosoft.com NOT for external.contoso.onmicrosoft.com.

SO User-1 CAN NOT instruct User3 to create the user accounts.

MAYBE that can be done after User-1 assigns Global Administrator or User Access Administrator Role to User-3.

upvoted 4 times

You have two Azure subscriptions named Sub1 and Sub2.

An administrator creates a custom role that has an assignable scope to a resource group named RG1 in Sub1.

You need to ensure that you can apply the custom role to any resource group in Sub1 and Sub2. The solution must minimize administrative effort.

What should you do?

- A. Select the custom role and add Sub1 and Sub2 to the assignable scopes. Remove RG1 from the assignable scopes.
- B. Create a new custom role for Sub1. Create a new custom role for Sub2. Remove the role from RG1.
- C. Create a new custom role for Sub1 and add Sub2 to the assignable scopes. Remove the role from RG1.
- D. Select the custom role and add Sub1 to the assignable scopes. Remove RG1 from the assignable scopes. Create a new custom role for Sub2.

Correct Answer: A

Community vote distribution

A (100%)

  **NaoVaz** Highly Voted 2 years, 7 months ago

Selected Answer: A

A) " Select the custom role and add Sub1 and Sub2 to the assignable scopes. Remove RG1 from the assignable scopes. "

To assure the solution minimizes the administrative effort, we just need to change the assignable scope list of the custom role.

Reference: <https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles#custom-role-properties>
upvoted 29 times

  **Mazinger** Highly Voted 2 years, 2 months ago

Selected Answer: A

To ensure that you can apply the custom role to any resource group in Sub1 and Sub2 while minimizing administrative effort, you should select the custom role and add both Sub1 and Sub2 to the assignable scopes.

In the Azure portal, navigate to the custom role that has been created and click on it.

By adding both Sub1 and Sub2 to the assignable scopes of the custom role, you can ensure that the role can be applied to any resource group in both subscriptions. This minimizes administrative effort by eliminating the need to create separate custom roles for each subscription.

Option B is not recommended as it would require creating a separate custom role for each subscription, which would increase administrative effort.

Option C is not recommended as it would only allow the custom role to be applied to resource groups in Sub1 and not Sub2.

Option D is not recommended as it would require creating a separate custom role for Sub2, which would increase administrative effort.

upvoted 10 times

  **[Removed]** Most Recent 8 months ago

Selected Answer: A

A is corerct
upvoted 1 times

  **AlbertKwan** 10 months, 4 weeks ago

Selected Answer: A

Finally, the community 100% agreed on a Correct answer.
upvoted 3 times


  **3c5adce** 11 months, 3 weeks ago

ChatGPT4 says A
upvoted 1 times

  **MCLC2021** 1 year ago

Selected Answer: A

A. Select the custom role and add Sub1 and Sub2 to the assignable scopes. Remove RG1 from the assignable scopes.
upvoted 1 times

  **BhunB** 1 year, 1 month ago

An easy way to remember this is that B, C, D all require to "create new custom roles".

The question is asking you to minimize administrative effort.

Answer A is the only outlier.
upvoted 6 times

  **Amir1909** 1 year, 2 months ago



A is correct
upvoted 1 times

  **Saurabh_Bhargav** 1 year, 2 months ago

a) "Custom roles can be shared between subscriptions that trust the same Microsoft Entra tenant"
it mean we can use the same custom role in sub1 and sub2.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles>
upvoted 1 times

  **Saurabh_Bhargav** 1 year, 2 months ago



C. Option
upvoted 1 times

  **NU88** 1 year, 4 months ago

Is Azure Custom Role a property of a subscription? or it sits above all subscriptions?
upvoted 1 times

  **AK4U_111** 2 years, 2 months ago

Answer is correct
upvoted 1 times

  **zellck** 2 years, 3 months ago

Selected Answer: A



A is the answer.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

If the Azure built-in roles don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group (in preview only), subscription, and resource group scopes.

Custom roles can be shared between subscriptions that trust the same Azure AD tenant.

upvoted 3 times

  **zellck** 2 years, 3 months ago



This option allows you to apply the custom role to any resource group in both Sub1 and Sub2, with minimal administrative effort as you are only modifying the scope of the existing custom role, instead of creating new roles for each subscription.
upvoted 1 times

  **[Removed]** 2 years, 3 months ago

on the test
upvoted 3 times



  **sourabhg** 2 years, 6 months ago

The correct answer is A.
upvoted 1 times

  **kerimnl** 2 years, 8 months ago

Selected Answer: A

Correct Answer is A for sure
upvoted 2 times

  **libran** 2 years, 8 months ago

Selected Answer: A

Correct Answer: A
upvoted 3 times

You have an Azure Subscription that contains a storage account named storageacct1234 and two users named User1 and User2. You assign User1 the roles shown in the following exhibit.

User1 assignments – storageacct1234

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (2)

Role	Scope	Group assignment	Condition
Reader	Resource group (inherited)	--	None
Storage Blob Data Contributor	This resource	--	Add

Deny assignments (0)

Classic administrators (0)

Which two actions can User1 perform? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. Assign roles to User2 for storageacct1234.

B. Upload blob data to storageacct1234.

C. Modify the firewall of storageacct1234.

D. View blob data in storageacct1234.

E. View file shares in storageacct1234.

Correct Answer: BD

Community vote distribution

BD (99%)

kerimnl

Highly Voted

2 years, 8 months ago

Selected Answer: BD

Correct Answer is:BD

upvoted 90 times

pmsiva

2 years, 6 months ago

For example, if you assign the Storage Blob Data Contributor role to user Mary at the level of a container named sample-container, then Mary is granted read, write, and delete access to all of the blobs in that container. However, if Mary wants to view a blob in the Azure portal, then the Storage Blob Data Contributor role by itself will not provide sufficient permissions to navigate through the portal to the blob in order to view it. The additional permissions are required to navigate through the portal and view the other resources that are visible there.

upvoted 18 times

virgilpza

Highly Voted

2 years, 8 months ago

Selected Answer: BD

correct answers: BD

upvoted 29 times

cvalladares123

1 year, 10 months ago

Storage Blob Data Contributor --> Read, write, and delete Azure Storage containers and blobs

Reader --> View all resources, but does not allow you to make any changes

Any permission has been granted at storage account level or file shares directly, so reading access to files share is not possible

upvoted 6 times

Diedo

1 year, 10 months ago

Azure file shares are deployed into storage accounts so I think it is BDE.

upvoted 6 times

  **Ben756** 1 year, 7 months ago

E is not the answer. The Reader role only grants User1 the permission to view the properties and metadata of the storage account, not the data inside it.

upvoted 9 times

  **lykeman26** 7 months, 4 weeks ago



The built-in Reader role in Azure actually does grant read access to view the contents of storage accounts, not just the metadata and properties. Specifically, a user assigned the Reader role on a storage account can:

List containers and blobs
Read blob contents
View queue messages
Read table entities
Read files in file shares

However, the Reader role is read-only. It does not allow creating, modifying, or deleting any data or resources within the storage account.

If you want to restrict a user to only viewing metadata and properties of the storage account without accessing the actual data, you would need to use a more limited custom role or adjust permissions at a more granular level.

upvoted 2 times

  **rodrod** 6 months, 1 week ago

no. what you are talking is " Storage Blob Data Reader" role not "Reader" role.

"Reader" role is just about management plane (settings, properties...), not data plane (content inside the containers)

upvoted 3 times

  **58b2872** Most Recent 4 months ago

Selected Answer: BD


View file shares in storageacct1234:

The Storage Blob Data Contributor role applies only to blobs and not to file shares. While the Reader role grants viewing permissions for file shares, User1 cannot manage file shares because the role does not provide such capabilities.

The correct answer is:

B. Upload blob data to storageacct1234
D. View blob data in storageacct1234

upvoted 1 times

  **Dankho** 7 months, 1 week ago

I concur, it's B and D. After some research I am good with this explanation:

Reader Role at the Resource Group Level: This role grants the ability to view all resources within the resource group, but it does not extend to viewing the contents of blob data or file shares in a storage account. User1 can see the storage account itself and its properties (like the account name, type, and configuration), but not the individual blob or file share data.

Storage Blob Data Contributor Role: This role allows User1 to perform actions related to blobs, including reading, writing, and deleting blob data specifically.

upvoted 1 times



  **[Removed]** 8 months ago

Selected Answer: BD

WRONG

B & D are correct



upvoted 1 times

  **Devs84** 8 months, 2 weeks ago

Selected Answer: BD

It has to be B and D

upvoted 1 times

  **CheMetto** 9 months, 1 week ago

Selected Answer: BD

Keep in mind there are 2 difference role in azure. 1 for resources, 1 for data. Even if you are owner of the subscription you can't access data, because you are managing resource, but can't access his data. In order to view and update data on a blob, you need storage blob data contributor, otherwise you can enable on Storage account level AD option, and you can access data as global admin



upvoted 1 times

  **SofiaLorean** 10 months, 1 week ago

I cleared the exam today. This question was in my exam. Thanks ET and everyone.

Most of the questions from ET.



upvoted 2 times



  **kyakya** 11 months, 2 weeks ago



Selected Answer: BD



read cannot read file share, because it have not any dataAction



upvoted 1 times



  **3c5adce** 11 months, 4 weeks ago
ChatGPT4 says B&D
upvoted 1 times


  **Vladds** 11 months, 4 weeks ago
Selected Answer: BD
It has to be B & D. The Reader role is scoped to resource group anyway
upvoted 2 times



  **Chris17** 12 months ago
Selected Answer: BD
correct answers: BD
upvoted 1 times



  **MCLC2021** 1 year ago
Selected Answer: BD
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#storage-blob-data-contributor>
upvoted 1 times



  **simplementeluca** 1 year, 1 month ago
This question was in exam 22/03/2024. My response BD
upvoted 4 times

  **MC420** 1 year, 1 month ago
Was it correct?
upvoted 1 times

  **Amir1909** 1 year, 1 month ago
B, D and E
upvoted 1 times

  **1828b9d** 1 year, 2 months ago
This question was in exam 01/03/2024
upvoted 3 times

  **MC420** 1 year, 1 month ago
What's the answer?
upvoted 1 times

  **LovelyGroovey** 1 year, 2 months ago
Correct answer: B and D. Why? Here is the answer: User1 can perform the following two actions based on their assigned roles:

Upload blob data to storageacct1234: User1 has been assigned the "Storage Blob Data Contributor" role for the storage account named storageacct1234. This role allows them to upload data to blob containers within that storage account.
View blob data in storageacct1234: Additionally, User1 has the "Reader" role at the Resource group (inherited) scope. While this role doesn't provide read permissions to data in Azure Storage, it does allow User1 to view storage account resources, including blob containers. Therefore, User1 can view blob data within the storageacct1234 storage account.
upvoted 4 times

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.

You need to view the error events from a table named Event.

Which query should you run in Workspace1?

- A. select * from Event where EventType == "error"
- B. Event | search "error"
- C. Event | where EventType is "error"
- D. Get-Event Event | where {\$_.EventType == "error"}

Correct Answer: B

Community vote distribution

B (100%)

TheB Highly Voted 2 years, 3 months ago

Selected Answer: B
Correct answer is B
other correct answer option can come in the following form:
Search in (Event) "Error"
Event | where eventType = "Error"
upvoted 14 times

lebeyic620 1 year, 1 month ago
Shouldn't the last one have double 'equal to'?
upvoted 4 times

MCLC2021 Highly Voted 1 year ago

Selected Answer: B
<https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/search-operator>
<https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/kql-quick-reference>
Use the | (pipe) operator to separate multiple commands.
Use the let keyword to create variables.
Use the where keyword to filter results.
Use the project keyword to select specific columns.
Use the summarize keyword to group and aggregate data.

The syntax is:
Table_name | search "search term"
Note:
There are several versions of this question in the exam. The question has three possible correct answers:
1. search in (Event) "error"
2. Event | search "error"
3. Event | where EventType == "error"
upvoted 10 times

Mark74 Most Recent 5 months ago

Selected Answer: B
B is correct answer
upvoted 1 times

[Removed] 8 months ago

Selected Answer: B
B is corect
upvoted 2 times

jecampos2 1 year, 2 months ago

Selected Answer: B
Correct answer is B
upvoted 1 times

Studyingengineer 1 year, 5 months ago
Will be doing exam next week. If this question isn't in my exam i sue Examtopics :P

upvoted 6 times

  **pinyonet** 1 year, 6 months ago

Selected Answer: B

Correct answer is B

There are several versions of this question in the exam. The question has three possible correct answers:

- 1. search in (Event) "error"
- 2. Event | search "error"
- 3. Event | where EventType == "error"



upvoted 1 times

  **ST5V5N** 1 year, 8 months ago

Its A

https://www.google.com/search?q=select+*+from+Event+where+EventType+%3D%3D+%22error%22&rlz=1C1CHBF_en-GBGB1039GB1039&oq=select+*+from+Event+where+EventType+%3D%3D+%22error%22&aqs=chrome..69i57j33i10i160l4.766j0j7&sourceid=chrome&ie=UTF-8

upvoted 1 times

  **Athul07** 1 year, 11 months ago



To view the error events from the "Event" table in Azure Log Analytics workspace "Workspace1," you should run the following query:

A. select * from Event where EventType == "error"

This query selects all records from the "Event" table where the EventType is equal to "error," allowing you to filter and view only the error events.

Note: Option B is not a valid Log Analytics query syntax, and options C and D use incorrect syntax for Log Analytics queries.

upvoted 2 times

  **Afsan** 2 years, 3 months ago

Event | search "error"

upvoted 2 times



  **ccemyilmazz** 2 years, 3 months ago

Selected Answer: B

Both B & C are OK, other possibilities are:

- 1) Event | search "Error"
- 2) Event | where eventType = "Error"
- 3) Search in (Event) "Error"

upvoted 3 times

  **ccemyilmazz** 2 years, 3 months ago

BTW, I just saw that "C" is NOT OK, My mistake

upvoted 2 times

  **khaled_razouk** 2 years, 4 months ago

Selected Answer: B

B. Event | search "error"

upvoted 2 times

You have an Azure App Services web app named App1.

You plan to deploy App1 by using Web Deploy.

You need to ensure that the developers of App1 can use their Azure AD credentials to deploy content to App1. The solution must use the principle of least privilege.

What should you do?

- A. Assign the Owner role to the developers
- B. Configure app-level credentials for FTPS
- C. Assign the Website Contributor role to the developers
- D. Configure user-level credentials for FTPS

Correct Answer: C

Community vote distribution

C (98%)

  **Mazinger** Highly Voted 2 years, 2 months ago

Selected Answer: C

C. Assign the Website Contributor role to the developers.

To allow the developers of App1 to use their Azure AD credentials to deploy content to App1 using Web Deploy, you should assign the Website Contributor role to the developers. This role provides the necessary permissions for developers to deploy content to the web app, but does not grant them excessive permissions that could be used to make unwanted changes.

Option A is not recommended as it would grant excessive permissions to the developers, which could be used to make unwanted changes.

Option B and D are not relevant to the scenario as the question is specifically asking for how to use Azure AD credentials for Web Deploy, not FTPS.

Option C is a potential solution, but the Website Contributor role provides a more targeted and appropriate level of permissions for the scenario.

upvoted 49 times

  **lebeyic620** 1 year, 1 month ago

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/web-and-mobile#website-contributor>

upvoted 1 times

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

Selected Answer: C

B is wrong because:

"To secure app deployment from a local computer, Azure App Service supports two types of credentials for local Git deployment and FTP/S deployment. These credentials are not the same as your Azure subscription credentials."

<https://learn.microsoft.com/en-us/azure/app-service/deploy-configure-credentials?tabs=cli>

Correct is C.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#website-contributor>

Microsoft.Resources/deployments/* - Create and manage a deployment

upvoted 30 times

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

Selected Answer: C

The Website Contributor role allows developers to manage web apps, including the ability to deploy content, without giving them broader permissions that come with roles like Owner

upvoted 1 times

  **Mark74** 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: C



it's C

upvoted 1 times

  **mojo86** 8 months, 3 weeks ago

Answer is C: The app-level credentials for FTPS do not allow deployment of content to an Azure App Services web app using Azure AD credentials.

upvoted 1 times

  **azmlan** 9 months, 1 week ago

Based on the information from the Azure documentation, the best solution is:
C. Assign the Website Contributor role to the developers
Here's why:
The Website Contributor role allows developers to manage websites, but not the underlying web plans. This adheres to the principle of least privilege by granting the minimum permissions needed to deploy the web app.
Some key points about the Website Contributor role:
It allows creating and managing websites
Developers can deploy content to websites they have access to
It does not allow managing the App Service plans or assigning roles to others

upvoted 1 times

  **testtaker09** 10 months, 3 weeks ago



was in the exam today 17/06/2024

upvoted 3 times

  **edurakhan** 11 months ago

on exam today 6/6/2024

upvoted 2 times

  **3c5adce** 11 months, 4 weeks ago

C. Assign the Website Contributor role to the developers
This role provides the necessary permissions for developers to deploy content to App1 using Web Deploy, adheres to the principle of least privilege by restricting permissions to what is needed for web deployment, and integrates with Azure AD for authentication.

upvoted 1 times

  **MCLC2021** 1 year ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/web-and-mobile#website-contributor>

upvoted 2 times

  **MCLC2021** 1 year ago

"using web deploy" --> It is not using FTP , so B y D incorrect..
"Least privilege" --> Answer A incorrect.



C is correct.

upvoted 4 times

  **smirnoffpremium** 1 year, 1 month ago

Passed AZ-104 today 03/07/24 879%.
99% of Examtopics questions in my test with exact same wording.
This question was on the test, I answered C.
Very Thanks to Examtopics.

upvoted 6 times

  **Seppi** 1 year, 1 month ago

good to hear, did you learn with the free version or did you buy all questions?

upvoted 2 times

  **LinuxLewis** 1 year, 2 months ago

I dont think it is C, as the role says:
{
"assignableScopes": [
"/"
],
"description": "Lets you manage websites (not web plans), but not access to them.",
"id": "/providers/Microsoft.Authorization/roleDefinitions/de139f84-1756-47ae-9be6-808fbbe84772",
"name": "de139f84-1756-47ae-9be6-808fbbe84772",

part of question is to ensure devs can use creds, so I think this is related to that. also dont see in JSON the append or modify action.



upvoted 1 times

  **lebeyic620** 1 year, 1 month ago

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/web-and-mobile#website-contributor>

Role has:
Microsoft.Resources/deployments/* Create and manage a deployment

upvoted 1 times

  **bacana** 1 year, 2 months ago



I beleve B is correct.
<https://learn.microsoft.com/en-us/azure/app-service/deploy-ftp?tabs=portal>

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

C is correct

upvoted 1 times

  **stanislaus450** 1 year, 2 months ago

Selected Answer: C

The correct answer is:

C. Assign the Website Contributor role to the developers.

Explanation:

Assigning the Website Contributor role to the developers would grant them the necessary permissions to deploy content to the Azure App Services web app (App1) without giving them excessive privileges. This role provides the necessary permissions for managing the website, including deployment, without granting ownership or administrative rights, thus adhering to the principle of least privilege.

upvoted 2 times

  **adilkhan** 1 year, 3 months ago

100% C is correct

upvoted 1 times

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

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: From Azure AD in the Azure portal, you use the Bulk invite users operation.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (73%)

A (27%)

- Georgego**

Highly Voted

 2 years, 3 months ago

Selected Answer: B

The Answer supplied is correct, it is No.
Reason:
The question states "You have a CSV file that contains the names and email addresses of 500 external users."
This implies that the required fields (Email and Redirection URL)are missing from the .csv file.
Here are the csv field pre-requisites that are needed for bulk upload of external users:
<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#prerequisites>
upvoted 71 times
- GreenTick** 5 months, 1 week ago

Microsoft do not intend to trick you to identifying incomplete/missing bits and pieces requirement for the scenario but have correct solution, the question is whether the solution to use bulk invite fit using CSV will fit the requirement to create guess users.

upvoted 3 times
- MeysamBayani** 2 years, 3 months ago

I think you can add Redirection url [inviteRedirectURL] for all user same <https://myapplications.microsoft.com> so it is possible we use Bullk

upvoted 6 times
- rodrod** 6 months, 1 week ago

if you change the wording of the question asking if the step they describe is correct, then yes it's possible with that CSV file. I guess it's even a YES if they said the CSV file only have names , as you would have said you can add manually those emails before the bulk :-)

upvoted 1 times
- sjsaran** 1 year, 7 months ago

It is correct, redirection URL is not based on the end user, organization can decide
Answer : A

upvoted 3 times
- shadad** 2 years, 2 months ago

He is not talking about the idea of using the Bulk, its the CSV file that not containing the right requirements for this task! you need the Email + Redirection URL so you can use it with Bulk invite.....not the Email + names !!

This Question mentioned on many versions. pay attention to the words.

upvoted 18 times
- alfaAzure** 1 year, 7 months ago

B, is correct. Refer to the question, be comprehensive, too much technicality guys.

upvoted 3 times

🗨️ 👤 **Muffay** Highly Voted 👍 2 years, 4 months ago

Selected Answer: A

Answer should be yes:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite>

Though, a new CSV file with additional information would need to be created.

"Required values are:

Email address to invite - the user who will receive an invitation

Redirection url - the URL to which the invited user is forwarded after accepting the invitation. If you want to forward the user to the My Apps page, you must change this value to <https://myapps.microsoft.com> or <https://myapplications.microsoft.com>."

upvoted 18 times

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

But it doesnt specify that you have the redirection URL. It says you only have the Names and email addresses. If it did specify then I would say Yes, but this isnt the case.

upvoted 8 times

🗨️ 👤 **Highgate** 8 months, 3 weeks ago

The MSLearn page says you can use <https://myapps.microsoft.com> or <https://myapplications.microsoft.com>. It says downloading a template CSV and validating the CSV you upload is part of the process, so you would just add the redirect URL. The solution meets the goal. Answer A.

upvoted 2 times

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

Incorrect

upvoted 2 times

🗨️ 👤 **4f45fce** Most Recent 🕒 2 weeks, 3 days ago

Selected Answer: A

The Bulk invite users operation in the Azure AD portal is specifically designed to:

Import a CSV file containing user details.

Invite multiple external (guest) users to your Azure AD tenant at once.

Since your goal is to create guest user accounts for 500 external users listed in a CSV file, this method is both correct and efficient.

upvoted 1 times

🗨️ 👤 **kriChe27** 1 month, 1 week ago

Selected Answer: A

Yes, using the Bulk invite users operation in Azure AD will meet the goal. This feature allows you to invite multiple external users as guest users by uploading a CSV file with their details.

Here's a brief overview of the process:

Prepare the CSV file: Ensure the file contains the required information, such as email addresses and invitation preferences.

Upload the CSV file: Navigate to Azure Active Directory > Users > Bulk operations > Bulk invite in the Azure portal.

Verify and submit: After uploading the file, Azure will validate the contents. Once validated, you can submit the bulk invitation operation.

This method efficiently handles the creation of guest user accounts for a large number of external users.

upvoted 1 times

🗨️ 👤 **janakaniranjan** 1 month, 1 week ago

Selected Answer: A

Explanation:

Azure Active Directory (Azure AD) allows bulk creation of guest users using the "Bulk invite users" operation in the Azure portal. This operation is specifically designed for inviting multiple external users (B2B guests) using a CSV file.

Steps for Bulk Inviting Users:

Navigate to Azure Active Directory in the Azure portal.

Go to Users > Bulk operations > Bulk invite users.

Upload the CSV file containing the names and email addresses of the 500 external users.

Azure AD sends invitation emails to these external users, allowing them to join as guest users.

Since the requirement is to create guest user accounts for external users, this method perfectly meets the goal.

Why the Answer is NOT B (No)?

The Bulk invite users operation is the correct and recommended approach for adding multiple external users efficiently.

No need for manual user creation or custom scripts, which would increase administrative effort.

upvoted 1 times



🗨️ 👤 **GarrethM** 2 months ago

Selected Answer: A

The Bulk invite users operation in Azure Active Directory (Azure AD) allows you to create multiple guest user accounts at once by uploading a CSV file. Since you have a CSV file with names and email addresses, this method is appropriate for inviting 500 external users as guests to your contoso.com tenant.

After the bulk invite, each external user will receive an email invitation to join as a guest. Once they accept, they can access resources based on their assigned permissions.

upvoted 1 times

  **Jakub4444** 2 months, 1 week ago

Selected Answer: A

Yes, this solution meets the goal.

The Bulk invite users operation in Azure Active Directory (Azure AD) allows you to import multiple guest users from a CSV file. Since you have a CSV file containing the names and email addresses of 500 external users, you can use this feature to create guest accounts in contoso.com.

Steps:

Go to Azure AD in the Azure portal.

Navigate to Users > Bulk operations > Bulk invite users.

Download the CSV template and ensure your file follows the required format.

Upload your CSV file containing the users' details.

Review and submit the request.

Each invited guest user will receive an invitation email.

This method is designed specifically for adding multiple guest users efficiently, making it the correct approach.

upvoted 3 times

  **Bravo_Dravel** 3 months, 3 weeks ago

Selected Answer: A

Steps for Bulk Inviting Users:

Navigate to Azure Active Directory in the Azure portal.

Select Users > Bulk create.

Choose the Invite guest users option.



Download the CSV template provided by Azure, if necessary.

Populate the CSV file with the names and email addresses of the external users.

Upload the completed CSV file.

Review the information and start the bulk invite operation.

upvoted 2 times

  **58b2872** 4 months ago



Selected Answer: B

Open the .csv template and add a line for each guest user. Required values are:

Email address to invite - the user to whom you want to send an invitation.

Redirection url - the URL to which the invited user is forwarded after accepting the invitation. If you want to forward the user to the My Apps page, you must change this value to <https://myapps.microsoft.com> or <https://myapplications.microsoft.com>.

upvoted 1 times

  **ankeshpatel2112** 4 months, 1 week ago

Selected Answer: A

Based on Question : Yes you can bulk invite users (Go to Active Directory >> Users >> Bulk Invite Users)

upvoted 1 times

  **minura** 4 months, 2 weeks ago

Selected Answer: B

Email and Redirection URL are required fields

upvoted 1 times

  **Announcement** 5 months, 2 weeks ago

answer is no..

look at point number 5.

<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite#understand-the-csv-template>

upvoted 1 times

  **junkz** 5 months, 4 weeks ago

if this is a no, then question 40 must be a no too, the only difference is that there we do it by powershell. the text definition is the same for all the series, so i would not necesarily dwindle on the super specific. i believe the process is what is evaluated here

upvoted 2 times

  **Chuong0810** 6 months ago

Selected Answer: A

For guest users, you would generally use the Bulk invite feature.

Steps can do:

Prepare the CSV file:

Ensure your CSV file is formatted correctly with the required columns, such as EmailAddress and DisplayName.

Navigate to Azure AD:

In the Azure portal, go to Azure Active Directory.



Bulk invite users:

Select Users.

Click on Bulk operations and then Bulk invite.

Upload your CSV file and follow the prompts to invite the users

upvoted 1 times

  **Dankho** 6 months, 2 weeks ago

Selected Answer: A

Going with Yes because you're just creating them, you're not inviting them. Here is Gemini...

You're absolutely right. The document you linked (<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite>) does mention that a "Redirection URL" is a required field for bulk invitations. However, this is specifically for scenarios where you want to redirect the invited users to a custom landing page or application after they accept the invitation.

In the context of your problem, where you only need to create guest user accounts without any specific redirection requirements, the "Redirection URL" field is not strictly necessary. Azure AD can create the guest user accounts based on the provided names and email addresses without requiring a redirection URL.

Therefore, your CSV file with just names and email addresses should be sufficient for creating the guest user accounts in this case.

upvoted 2 times

  **Bokhtar** 7 months ago

bulk invite needs names email and redirection url which is missing so the answer is NO

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct

a PowerShell script must be created that runs the New-AzureADMSInvitation cmdlet for each external user.

look at Q40 (Topic 1)

upvoted 3 times

HOTSPOT -

You have an Azure subscription that is linked to an Azure AD tenant. The tenant contains the custom role-based access control (RBAC) roles shown in the following table.

Name	Description
Role1	Azure subscription role
Role2	Azure AD role

From the Azure portal, you need to create two custom roles named Role3 and Role4. Role3 will be an Azure subscription role. Role4 will be an Azure AD role.

Which roles can you clone to create the new roles? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role3:

Role1 only

Built-in Azure subscription roles only

Role1 and built-in Azure subscription roles only

Built-in Azure subscription roles and built-in Azure AD roles only

Role1, Role2, built-in Azure subscription roles, and built-in Azure AD roles

Role4:

Role2 only

Built-in Azure AD roles only

Role2 and built-in Azure AD roles only

Built-in Azure AD roles and built-in Azure subscription roles only

Role1, Role2, built-in Azure AD, and built-in Azure subscription roles

Answer Area

Role3:

Role1 only

Built-in Azure subscription roles only

Role1 and built-in Azure subscription roles only

Built-in Azure subscription roles and built-in Azure AD roles only

Role1, Role2, built-in Azure subscription roles, and built-in Azure AD roles

Correct Answer:

Role4:

Role2 only

Built-in Azure AD roles only

Role2 and built-in Azure AD roles only

Built-in Azure AD roles and built-in Azure subscription roles only

Role1, Role2, built-in Azure AD, and built-in Azure subscription roles

TorresW

Highly Voted

2 years, 3 months ago

<https://www.examtopycs.com/discussions/microsoft/view/57784-exam-az-500-topic-2-question-58-discussion/>

i found similar questions in other page

upvoted 30 times



jimmyml



2 years, 3 months ago



Thanks. Answer should be



Role3: Role1 and built-in Azure subscription roles only



Role4: Role2 only
Explanation: You cannot clone built-in Azure AD role
upvoted 165 times



  **ChrisEkorhi** 1 year, 10 months ago
This is the correct answers
Role3: Role1 and built-in Azure subscription roles only
Role4: Role2 only - For Azure AD role, you can only clone from custom role like Role 2 and cannot clone from built-in role. Please ge test yourself using Azure free account.
upvoted 8 times



  **shandorcoachman** 2 years, 2 months ago
What about this: <https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal> ? It seems you can.
upvoted 2 times



  **shandorcoachman** 2 years, 2 months ago
Correcting myself, this is a subscription role.
upvoted 7 times




  **Paul_white** 2 years, 2 months ago
This is the best answer here!!!
<https://www.examttopics.com/discussions/microsoft/view/57784-exam-az-500-topic-2-question-58-discussion/>
upvoted 4 times



  **Panapi** 2 years, 2 months ago
Answer is correckt Valid! This question was on the exam 22/02/2023. Scored 920. Thanks guys!
upvoted 23 times




  **Sandip671** 1 year, 6 months ago
Hiii my exam are in 10 days plz help me to make my concepts clear
upvoted 1 times



  **neolisto** 1 year, 5 months ago
Sandip671 how your exam? Did you pass it?
upvoted 3 times



  **ki01** 1 year, 4 months ago
it's usually a bad idea to book an exam soon when you have very little idea of what you're doing....
upvoted 2 times

  **EIDakhli** Highly Voted  2 years, 3 months ago
Role3: Role1 and Azure subscription Roles only.
Role4: Role2 only
Explanation:
There's a difference between Built-in AD roles and Built-in Subscription roles.
Built-in AD roles can't be cloned, but built-in subscription roles can be. Custom roles of either type can be cloned.
To clone the Bulit-in subscription Role, you open the subscription or the Resource group where you want to create the custom role and assign the permissions --> Go to Access Control (IAM) --> Roles tab --> Search for the subscription Role then clone it from the three dots in the right of the role.
Reference: <https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>
upvoted 27 times

  **Georgego** 2 years, 3 months ago
Tested in LAB environment and can confirm
Role3: Role1 and Azure subscription Roles only.
Role4: Role2 only
upvoted 13 times

  **feralberti** Most Recent  6 months, 2 weeks ago
From Azure AD roles: "You can clone the baseline permissions from a custom role but you can't clone a built-in role."
<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/custom-create>
So the question is kind of ambiguous, in the end what you want to clones are the permissions of the role, in that case the answer provided is correct, if you take it literally (as i would do) then it should be "Role 2 only"
upvoted 2 times



  **d7fb451** 7 months, 1 week ago
<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/custom-create>
upvoted 1 times



  **[Removed]** 8 months ago
WRONG

Role3: Role1 and built-in Azure subscription roles only
Role4: Role2 only
upvoted 2 times



  **certainly** 8 months, 3 weeks ago

Not sure if I am the only one being confused by the correct answer discussed here.
Role3: Role1 and built-in Azure subscription roles only
To create an Azure subscription role, you can clone existing Azure subscription roles Role1. it is a valid template. Built-in Azure subscription roles can also be used. But not necessary cloning BOTH.
So correct answer should
Role3: Role1 only
Role4: Role2 only
upvoted 1 times



  **certainly** 7 months, 1 week ago
nvm. i got it now. correct answer
Role3: Role1 and Azure subscription Roles only.
Role4: Role2 only
upvoted 1 times



  **CheMetto** 9 months, 1 week ago
In other exam, i always answered custom role of azure + builtin, and custom role for entra id, but i found out is wrong on azure side, try it on your own! I created a custom role, even 2 days ago, then on IAM i search it and click on "Clone role". This role wasn't clonable, i could even find it on the search manually. So the answer is:



Azure can copy only from built-in Azure Role, so is the second one.
For Azure AD (Entra ID), you can copy only from custom role, so is the first one
upvoted 1 times



  **CheMetto** 9 months, 1 week ago
You don't need to get a subscription to test it, just in portal.azure.com, search for management group -> create a new one -> access the new one -> go to IAM -> create a custom role -> try to clone it! You get what i'm talking about, nothing!



I thought it was also an issue withing my tenant, so i decide to go on another oldest tenant... same issue! Can't clone a role which is not a built-in azure subscription role
upvoted 1 times



  **CheMetto** 9 months, 1 week ago
i was wrong. it was a bug/issue of my tenant. i could do that on another one
upvoted 1 times

  **ajay01avhad** 9 months, 1 week ago
For Role3, you should select: Role1 and built-in Azure subscription roles only
For Role4, you should select: Role2 and built-in Azure AD roles only
upvoted 1 times



  **varinder82** 11 months, 3 weeks ago
Final Answer:
Role3: Role1 and built-in Azure subscription roles only
Role4: Role2 only
upvoted 3 times



  **3c5adce** 11 months, 4 weeks ago
Role3: Role1 and built-in Azure subscription roles only
Role4: Role2 only
Explanation: You cannot clone built-in Azure AD role
upvoted 1 times



  **Amir1909** 1 year, 2 months ago
Role3: Role1 and built-in subscription roles only
Role4: Role2 only
upvoted 4 times

  **mihir25** 1 year, 5 months ago
Thanks. Answer should be
Role3: Role1 and built-in Azure subscription roles only
Role4: Role2 only
Explanation: You cannot clone built-in Azure AD role

I've done Scenario and it's true that role 3 = role 1 + azure ad role
role 4 = role 2
upvoted 1 times

  **pradeepbadisa** 1 year, 7 months ago
Built-in AD roles can't be cloned, but built-in subscription roles can be. Custom roles of either type can be cloned.
upvoted 1 times

  **Babustest** 1 year, 7 months ago
I have tested this in lab. Role4 can be cloned only from Role2. When I try to create a new AD role, it's giving only one option 'Clone from a custom role'.
upvoted 1 times

  **Prasis** 1 year, 7 months ago

Role3: Role1 and built-in Azure subscription roles only

Role4: Role2 only

https://www.youtube.com/watch?v=qbnuwEohUbo&list=PLIKA5U_Yqgof3H0YWhzvarFixW9QLTr4S&index=46



upvoted 4 times

  **SL4Y3R_111** 1 year, 7 months ago

Role3: Role1 and built-in Azure subscription roles only

Role4: Role2 only

upvoted 2 times

  **oopspruu** 1 year, 8 months ago

There is a difference between Azure Roles and Azure AD Roles. Their "cloning" rules are not the same. While you can clone an in-built Azure role, you CANNOT clone in-built Azure AD role. When creating a custom role in Azure AD, you can either choose a custom role already created OR start from scratch. So for 2nd, Answer should be Role2 only.

upvoted 1 times

DRAG DROP

-

You have an Azure subscription named Sub1 that contains two users named User1 and User2.

You need to assign role-based access control (RBAC) roles to User1 and User2. The users must be able to perform the following tasks in Sub1:

- User1 must view the data in any storage account.
- User2 must assign users the Contributor role for storage accounts.

The solution must use the principle of least privilege.

Which RBAC role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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.

RBAC roies

Owner

Contributor

Reader and Data Access

Storage Account Contributor

Answer Area

User1:



User2:

Answer Area



Correct Answer:



User1: Reader and Data Access



User2: Owner

-   **Muffay** Highly Voted 2 years, 4 months ago

Answer is correct.
"Reader and Data Access":
"Lets you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys."

"Owner" is needed to manage permissions, as "User Access Administrator" is not offered as an option.
upvoted 96 times
-   **mohsanarfandanish** Highly Voted 2 years, 1 month ago

Cleared Exam 930 was appeared in exam 18/3/2023 ANS most upvoted
upvoted 19 times
-   **kriChe27** Most Recent 1 month, 1 week ago

User1:
Assign the Reader and Data Access role. This role allows User1 to view all resources, including data in storage accounts, without granting permissions to modify or delete the data.
User2:
Assign the Owner role. This role allows User2 to manage all resources, including assigning roles to other users, which covers the requirement to assign the Contributor role for storage accounts.
This ensures that User1 can view data in storage accounts and User2 can assign roles to other users, adhering to the principle of least privilege.
upvoted 1 times
-   **nnamacha** 1 month, 3 weeks ago

There is no role called read and data access. So it's contributor and Storage account contributor
upvoted 1 times

🗨️ 👤 **vombat186** 1 month ago
WRONG. <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#reader-and-data-access>
upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago
CORRECT

since User Access Administrator is not provided in the options to follow the less privilege principle, the owner is correct for sure.
upvoted 2 times

🗨️ 👤 **18c2076** 1 year, 1 month ago
Storage Account Contributor does not follow the principle of least privilege. Storage Account Contributor would allow a user that is requested to ONLY have the ability to READ/VIEW the data in the storage account, to do many other things such as Write/List/Delete/Move the data in the storage accounts. They only need to be able to view/read. Therefore, Reader, and Data Access follow this principle.

RBAC roles for Storage Accounts:
Role: Read and Data Access - Lets you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.

Please see reference documentation from MS Learn on Read and Data Access role:
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#reader-and-data-access>
upvoted 1 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago
Correct
upvoted 1 times

🗨️ 👤 **jeru81** 1 year, 3 months ago
Answer is wrong.
there is a 5th option User Access Administrator, which is cut out here. You see the 5 dots?
-Reader and Data Access
-User Access Administrator

;)
upvoted 9 times

🗨️ 👤 **MSBITSM** 1 year, 2 months ago
If there was indeed an option for User Access Administrator, that would be correct.
But in this case, owner will do the trick.
upvoted 2 times

🗨️ 👤 **devops_devops** 1 year, 3 months ago
This question was in exam 15/01/24
upvoted 3 times

🗨️ 👤 **Ahkhan** 1 year, 5 months ago
I got this question today in my exam—11/14 2023.
upvoted 3 times

🗨️ 👤 **Azc_T** 1 year, 4 months ago
Did you use free access? Are these questions from free access enough to clear exam.
upvoted 1 times

🗨️ 👤 **Rednevi** 1 year, 7 months ago
Remember:
Contributor can NOT assign roles
upvoted 2 times

🗨️ 👤 **Alandt** 1 year, 4 months ago
Exactly, only owner if I'm correct?
upvoted 1 times

🗨️ 👤 **fe0b3b4** 1 year, 4 months ago
Also User Access Administrator:

User Access Administrator: can assign roles but can't do anything with the actual resources, so manages access but not the resources.



Contributor: can do everything with the actual resources but can't assign roles, so manages the resources but not the access to them.

Owner: can do everything, most powerful role in Azure.
upvoted 3 times

🗨️ 👤 **Alandt** 1 year, 3 months ago
Good point!
upvoted 1 times

🗨️ 👤 **Rams786** 1 year, 7 months ago

This question was on my exam on 22 Sep 2023. scored 900 i answered most Voted
upvoted 3 times

  **Azc_T** 1 year, 4 months ago



Did you use free access? Are these questions from free access enough to clear exam
upvoted 1 times

  **Indy429** 1 year, 4 months ago

No you should get Contributor access to be able to go through everything, especially the case studies
upvoted 1 times

  **3c5adce** 12 months ago



How do you access the case studies?
upvoted 1 times

  **rodrod** 6 months, 1 week ago

he just explained...
upvoted 1 times

  **skavichal** 1 year, 10 months ago

user 1 Reader and data access
user2 should be owner, Storage Account Contributor can't be possible as it can read roles and roles assignment but can't assign any role to user.
upvoted 2 times

  **Athul07** 1 year, 11 months ago

User1: Reader
User2: Storage Account Contributor
upvoted 1 times

  **18c2076** 1 year, 1 month ago

Storage Account Contributor does not follow the principle of least privilege. Storage Account Contributor would allow a user that is requested to ONLY have the ability to READ/VIEW the data in the storage account, to do many other things such as Write/List/Delete/Move the data in the storage accounts. They only need to be able to view/read. Therefore, Reader, and Data Access follow this principle.

RBAC roles for Storage Accounts:

Role: Read and Data Access - Lets you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.

Please see reference documentation from MS Learn on Read and Data Access role:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#reader-and-data-access>

upvoted 1 times

  **SIAMIANJI** 1 year, 11 months ago

User1: Storage Account Contributor
User2: Owner
upvoted 2 times

  **18c2076** 1 year, 1 month ago

Storage Account Contributor does not follow the principle of least privilege. Storage Account Contributor would allow a user that is requested to ONLY have the ability to READ/VIEW the data in the storage account, to do many other things such as Write/List/Delete/Move the data in the storage accounts. They only need to be able to view/read. Therefore, Reader, and Data Access follow this principle.



RBAC roles for Storage Accounts:

Role: Read and Data Access - Lets you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.

Please see reference documentation from MS Learn on Read and Data Access role:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#reader-and-data-access>

upvoted 1 times

  **zellck** 2 years, 3 months ago

User1: Read and Data Access
User 2: Owner

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader-and-data-access>

Lets you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner>

Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

upvoted 10 times

  **Whatsamattr81** 2 years, 3 months ago

View Data in ANY storage account (assume storage account only)

Reader and Data Access gives a lot more than just storage account permissions - but Storage account contributor gives you access to do a lot ore than just Read / View data. Tricky one. Neither choices are perfect. But SAC role lets you do more than just 'view' data...

upvoted 3 times

  **18c2076** 1 year, 1 month ago

Its not okay to be wrong in this instance where you're vomiting it all over the internet.

Storage Account Contributor does not follow the principle of least privilege. Storage Account Contributor would allow a user that is requested to ONLY have the ability to READ/VIEW the data in the storage account, to do many other things such as Write/List/Delete/Move the data in the storage accounts. They only need to be able to view/read. Therefore, Reader, and Data Access follow this principle.

RBAC roles for Storage Accounts:

Role: Read and Data Access - Lets you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.

Please see reference documentation from MS Learn on Read and Data Access role:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#reader-and-data-access>

upvoted 1 times

  **lkjsatlwjwwge** 2 years, 3 months ago

It's true that Reader&Data Access allows writing, but you need to grant the role with the least permissions that will allow viewing, and according to <https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal>, Storage Acct Contributor gives you even more permissions. So it ought to be R&DA.

upvoted 1 times

You have an Azure subscription that contains 10 virtual machines, a key vault named Vault1, and a network security group (NSG) named NSG1. All the resources are deployed to the East US Azure region.

The virtual machines are protected by using NSG1. NSG1 is configured to block all outbound traffic to the internet.

You need to ensure that the virtual machines can access Vault1. The solution must use the principle of least privilege and minimize administrative effort



What should you configure as the destination of the outbound security rule for NSG1?

- A. an application security group
- B. a service tag
- C. an IP address range

Correct Answer: B



Community vote distribution

B (100%)

-   **Iszy** Highly Voted 2 years, 3 months ago



The correct answer is B. a service tag.

In order to ensure that the virtual machines can access Vault1 while also using the principle of least privilege and minimizing administrative effort, you should configure a service tag as the destination of the outbound security rule for NSG1. Service tags represent a group of IP addresses associated with Azure PaaS and SaaS services. By specifying a service tag as the destination of the outbound security rule, you can allow the virtual machines to access Vault1 without having to manually specify the IP addresses of Vault1. This reduces administrative effort and ensures that the virtual machines are only able to access Vault1, rather than any other internet destination.

upvoted 77 times
-   **Muffay** Highly Voted 2 years, 4 months ago

Selected Answer: B



B - Service Tag is correct.
<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags>
"AzureKeyVault" tag can be used in outbound NSGs.

upvoted 26 times
-   **kriChe27** Most Recent 1 month, 1 week ago



Selected Answer: B

To ensure that the virtual machines can access Vault1 while adhering to the principle of least privilege and minimizing administrative effort, you should configure the destination of the outbound security rule for NSG1 to use
B. a service tag.



Specifically, you should use the AzureKeyVault service tag. This service tag represents the IP addresses used by Azure Key Vault, allowing your virtual machines to access Vault1 without opening broader access to the internet.

upvoted 2 times
-   **kriChe27** 1 month, 1 week ago

AzureKeyVault service tag specifically represents the IP addresses used by Azure Key Vault. By using this service tag in your network security group (NSG) rules, you can allow or deny traffic to and from Azure Key Vault without needing to specify individual IP addresses. This is particularly useful for scenarios where you want to ensure secure access to your key vaults while blocking other outbound traffic.
For example, if you want your virtual machines to access Vault1, you can create an outbound security rule in NSG1 with the destination set to the AzureKeyVault service tag. This allows the VMs to communicate with Azure Key Vault while keeping other outbound traffic blocked



upvoted 1 times
-   **rodrod** 6 months, 1 week ago

it says " least privilege"
but B will give access to all vaults, not only vault1.
I don't like this question.
I would rather answer C and create a private endpoint to vault1 but one will say the question does not say there is a private endpoint, and it says least administrative task....
Those days, Who wants to favor less admin task compare to least permissions??



upvoted 4 times
-   **[Removed]** 8 months ago



Selected Answer: B



B is correct
upvoted 1 times



  **3c5adce** 11 months, 4 weeks ago
B. a service tag

Service tags in Azure simplify the security definition for Azure services, allowing you to define network access controls on NSG rules without having to know the specific IP addresses. Specifically, you can use the "AzureKeyVault" service tag to enable virtual machines to access Azure Key Vault services like Vault1, securely and efficiently. This approach directly aligns with the principle of least privilege by restricting outbound traffic specifically to the Azure Key Vault service, thereby minimizing broader internet access and reducing administrative complexity.
upvoted 2 times

  **Amir1909** 1 year, 1 month ago
B is correct
upvoted 1 times

  **tripleaholic** 1 year, 5 months ago
similar as question 32 on <https://www.examtopics.com/exams/microsoft/az-104/view/51/>
upvoted 1 times

  **Rams786** 1 year, 7 months ago
This question was on my exam on 22 Sep 2023. scored 900 i answered B
upvoted 5 times

  **rodrod** 6 months, 1 week ago
how does it help to know the correct answer? you didn't get the detail of each question right?
upvoted 1 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: B

To ensure that the virtual machines can access Vault1 while adhering to the principle of least privilege and minimizing administrative effort, you should use Azure's built-in service tags. These service tags represent a group of IP address prefixes from a given Azure service. When you want to allow communication between Azure services and resources, using service tags reduces the complexity of IP address management.

For your requirement, Azure provides a service tag specifically for Azure Key Vault: AzureKeyVault. By using this service tag, you ensure that your virtual machines can only access Azure Key Vault in the East US region and not other unrelated internet resources.

Therefore, the correct answer is:
B. a service tag.
upvoted 1 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: B

B most voted.
upvoted 1 times

  **Aquintero** 1 year, 9 months ago

Selected Answer: B

Una etiqueta de servicio representa un grupo de prefijos de direcciones IP de un servicio de Azure determinado. Microsoft administra los prefijos de direcciones que la etiqueta de servicio incluye y actualiza automáticamente dicha etiqueta a medida que las direcciones cambian, lo que minimiza la complejidad de las actualizaciones frecuentes en las reglas de seguridad de red.

Puede usar etiquetas de servicio para definir controles de acceso a la red en grupos de seguridad de red, Azure Firewall y rutas definidas por el usuario. Use etiquetas de servicio en lugar de direcciones IP específicas cuando cree reglas de seguridad y rutas.
upvoted 4 times


  **BJS_AzureExamTopics** 1 year, 9 months ago

Service tag is the least work. MSFT answers are ALWAYS the least administrative effort answers, and there will usually be only one choice that stands out.
upvoted 2 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: B

B - Service Tag is correct.
<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags>
"AzureKeyVault" tag can be used in outbound NSGs.
upvoted 3 times

  **zelck** 2 years, 3 months ago



Selected Answer: B

B is the answer.

A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

You can use service tags to achieve network isolation and protect your Azure resources from the general Internet while accessing Azure services that have public endpoints. Create inbound/outbound network security group rules to deny traffic to/from Internet and allow traffic to/from AzureCloud or other available service tags of specific Azure services.

upvoted 3 times

  **zelck** 2 years, 3 months ago

Selected Answer: B



B is the answer.

<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview>

A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.



You can use service tags to achieve network isolation and protect your Azure resources from the general Internet while accessing Azure services that have public endpoints. Create inbound/outbound network security group rules to deny traffic to/from Internet and allow traffic to/from AzureCloud or other available service tags of specific Azure services.

upvoted 2 times

  **zelck** 2 years, 3 months ago

You should configure a service tag as the destination of the outbound security rule for NSG1. This will allow the virtual machines to access Vault1 while still adhering to the principle of least privilege and minimizing administrative effort. A service tag represents a group of Azure resources that are identified by a common tag, in this case, the key vault. By configuring the outbound rule to allow traffic to the key vault service tag, you are ensuring that only traffic to the key vault is allowed, and not to any other internet destinations. This is more secure and efficient than specifying an IP address range or configuring an application security group.

upvoted 4 times

  **Muffay** 2 years, 4 months ago

B - Service Tag is correct.

<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags>

"AzureKeyVault" tag can be used in outbound NSGs.

upvoted 3 times

You have an Azure AD tenant named adatum.com that contains the groups shown in the following table.

Name	Member of
Group1	None
Group2	Group1
Group3	Group2

Adatum.com contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3
User4	None

You assign the Azure Active Directory Premium Plan 2 license to Group1 and User4.

Which users are assigned the Azure Active Directory Premium Plan 2 license?

- A. User4 only
- B. User1 and User4 only
- C. User1, User2, and User4 only
- D. User1, User2, User3, and User4

Correct Answer: B

Community vote distribution

B (92%)

4%

sandorh

Highly Voted

2 years, 4 months ago

Selected Answer: B

Nevermind, the answer is B
<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>
Under Limitations and known issues:
"Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied."
upvoted 101 times

suresh0512

2 years, 4 months ago

What about the user4, he is set to none and gets assigned whatever the new role is assigned?
upvoted 3 times

Hull

2 years, 3 months ago

"You assign the Azure Active Directory Premium Plan 2 license to Group1 and User4."

User 4 is assigned the license directly
upvoted 20 times

helixsam

Highly Voted

2 years, 3 months ago

Selected Answer: B

A. User4 only (INCORRECT = Also Group1 has directly assigned licenses)
B. User1 and User4 only (CORRECT = Both have directly assigned license)
C. User1, User2, and User4 only (INCORRECT = User2 is member of Group2 that is NESTED to Group1. NESTED Group are NOT Supported as per MS KB: Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.
REF: <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>)
D. User1, User2, User3, and User4 (INCORRECT= Same reason answer C)
upvoted 23 times

Dankho

7 months ago

The document does not state that you can't have licenses for nested groups; rather, it explains how licensing works and clarifies that licenses assigned to parent groups will apply to all users in nested groups.

upvoted 2 times

  **GohanF2** 2 years, 1 month ago

Thank you ! I didn't know about the nested groups licenses inheritance

upvoted 3 times

  **Mitko_V_Milkov** Most Recent 4 months ago

Selected Answer: D

If you do a bit of a research you will find out that the answer is actually D. Dankho is right but he is not explaining his logic or knowledge. Basically, inheritance do not work if you apply the license to "nested" group. This means that if you apply to Group 2, licenses will not be automatically inherited by Group 3. However, Group 1 is not "nested", which means that the licenses will propagate to all other groups, regardless if these are direct member of Group 1 or not.

upvoted 1 times

  **Mitko_V_Milkov** 3 months ago

Changed my mind to B. I thought my logic is correct, but I am not convinced now...

upvoted 2 times

  **Phat** 3 months, 3 weeks ago

"Group-based licensing currently does not support groups that contain other groups"

here: group1 is containing group2, group2 contains group3.



so, group2 & group 3 are nested groups.

so licensing not support for group1 (contain other group).

" If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied"

if apply for nested group2, license is effective for only users in group2, and not effective for group3.

upvoted 1 times

  **Sholasleek** 5 months, 2 weeks ago

Correct, group-based licensing in Microsoft 365 does not support nested groups. This means that if you assign licenses to a nested group (a group that contains other groups), only the users in the first-level group will receive the licenses.

upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: B

B is corerct

upvoted 1 times

  **testtaker09** 10 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 2 times

  **testtaker09** 10 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

Based on this setup:

User1 receives the license through their membership in Group1.

User4 receives the license directly assigned to them.

Therefore, the correct answer is:


B. User1 and User4 only are assigned the Azure Active Directory Premium Plan 2 license.

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

B is correct

upvoted 1 times

  **Ahkhan** 1 year, 5 months ago

I got this exact question on my exam today on 11/14/2023.

upvoted 2 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: B

This is correct

upvoted 1 times

  **AntaninaD** 1 year, 7 months ago



Got this question on 09/09/23

upvoted 2 times

  **CarlosMarin** 1 year, 8 months ago

This question was in my exam on 31/08/2023.

upvoted 3 times

  **ecliptor** 1 year, 9 months ago

Estava no exame 28/07/23

upvoted 2 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: B

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

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

upvoted 3 times

  **Dankho** 7 months ago

I'm not sure you guys are really reading the references mentioned.

While nested groups can inherit licenses from parent groups, you cannot assign licenses at the nested level (e.g., Group3) directly. They must be assigned at the highest level (e.g., Group1).

upvoted 1 times

  **Navigati0n** 1 year, 9 months ago

User1 and User4 only.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

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

upvoted 2 times

  **[Removed]** 1 year, 10 months ago

Selected Answer: D

Group2 member of Group1 -> If we assign Premium Plan2 -> Group2 too assigned same license -> User2

Group3 member of Group2 -> member of Group1 -> If we assign Premium Plan2 -> Group3 too assigned same license -> User3

upvoted 1 times

HOTSPOT -

You have an Azure AD tenant named contoso.com.

You have two external partner organizations named fabrikam.com and litwareinc.com. Fabrikam.com is configured as a connected organization.

You create an access package as shown in the Access package exhibit. (Click the Access package tab.)

New access package

* Basics

Resource roles

* Requests

Requestor information

* Lifecycle

Review + Create

Summary of access package configuration

Basics

Name

Description

Catalog name

package1

Guest users

General

Resource roles

Resource	Type	Sub Type	Role
Group1	Group and Team	Security Group	Member

Requests

Users who can request access

Require approval

Enabled

All configured connected organizations

No

Yes

Requestor information

Questions

Question	Answer format	Multiple choice optio...	Required
----------	---------------	--------------------------	----------

Attributes (Preview)

Attribute type	Attribute	Default display string	Answer format	Multi
----------------	-----------	------------------------	---------------	-------

Lifecycle

Access package assignments expire

Require access reviews

After 365 days

No

You configure the external user lifecycle settings as shown in the Lifecycle exhibit. (Click the Lifecycle tab.)

Manage the lifecycle of external users

Select what happens when an external user, who was added to your directory through an access package request, loses their last assignment to any access package.

Block external user from signing in to this directory Yes No

Remove external user Yes No

Number of days before removing external user from this directory

Delegate entitlement management

By default, only Global Administrators and User Administrators can create and manage catalogs, and can manage all catalogs. Users added to entitlement management as Catalog creators can also create catalogs and will become the owner of any catalogs they create.

Catalog creators ⓘ 0 selected
[Add catalog creators](#)

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Litwareinc.com users can be assigned to package1.	<input type="radio"/>	<input type="radio"/>
After 365 days, fabrikam.com users will be removed from Group1.	<input type="radio"/>	<input type="radio"/>
After 395 days, fabrikam.com users will be removed from the contoso.com tenant.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Litwareinc.com users can be assigned to package1.	<input type="radio"/>	<input checked="" type="radio"/>
After 365 days, fabrikam.com users will be removed from Group1.	<input checked="" type="radio"/>	<input type="radio"/>
After 395 days, fabrikam.com users will be removed from the contoso.com tenant.	<input checked="" type="radio"/>	<input type="radio"/>

- PlaceboC6** Highly Voted

2 years, 2 months ago

N - Because not Connected
Y - Because when it expires it is removed from the group. Proof to follow
Y - Because..math
<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources>
When a user's access package assignment expires, they are removed from the group or team, unless they currently have an assignment to another access package that includes that same group or team.
upvoted 152 times
- areait**

2 months, 1 week ago

Tested in the labs
N because not connected
N because they will be blocked only as it states in the "Manage lifecycle of external users"
Y The only one right bc it's 365 + 30 in order to remove users

if u have any doubt you can check this video : <https://www.youtube.com/watch?v=J136cq9r0u8> with the title "54. MS Azure Administrator Associate AZ 104 - Access Package, Guest Users, Entitlement Management"
upvoted 1 times
- a6bd45e**

9 months, 3 weeks ago

Regarding the first statement: The package is set so those from organization that is not connected cannot request to be added. Does it mean they cannot be assigned (by Owner for example)?
The package defines "cannot request access".
The statement says "can be assigned".

upvoted 3 times

  **NotKnownForMuch** 4 months, 2 weeks ago

First statement is Yes

In some cases, you might want to directly assign specific users to an access package so that users don't have to go through the process of requesting the access package. To directly assign users, the access package must have a policy that allows administrator direct assignments.

<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-assignments>

upvoted 1 times

  **3c5adce** 11 months, 3 weeks ago

Confirmed

upvoted 1 times

  **AK4U_111** 2 years, 2 months ago

After reading this article, i would say NYY is correct.

Thank you

upvoted 10 times

  **Ruby1133299** Highly Voted  2 years, 3 months ago

N not a connected organisation

N expired not remove

Y 365 + 30 = 395 removed

upvoted 104 times

  **RougePotatoe** 2 years, 3 months ago

Why don't people cite their sources. so we know for sure that expired isn't the same as removed.

upvoted 4 times

  **RougePotatoe** 2 years, 3 months ago

I mis-read the question. I still wish people would cite their sources though.

upvoted 6 times

  **Indy429** 1 year, 4 months ago

This is the right answer

If Q2 said "EXPIRE" it would be Yes, but it said "REMOVE" which will only happen 30 days after expiring

upvoted 1 times

  **Stunomatic** Most Recent  6 months, 2 weeks ago



after expiration of access package

After access package expiration (365 days): External users lose access to the resources in the package, and they are removed from any groups or roles tied to the package.

30 days later: The external users will be deleted from your Azure AD tenant (if they have no other access packages or assignments).

Y N N

upvoted 2 times

  **Stunomatic** 6 months, 2 weeks ago

sorry N Y Y

upvoted 2 times

  **behradcld** 8 months ago

I think the answer is correct:

Yes: Because users can be assigned but they can not request

No: Because expired not removed

Yes: correct after 395 will be removed

upvoted 3 times

  **[Removed]** 8 months ago

WRONG

No

No

Yes

upvoted 2 times

  **varinder82** 11 months, 3 weeks ago

Final Answer:

N not a connected organisation

N expired not remove

Y 365 + 30 = 395 removed

upvoted 5 times

  **3c5adce** 11 months, 4 weeks ago

ChatGPT4 says No no no

upvoted 1 times

🗨️ 👤 **2fd1029** 8 months, 1 week ago

We don't care what ChatGPT says. ChatGPT gets questions wrong all the time.
upvoted 8 times

🗨️ 👤 **SkyZeroZx** 1 year, 4 months ago

1.- N : Because not has a permissions
2.- N : Because is expired not delete
3.-Y : Because 365 + 30 to delete/remove is correct
The answer
https://www.youtube.com/watch?v=J136cq9r0u8&list=PLIKA5U_Yqgof3H0YWhzvarFixW9QLTr4S&index=53
upvoted 17 times

🗨️ 👤 **Jedi_sg2000** 10 months, 1 week ago

that make sense!
upvoted 1 times

🗨️ 👤 **hebb0777** 1 year, 5 months ago

N
N : "When a user's access package assignment expires, they're removed from the group or team, unless they currently have an assignment to another access package that includes that same group or team" .. <https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources>
Y - 365+30 = 395 deleted.
upvoted 3 times

🗨️ 👤 **katrvintraiz** 1 year, 5 months ago

The answer
https://www.youtube.com/watch?v=J136cq9r0u8&list=PLIKA5U_Yqgof3H0YWhzvarFixW9QLTr4S&index=53
upvoted 9 times

🗨️ 👤 **ziggy1117** 1 year, 6 months ago

N
N - When a user's access package assignment expires, they're removed from the group or team, unless they currently have an assignment to another access package that includes that same group or team.
<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-resources#add-a-group-or-team-resource-role>
Y
upvoted 1 times

🗨️ 👤 **ziggy1117** 1 year, 6 months ago

sorry should be N-Y-Y
upvoted 4 times

🗨️ 👤 **amsioso** 1 year, 6 months ago

N,N,Y
<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-external-users#manage-the-lifecycle-of-external-users>
upvoted 2 times

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

By default, when an external user no longer has any access package assignments, they're blocked from signing in to your directory. After 30 days, their guest user account is removed from your directory.
upvoted 1 times

🗨️ 👤 **Series_0011** 1 year, 6 months ago

N
Y - Group membership is only maintained after losing access to the access package if it was previously in the group before being assigned to the access package or if they are assigned to another access package that also includes that group or team. When access expires they are removed from the group or team.
Y



<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources>
upvoted 4 times

🗨️ 👤 **skeleto11** 1 year, 7 months ago

NO - Not connected
NO - It is not removed from the group
when their access package assignment is removed, they remain in the resource role. For example, if a user was a member of a group, and was assigned to an access package that included group membership for that group as a resource role, and then that user's access package assignment was removed, the user would retain their group membership.
<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources>
Y - 365+30 = 395 deleted.
upvoted 1 times

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

The answer for the second question should be YES - "When a user's access package assignment expires, they're removed from the group or team, unless they currently have an assignment to another access package that includes that same group or team." -> Source of the explanation is your link: <https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources>
upvoted 4 times

  **itismadu** 7 months, 3 weeks ago

From the link
"When a user's access package assignment expires, they're removed from the group or team, unless they currently have an assignment to another access package that includes that same group or team"
<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-resources>
sO IT SHOULD BE
n
y
y
upvoted 1 times

  **mandogrogus** 1 year, 7 months ago

NNY makes sense, but why is Y marked with red in 1 ?
upvoted 1 times

  **oopspruu** 1 year, 8 months ago

It is NYY.
N - Not a connected organization
Y - After 365 days, the access package expires. If you read the description of "Manage Lifecycle" carefully, the removal part needs the expiration to go on for at least 30 days. Which means:
Y - $365 + 30 = 395$ Days == Removal
upvoted 3 times

  **gachocop3** 1 year, 9 months ago

NNY
1- Not a connected organization
2. Expired no remove
3. $365 + 30 = 395 =$ removed
upvoted 7 times

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Assign User1 the Network Contributor role for VNet1.
- B. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- C. Assign User1 the Owner role for VNet1.
- D. Assign User1 the Network Contributor role for RG1.

Correct Answer: C

Community vote distribution

C (100%)

- myarali**

Highly Voted

2 years, 2 months ago

Selected Answer: C

There is only two choices for that puspouse;

 - Assign User1 the Owner role for VNet1.
 - Assign User1 the User Access Administrator role for VNet1.

upvoted 33 times
- Nick111111**

Highly Voted

1 year, 9 months ago

I did see this on the exam

upvoted 6 times
- Mark74**

Most Recent

5 months ago

Selected Answer: C

C seems correct for me

upvoted 1 times
- [Removed]**

8 months ago

Selected Answer: C

C is corerct

upvoted 2 times
- 3c5adce**

1 year ago

To ensure that User1 can assign the Reader role for VNet1 to other users, you should:

A. Assign User1 the Network Contributor role for VNet1.

The Network Contributor role grants permissions to manage network resources, including virtual networks (VNet1), but restricts access to only those resources.

By assigning User1 the Network Contributor role for VNet1, you provide them with the necessary permissions to manage role assignments specifically for VNet1, including assigning the Reader role to other users.

This approach adheres to the principle of least privilege by granting only the necessary permissions for managing network resources without providing broader access to other resources in the subscription or resource group.



Option C is incorrect because assigning the Owner role for VNet1 provides excessive permissions, allowing User1 to manage all aspects of the virtual network, which exceeds the requirement to assign the Reader role to other users.

upvoted 1 times
- OtunbaDan**



10 months, 1 week ago

Real life reason why you should not use AI generated answers as against researching real real. this answer is from either chatgpt or germini.

upvoted 4 times


  **tashakori** 1 year, 1 month ago

C is right
upvoted 2 times



  **Notteb** 2 years, 2 months ago

Selected Answer: C



C. seems correct
upvoted 2 times

  **Ni33** 2 years, 3 months ago

C is correct. It is the only role in the give options have capability to assign permissions.
upvoted 2 times

  **zellck** 2 years, 3 months ago

Same as Question 53.
<https://www.examttopics.com/discussions/microsoft/view/74021-exam-az-104-topic-2-question-53-discussion>
upvoted 4 times

  **zellck** 2 years, 3 months ago



Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>
upvoted 1 times

  **vali6969** 2 years, 3 months ago

C is correct only Owner can assign roles (even reader role).
upvoted 1 times

  **Mo22** 2 years, 3 months ago

Selected Answer: C

Correct
upvoted 1 times

  **Georgego** 2 years, 3 months ago

Selected Answer: C

Answer is correct.
upvoted 1 times

HOTSPOT


You have an Azure subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The groups are configured as shown in the following table.

Name	Type	Azure AD roles can be assigned to the group
Group1	Security	Yes
Group2	Security	Yes
Group3	Microsoft 365	Yes

You have a resource group named RG1 as shown in the following exhibit.


RG1 | Access control (IAM)
...

Resource group

<<
+ Add
↓ Download role assignments
≡ Edit columns
↻ Refresh
✕ Remove

📄 Overview
📅 Activity log
👤 Access control (IAM)
🏷️ Tags
🌐 Resource visualizer
⚡ Events

Settings
📦 Deployments
🛡️ Security
📄 Policies
📊 Properties
🔒 Locks

Check access
Role assignments
Roles
Deny assignments
Classic administrator



Number of role assignments for this subscription ⓘ

2

2000

Type : All
Role : All
Scope : All subscriptions

2 items (1 Users, 1 Groups)

<input type="checkbox"/>	Name	Type	Role	Scope	Condition
✓	Owner				
<input type="checkbox"/>	 GR Group1	Group	Owner ⓘ	This resource	None
<input type="checkbox"/>	 PR privi...	User	Owner ⓘ	Subscription (Inherited)	None

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
You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	<input type="radio"/>	<input type="radio"/>
You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	<input type="radio"/>	<input type="radio"/>
You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for	<input type="radio"/>	<input type="radio"/>

Answer Area		
	Statements	
Correct Answer:	You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	<div><div>Yes</div><div>No</div></div>
	You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	<div><div>Yes</div><div>No</div></div>
	You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for	<div><div>Yes</div><div>No</div></div>

- HenriksDisciple

Highly Voted

2 years, 3 months ago

Just tested in my Azure test environment.
Answer is:
1. No
2. No
3. Yes

Don't know where rpalanivel83 got his answers from
upvoted 119 times
- JimmyYop

2 years, 2 months ago

Nesting is currently not supported for groups that can be assigned to a role. and the screen grab shows that the groups are assigned a role as YES. Answers are correct
upvoted 15 times
- 3c5adce

11 months, 3 weeks ago

Confirmed by ChatGPT4
upvoted 1 times
- AndreaStack

2 years, 3 months ago

me too but... where you found yours instead?
upvoted 3 times
- o0o0

1 year, 8 months ago

Just test and did not have your results.
1- Yes
2- No
3- No
upvoted 13 times
- tableton

1 year, 1 month ago

My test had this results too
upvoted 1 times
- hebbo777

1 year, 5 months ago

agree, i tested first point is yes, 2&3 Office 365 not supporting membership
upvoted 2 times
- LauLauLauw

Highly Voted

2 years, 3 months ago

All 3 statements tested:
Yes
It is possible to add Group2 to Group1, after checking the effective access the user in Group2 is owner.
No
M365 groups cant be added to membership of another group
Yes
the statement is not complete but if it states to assign the role to Group3 directly it is possible
upvoted 62 times
- SanSoni

11 months, 3 weeks ago

I tested and confirm it
upvoted 1 times
- eduardokm

2 years ago

The first is NO.
Role assignment property that can only be used with Plan 1 and Plan 2, it was just created to not allow erroneous nesting of permission roles. Without it you can use any group to assigned role and nesting, but taking the risk.
upvoted 3 times
- Notteb

2 years, 3 months ago

i'm going with Y,N,Y also
Group nesting of Sec groups is possible.
Nesting of a M365 group to a Sec group is however not possible.
upvoted 10 times
- bennyreis

2 year, 1 month ago

they are azure ad role enabled. nesting is not supported

upvoted 3 times

  **daws08322** 2 years, 2 months ago

There is a difference with adding a group and assigning a role by adding a group.

upvoted 3 times


  **70ec7c1** Most Recent 1 month, 2 weeks ago

1. Yes. It now (March 19, 2025) appears that you can inherit RBAC roles through nested group membership. Tested on Azure Portal.

2. No. As others have indicated, Azure Portal does not allow adding a MS 365 Group to a Security group. Did not try CLI.

3. User3 is a member user (assumed). The fact that he belongs to a MS 365 group does not change this status. As a member user, we can assign RBAC (including privileged) roles to User 3. Tested on Azure Portal.

upvoted 2 times

  **ahhatem** 2 months, 1 week ago

The answer is actually correct:

1- Children groups will inherit the permissions of the parent. But the question mentions that the group is set to "azure ad roles can be assigned to this group". This option prevents nesting. So the parent can't actually have any sub-groups.

2- Microsoft 365 groups can't be added a child to a security group

3- You actually can assign a Microsoft 365 group a role on an azure resource

upvoted 1 times

  **Bhuru** 2 months, 3 weeks ago

The answer is:

No - nesting does not work

No - you cannot mix m365 groups with security groups

No - M365 groups do not work in azure RBAC environment

Learn or Perish

upvoted 3 times

  **czegi90** 3 months ago

1. Yes

2. No

3. Yes

"Nesting is currently not supported for groups " <-- I guess it was true in the past, but not anymore.

You can add Group2 as a member of Group1 and members of Group2 inherit the RBAC roles assigned to Group1. (I tested this today)

upvoted 1 times

  **cris_exam** 3 months ago

What are you talking about? If the "Microsoft Entra roles can be assigned to the group" is set to YES, then nesting is not possible.

As the question states, that feature is enabled for all groups, hence nesting for Security Groups that have Entra ID roles assignment enabled, is not possible.

Correct answer is

N - Nesting not possible

N - M365 groups cannot be nested in Sec Groups

Y - Just as Group is configured as owner to RG, you can do the same to Group 3



Also, just tested in a lab and confirm.

upvoted 1 times

  **cris_exam** 3 months ago

Y - Just as Group1 is configured as owner to RG1, you can do the same to Group 3*

upvoted 1 times

  **Odc4dd8** 3 months, 2 weeks ago

no

no



Yes

upvoted 1 times

  **b411470** 5 months, 1 week ago

all the questions ask 'You can assign...' but it doesn't tell me what permissions I have. Not enough info in this question. I hate these types of questions. I am supposed to assume I can assign I guess?

upvoted 2 times

  **WALL47** 4 months ago

You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.

True:

Group2 is a security group, and it can be added as a member of Group1, which already has the Owner role for RG1. This will allow User2, who is a member of Group2, to inherit the Owner role.

"You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1."

False:



Since Group3 is a Microsoft 365 group, it cannot be nested within Group1, which is a security group. Therefore, User3 cannot inherit the Owner role through this method.

"You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for RG1."

True:

Directly assigning the Owner role to Group3 for RG1 will grant User3, who is a member of Group3, the Owner role for RG1.

upvoted 2 times



  **Chuong0810** 6 months ago

You can use nested security groups to assign RBAC roles in Azure (not Microsoft 365 group). Nested groups are not currently supported for all Azure services and features.

Directly assigning an Azure RBAC role to a Microsoft 365 group is not possible. This is because Microsoft 365 groups are primarily designed for collaboration within Microsoft 365 services and do not have the necessary security attributes to be directly assigned Azure RBAC roles.

So the answers are: 1. Yes, 2. No, 3. No

upvoted 1 times

  **rodrod** 6 months, 1 week ago

so many confusion.

Many people saying "Nesting is supported in Azure subscription roles. The question clearly shows that it is referencing an Azure subscription role. The link you have supplied is about unsupported nested groups in Azure Active Directory."

Forget about roles, or RBAC or whatever :-) Nested Group Support in RBAC is irrelevant.


think about nested groups. the point is , you can't create a nested group anyways.

you will NOT be able to include any group to a role-assignable group, they are all assignable groups so those groups can't have child...

So there is no point about whether nested group is supported by X or Y, because... there is NO nested group!

so it's N-N for the 2 first questions



upvoted 1 times

  **feralberti** 6 months, 2 weeks ago

i think this one explicitly addresses questions 1 <https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#groups>

So the answers are Y for the nested group RBAC role inheritance

upvoted 2 times

  **jamesf** 6 months, 2 weeks ago

1. NO

2. NO

3. YES

Group nesting isn't supported. A group can't be added as a member of a role-assignable group.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept#restrictions-for-role-assignable-groups>

upvoted 5 times

  **[Removed]** 8 months ago

CORRECT

upvoted 2 times

  **a_786_b** 8 months, 3 weeks ago

1.

No, role assignments do not automatically propagate to nested groups in Azure. Azure Role-Based Access Control (RBAC) does not support the automatic inheritance of role assignments for nested groups.

2. No, a Microsoft 365 group cannot be a member of a security group in Azure AD. Microsoft 365 groups (formerly known as Office 365 groups) are designed primarily for collaboration purposes and integrate with tools like Outlook, Teams, SharePoint, and others. They are different from security groups, which are used for managing permissions to resources within Azure and other Microsoft services.

3. Yes, a Microsoft 365 group can be assigned as the owner of a resource group in Azure. In Azure Role-Based Access Control (RBAC), you can assign roles, including the "Owner" role, to users, security groups, or Microsoft 365 groups.

upvoted 6 times

  **CheMetto** 9 months, 3 weeks ago

Who knows if they truly test it?

We don't need to trust anyone, only documentation is truly trustable.

The answer is No No Yes for this simple reason:

Adding groups as members of a role-assignable group is not supported. So we don't need to understand nested group assignment or everything else. Those group has role-assignable set to true, so this group can't have other groups inside of it. So the first 2 are false because you can't.

<https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups#add-or-remove-a-group-from-another-group>

upvoted 2 times

  **hakeem89** 11 months ago

1. Yes: you can use nested security group to assign RBAC roles in Azure (don't confuse this with Entra) - tested and verified in the lab

2. No: you can not nest Microsoft 365 group in a security group (it will be grayed out)

3. Yes: you can assign an owner role directly to a Microsoft 365 group in Azure

upvoted 9 times

  **Amir1909** 1 year, 1 month ago

Given answer is right

upvoted 1 times

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader role for Subscript on 1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the Owner role for VNet1.
- C. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription 1.
- D. Assign User1 the Contributor role for VNet1.

Correct Answer: B

Community vote distribution

B (100%)

- phantom31**

Highly Voted

7 months, 3 weeks ago

Why filling up with repetitions just to increase question number?

upvoted 7 times
- Mark74**

Most Recent

5 months ago

Selected Answer: B

B is correct

upvoted 1 times
- [Removed]**

8 months ago

Selected Answer: B

B is corerct

upvoted 1 times
- 3c5adce**

1 year ago

To ensure that User1 can assign the Reader role for VNet1 to other users, you should:

D. Assign User1 the Contributor role for VNet1.

Explanation:

The Contributor role grants permissions to manage resources within a specific scope, such as a virtual network (VNet1) in this case. By assigning User1 the Contributor role for VNet1, you provide them with the necessary permissions to manage role assignments specifically for VNet1, including assigning the Reader role to other users. This approach adheres to the principle of least privilege by granting only the necessary permissions for managing resources (in this case, VNet1) without providing broader access to other resources in the subscription or resource group.

Option B is incorrect because assigning the Owner role for VNet1 provides excessive permissions, allowing User1 to manage all aspects of the virtual network, which exceeds the requirement to assign the Reader role to other users.

upvoted 1 times
- JackGelder**

11 months, 3 weeks ago

Contributor role does not allow you to assign roles

upvoted 7 times
- GoldenDisciple2**

1 year, 8 months ago

Selected Answer: B

If you got Q71 Topic 2 wrong, then you shouldn't get this one wrong. If you do, go back to Q71 then come back to this one...

upvoted 1 times
- BJS_AzureExamTopics**

1 year, 9 months ago

AK4U - stop! LOL

upvoted 1 times

🗨️ 👤 **ASKBO** 1 year, 10 months ago

Same with topic 2 question 53
upvoted 2 times

🗨️ 👤 **myarali** 2 years, 1 month ago

Selected Answer: B

B is the answer.
upvoted 2 times

🗨️ 👤 **AK4U_111** 2 years, 2 months ago

if they were all that easy, everyone would be certified :-)
upvoted 4 times

🗨️ 👤 **zellck** 2 years, 2 months ago

Same as question 71.
<https://www.examttopics.com/discussions/microsoft/view/95675-exam-az-104-topic-2-question-71-discussion>
upvoted 3 times

🗨️ 👤 **zellck** 2 years, 2 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner>
Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
upvoted 2 times

🗨️ 👤 **Nzudin** 2 years, 2 months ago

YES THE ANSWER IS B
upvoted 1 times

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

Selected Answer: B

B seems fine
upvoted 4 times

Your on-premises network contains a VPN gateway.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A. Azure Application Gateway
- B. private endpoints
- C. a network security group (NSG)
- D. Azure Virtual WAN

Correct Answer: B

Community vote distribution

B (99%)

hevfe01

Highly Voted

2 years, 2 months ago

Selected Answer: B

Per the MS documentation, private endpoint seems to be the proper choice: "You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet."
Link: <https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>
upvoted 41 times

shadad

Highly Voted

2 years, 2 months ago

Selected Answer: B

I took Exam of Azure- 104 at 27/2/2023
I score 920 points out of 1000 points. This was on it and my answer was: B
upvoted 29 times

Joyariffic

10 months, 4 weeks ago

so if you already passed, why are you on here studying the practice questions?
upvoted 7 times

nailedIT

9 months ago

Bots everywhere :D
Always the same sentence structure
upvoted 6 times

MackD

Most Recent

4 months, 3 weeks ago

Selected Answer: B

Exam december 2024, private endpoints.
upvoted 5 times

Jaiiee

4 months, 3 weeks ago

Selected Answer: B

Requirement:
Ensure all traffic between VM1 (connected to VNet1) and storage1 (a storage account) travels across the Microsoft backbone network.

Key Details:

VNet1: Enabled forced tunneling.
VM1: Connected to VNet1.

Storage1: Storage account.
Solution Approach:

To route traffic between a virtual machine and a storage account over the Microsoft backbone network, you must use Private Endpoints. Private Endpoints provide private connectivity to Azure services such as storage accounts by mapping the service to a private IP address within the virtual network. This ensures traffic does not traverse the public internet.

upvoted 1 times

  **Mark74** 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

B is corerct

upvoted 1 times

  **Amir1909** 1 year, 1 month ago

B is correct

upvoted 2 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: B

To ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network without going out to the public internet, you should use a private endpoint.

A private endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet. Any traffic between your virtual machine and the storage account will traverse over the VNet and stay on the Microsoft backbone network, without ever leaving it.

Thus, the correct answer is:

B. private endpoints.

upvoted 4 times

  **CarlosMarin** 1 year, 8 months ago

This question was in my exam on 31/08/2023.

upvoted 2 times

  **kioks23** 1 year, 7 months ago

I don't believe you. You are spamming every question with this reply

upvoted 14 times

  **behradcld** 8 months ago

maybe he didnt pass the exam and he's here for practice again, come on don't judge people

upvoted 1 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: B

"Azure Private Link enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.

Traffic between your virtual network and the service travels the Microsoft backbone network. Exposing your service to the public internet is no longer necessary. "

<https://learn.microsoft.com/en-us/azure/private-link/private-link-overview?toc=%2Fazure%2Fvirtual-network%2Ftoc.json>

upvoted 1 times

  **ecliptor** 1 year, 9 months ago



Estava no exame hoje

upvoted 2 times

  **allyQ** 2 years, 2 months ago


B: Take the VPN / VPN Gateway resources out of the question and the answer would be the same.

upvoted 1 times

  **Takate** 2 years, 2 months ago

VPN is not part of Az-104 exam right ?

upvoted 1 times

  **allyQ** 2 years, 2 months ago

It is, but I dont think its a VPN question.

upvoted 2 times

  **insanewriters** 2 years, 2 months ago

It is.

upvoted 2 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: B

A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network.

The service could be an Azure service such as:

Azure Storage
Azure Cosmos DB
Azure SQL Database
Your own service, using Private Link service.

<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview>

upvoted 5 times

  **elior19940** 2 years, 2 months ago

answer is B:



Private endpoints are used to provide secure and private connectivity from a virtual network to Azure storage. When you configure a private endpoint, a private IP address is assigned to the storage account within the virtual network. All traffic to the storage account goes over the Microsoft backbone network, rather than over the public internet, providing increased security and reliability. By configuring a private endpoint for the storage account in this scenario, you can ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

upvoted 4 times

  **elior19940** 2 years, 2 months ago

is it new question?

upvoted 3 times

  **shadad** 2 years, 2 months ago

Yes it is and the answer is B Private endpoints

upvoted 1 times

  **examkiddos** 2 years, 2 months ago

Selected Answer: D

Optimized routing using the Microsoft global network
<https://azure.microsoft.com/en-us/products/virtual-wan>

upvoted 1 times

  **lockmas101** 3 months, 2 weeks ago

it cant be D. This is more of LAN connection, rather than WAN

upvoted 1 times

HOTSPOT

-

You have an Azure subscription that contains a user named User1 and the resources shown in the following table.

Name	Type
RG1	Resource group
networkinterface1	Virtual network interface
NSG1	Network security group (NSG)

NSG1 is associated to networkinterface1.

User1 has role assignments for NSG1 as shown in the following table.

Role	Scope
Contributor	This resource
Reader	Subscription (Inherited)
Storage Account Contributor	Resource group (Inherited)

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 create a storage account in RG1.	<input type="radio"/>	<input type="radio"/>
User1 can modify the DNS settings of networkinterface1.	<input type="radio"/>	<input type="radio"/>
User1 can create an inbound security rule to filter inbound traffic to networkinterface1.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements

Yes

No

Correct Answer:

User1 can create a storage account in RG1.

User1 can modify the DNS settings of networkinterface1.

User1 can create an inbound security rule to filter inbound traffic to networkinterface1.

☒

☐

☒

- skydivex

Highly Voted

2 years, 2 months ago

Correct Answers. YES, No, Yes
(YES)User1 can create a storage account in RG1, since User1 has Storage Account Contribute Role inherited from Resource Group.
(NO) User1 can modify the DNS settings of networkinterface1, since it requires Network Contribute role referring to the following link.
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface?tabs=network-interface-portal#permissions>
(YES) User1 can create an inbound security rule to filter inbound traffic to networkinterface1, since User1 has Contributor role for NSG1
upvoted 105 times
- 3c5adce

11 months, 3 weeks ago



Confirmed by ChatGPT4
upvoted 3 times
- Chris76

2 years ago

Wrong. Answer is N-N-Y. You cannot create new storage accounts with a "Storage Account Contributor" role, only manage existing. Don't confuse people.
upvoted 30 times
- vrn1358

3 months ago

please not that NSG has "Storage Account Contributor" role not RG1. So you can not create Storage account in RG1
upvoted 1 times

  **deroid** 1 year, 7 months ago

No, You can create Storage Accounts from Storage Account Contributor Role
/*

Microsoft.Storage/storageAccounts/* Create and manage storage accounts

*/

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-account-contributor>

upvoted 12 times

  **sardonique** 1 year, 7 months ago

Storage Account Contributor:

Actions Description

Microsoft.Authorization/*/read Read roles and role assignments

Microsoft.Insights/alertRules/* Create and manage a classic metric alert

Microsoft.Insights/diagnosticSettings/* Creates, updates, or reads the diagnostic setting for Analysis Server

Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action Joins resource such as storage account or SQL database to a subnet. Not alertable.

Microsoft.ResourceHealth/availabilityStatuses/read Gets the availability statuses for all resources in the specified scope

Microsoft.Resources/deployments/* Create and manage a deployment

Microsoft.Resources/subscriptions/resourceGroups/read Gets or lists resource groups.

Microsoft.Storage/storageAccounts/* Create and manage storage accounts

Microsoft.Support/* Create and update a support ticket

upvoted 4 times

  **umavaja** 1 year, 2 months ago

Storage Account Contributor

Permits management of storage accounts. Provides access to the account key, which can be used to access data via Shared Key authorization.

Learn more

Actions Description

Microsoft.Authorization/*/read Read roles and role assignments

Microsoft.Insights/alertRules/* Create and manage a classic metric alert

Microsoft.Insights/diagnosticSettings/* Creates, updates, or reads the diagnostic setting for Analysis Server

Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action Joins resource such as storage account or SQL database to a subnet. Not alertable.

Microsoft.ResourceHealth/availabilityStatuses/read Gets the availability statuses for all resources in the specified scope


Microsoft.Resources/deployments/* Create and manage a deployment

Microsoft.Resources/subscriptions/resourceGroups/read Gets or lists resource groups.

Microsoft.Storage/storageAccounts/* Create and manage storage accounts

Microsoft.Support/* Create and update a support ticket

upvoted 3 times

  **umavaja** 1 year, 2 months ago

Yes with Role Storage Account Contributor with following action, it can create and manage storage account

Microsoft.Storage/storageAccounts/* Create and manage storage accounts

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-account-contributor>

upvoted 1 times

  **zelck** Highly Voted 2 years, 2 months ago

YNY is the answer.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-account-contributor>
- Microsoft.Storage/storageAccounts/* Create and manage storage accounts

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader>

View all resources, but does not allow you to make any changes.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#contributor>

Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

upvoted 23 times

  **Ponpon3185** Most Recent 1 month, 3 weeks ago

I think NNY...but it seems that Storage Account Contributor is able to create Storage Account: <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#storage-account-contributor>

"Microsoft.Storage/storageAccounts/* Create and manage storage accounts"

So Y/N/Y

upvoted 1 times

  **Abhisk127** 3 months, 2 weeks ago

No, a user with the Storage Account Contributor role in Azure cannot create new storage accounts. However, they can manage classic storage accounts.

Explanation



The Avere Contributor role in Azure allows users to create and manage storage accounts.

The Storage Account Contributor role in Azure only allows users to manage classic storage accounts.

The Contributor role in Azure allows users to create and manage resources, but not set access controls or manage billing.



Users can assign Azure roles at the level of the subscription, resource group, storage account, or container.

upvoted 1 times

  **Riz504** 4 months, 2 weeks ago

Correct Answers. YES, No, Yes
(YES) User1 can create a storage account in RG1, since User1 has Storage Account Contributor Role inherited from Resource Group.
(NO) User1 can NOT modify the DNS settings of networkinterface1, since it requires Network Contributor role referring to the following link.
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface?tabs=network-interface-portal#permissions>
(YES) User1 can create an inbound security rule to filter inbound traffic to networkinterface1, since User1 has Contributor role for NSG1

upvoted 1 times

  **Stunomatic** 6 months, 2 weeks ago

Even if NSG1 is associated with networkInterface1, the user will not be able to modify networkInterface1's DNS settings unless they have the appropriate role assigned directly on the network interface or a higher scope like the resource group (RG1) or subscription.

Even though NSG1 is associated with networkInterface1, the Network Contributor role on NSG1 does not give the user permission to manage or modify networkInterface1.

upvoted 2 times

  **[Removed]** 7 months, 1 week ago

CORRECT

upvoted 2 times

  **[Removed]** 8 months ago

CORRECT

upvoted 2 times

  **tcoelho28** 8 months, 4 weeks ago

Correct Answers. No, No, Yes
NO - Storage Account Contributor Role only permits management of storage accounts. Provides access to the account key, which can be used to access data via Shared Key authorization.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 1 times

  **SrWalk49** 9 months ago

Role can create. Asked ChatGPT why is this an exception to the traditional setup:

The "Storage Account Contributor" role in Azure is designed to provide extensive management capabilities specific to storage accounts, including creating and deleting storage accounts. This differs from more general "Contributor" roles, which typically do not allow resource creation or deletion at the subscription level to prevent significant changes that could impact overall resource management.



upvoted 1 times

  **MSExpertGER** 10 months, 3 weeks ago

The Storage Account Contributor Role does not allow to create Storage Accounts. You may set certain things on the SAC, but not create them within the given scope. <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#storage-account-contributor>

- 1) NO - because Storage Account Contributor as of 2024 doesn't allow Creation of Storage Accounts.
- 2) YES - Owner of the NIC
- 3) NO - there is no information given about any other rights to any other scope related to the NSG. So the user has only Reader rights on the NIC, inherited from Subscription.

upvoted 4 times

  **asaulu** 11 months, 3 weeks ago

2. Yes. The "Contributor" role at the resource group level inherited by the network security group (NSG1) associated with networkinterface1 would generally allow a user to modify the resources within that group. Since DNS settings are a part of network interface configuration, and the network interface is associated with NSG1, User1 should be able to modify these settings.

upvoted 2 times

  **Wassel_Laouini** 12 months ago

I think it's Yes, No, No: because you need Network contributor to be able to make changes to the NSG and NIC

upvoted 3 times

  **Pt4r** 1 year ago



- User1 can create a storage account in RG1.
1. Yes. User1 has the "Contributor" role on the subscription level inherited by the resource group RG1. This role allows creating new resources within the subscription and thus within any resource group in the subscription, including RG1.
 - User1 can modify the DNS settings of networkinterface1.
 2. Yes. The "Contributor" role at the resource group level inherited by the network security group (NSG1) associated with networkinterface1 would generally allow a user to modify the resources within that group. Since DNS settings are a part of network interface configuration, and the network interface is associated with NSG1, User1 should be able to modify these settings.
 3. User1 can create an inbound security rule to filter inbound traffic to networkinterface1.
- Yes. User1 has the "Contributor" role on NSG1 which gives them the ability to manage network security rules, including creating new inbound security rules.

upvoted 3 times

  **Amir1909** 1 year, 1 month ago

Given answer is right

upvoted 1 times

  **bacana** 1 year, 2 months ago

User1 has role assignments for NSG1 not for RG. He can't create storage account.
upvoted 1 times

  **18c2076** 1 year, 1 month ago

His Storage Account Contributor role is inherited down from the RG. Read again. Try again. You failed.
upvoted 2 times

  **BluAlien** 1 year ago

.. and where is specified that NSG1 is in RG1 ? Nowhere, noway NNY
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

Yes
No
Yes
upvoted 1 times

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the Access Administrator role for VNet1.
- C. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- D. Assign User1 the Network Contributor role for RG1.

Correct Answer: B

Community vote distribution

B (100%)

- yettie79**

Highly Voted

2 years, 1 month ago

B is correct, You need to have the Owner Role or Access Administrator role to assign roles but Access Administrator role is preferred as it is least privilege.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>
upvoted 16 times
- ggogel**

Highly Voted

1 year, 5 months ago

Shouldn't this be "User" Access Administrator?
upvoted 14 times
- Mark74**

Most Recent

5 months ago

Selected Answer: B

B is correct
upvoted 1 times
- [Removed]**

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times
- tfdestroy**

1 year, 4 months ago

Selected Answer: B

A: Removing Security Reader won't grant additional permissions for assigning roles. Contributor for RG1 only manages resources within the group, not role assignment.
C: Removing Reader and Security Reader is unnecessary and removes existing access. Additionally, Contributor for Subscription1 is too broad and grants too many privileges.
D: Network Contributor only manages network resources like subnets and load balancers, not role assignment for VNet1.
The Access Administrator role specifically grants the "Microsoft.Authorization/roleAssignments/write" permission, which allows adding and removing role assignments, including assigning the Reader role for VNet1 to other users. This role provides the exact capability required without granting excessive permissions.

Therefore, B. Assign User1 the Access Administrator role for VNet1 is the correct solution to enable User1 to assign the Reader role for VNet1 to other users.
upvoted 2 times

LemonVine

1 year, 8 months ago

Selected Answer: B

I would go for the B
upvoted 1 times

Athul07

1 year, 11 months ago

To ensure that User1 can assign the Reader role for VNet1 to other users, you should assign User1 the Network Contributor role for RG1.

The Network Contributor role allows users to manage network resources, including virtual networks and their associated resources. By assigning User1 the Network Contributor role for RG1, they will have the necessary permissions to assign the Reader role for VNet1 to other users within the same resource group.

Therefore, the correct option is:



D. Assign User1 the Network Contributor role for RG1.

upvoted 1 times

  **GoldBear** 1 year, 4 months ago

Sorry, this is wrong. The correct answer is B - Access Administrator role.

upvoted 1 times

  **al_john** 1 year, 3 months ago

The "Contributor" not permit access permission !

upvoted 1 times

  **xRiot007** 1 year, 11 months ago

For a user to assign roles he needs to have the Owner role or Access Administrator role.
In this case, B is the only viable answer.

upvoted 1 times

  **obaali1990** 2 years, 1 month ago

Selected Answer: B

Selected Answer: B

upvoted 2 times

  **myarali** 2 years, 1 month ago

Selected Answer: B

You need User Administrator Role for assigning the Reader role to User1 for VNet1

upvoted 2 times

  **WreckIT** 2 years, 1 month ago

Selected Answer: B

B. Assign User1 the Access Administrator role for VNet1.

upvoted 4 times

HOTSPOT

-

You have three Azure subscriptions named Sub1, Sub2, and Sub3 that are linked to an Azure AD tenant.

The tenant contains a user named User1, a security group named Group1, and a management group named MG1. User is a member of Group1.

Sub1 and Sub2 are members of MG1. Sub1 contains a resource group named RG1. RG1 contains five Azure functions.

You create the following role assignments for MG1:

- Group1: Reader
- User1: User Access Administrator

You assign User the Virtual Machine Contributor role for Sub1 and Sub2.

Answer Area

Statements	Yes	No
The Group1 members can view the configurations of the Azure functions.	<input type="radio"/>	<input type="radio"/>
User1 can assign the Owner role for RG1.	<input type="radio"/>	<input type="radio"/>
User1 can create a new resource group and deploy a virtual machine to the new group.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
The Group1 members can view the configurations of the Azure functions.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can assign the Owner role for RG1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can create a new resource group and deploy a virtual machine to the new group.	<input type="radio"/>	<input checked="" type="radio"/>

Shadowner Highly Voted 2 years, 1 month ago
Personally I think its YYN.

- 1) GROUP1 Reader access, provides access to view all items, except secrets
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader>
 - 2) To Assign OWNER role, you need to either Owner role or User Administrator Access Role
<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal-subscription-admin#prerequisites>
 - 3) Neither User Access Admin Role nor the Reader Role allows to create new resources.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>
- upvoted 78 times

Slimus 1 year, 11 months ago
3rd - Yes. it's says "You assign User the Virtual Machine Contributor role for Sub1 and Sub2."
upvoted 5 times



kam1122 6 months ago
No, user cannot create RG
upvoted 3 times

090200f 11 months ago



neither and nor.. so not able to create new resources
upvoted 1 times

  **Simplon** 1 year, 1 month ago


No, User has only the Virtual Machine Contributor role for Sub1 and Sub2 but not to create a new RG before.
upvoted 6 times

  **Chris76** 2 years ago

Group1 is not said to be under MG1. And not associated with any subscriptions. So why you think first answer is Y ?
upvoted 6 times

  **AN79** 1 year, 12 months ago



It clearly states Group1 is assigned Reader role at the MG1 Scope
upvoted 14 times

  **Indy429** 1 year, 4 months ago



I agree
upvoted 2 times

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

So a User Access Administrator can't create new resource groups but they can assign a user with the Owner role, and the user with the Owner role *can* create new resource groups?
I feel like Im missing something.
upvoted 17 times

  **josola** 1 year, 6 months ago

That's why there are data breaches. A user doesn't have direct to create resources, but that account to give access to another account to create a resource (give owner role). It happens all the time.
upvoted 2 times

  **ajdann** 1 year, 8 months ago

That is exactly the point of User Access Administrator
upvoted 2 times

  **skeleto11** 1 year, 10 months ago


The owner role can create resource groups, but in this case he owns only one Resource Group called RG1, so he cannot create new groups.
upvoted 1 times

  **sardonique** 1 year, 7 months ago

it is not odd, access is always logged, so if the user access administrator were to perform shady stuff, his activity would be traceable
upvoted 1 times

  **Abhisk127** Most Recent  3 months, 2 weeks ago

Who are these people, who says it was appeared in exam on the particular date but never mentioned what answers they selected/ticked on it.
upvoted 2 times

  **Riz504** 4 months, 2 weeks ago

Added one "NOT" in answer 2 what you have missed.
upvoted 1 times

  **Chuong0810** 6 months ago

All are YES
A - The Group1 have Reader role on MG1
B - User1 has User Access Administrator role on MG1.
C - As User1 has User Access Administrator role, User1 can assign any roles necessarily itself to create a new resource group and deploy a virtual machine to the new group.
upvoted 1 times

  **[Removed]** 8 months ago

CORRECT
upvoted 2 times

  **etrop** 9 months ago

I'm going to say NYN here.
No because even though the user has reader if you try to go and actually view the configuraiton of the function in the portal with this you don't see much. In fact what you do see is mostly an error or some fields that have names, but not any of their values and even the fields are wrong in most cases so N, the user needs a data level access perm to see the configuration itself. It can see the function for sure, it can see all of its data plane settings yes, but not its configuration.

2.) Y Because the user has User Access Administrator so can see it.
3.) N Because the user can't create a new resource group with those perms.
upvoted 2 times

  **3c5adce** 11 months, 3 weeks ago

ChatGPT4 says all yes
upvoted 1 times

🗨️ 👤 **Mentalfloss** 9 months, 2 weeks ago

ChatGPT appears to be wrong quite often.
upvoted 5 times

🗨️ 👤 **3c5adce** 11 months, 4 weeks ago

All are YES / TRUE - vetted out by ChatGPT4 on 05/10/24
A - The Group1 members can view the configurations of the Azure functions.
B - User1 can assign the Owner role for RG1.
C - User1 can create a new resource group and deploy a virtual machine to the new group.
upvoted 1 times

🗨️ 👤 **GlixRox** 10 months, 2 weeks ago

User1 doesn't have contributor or owner roles for any level. VM contributor is specifically just for VM deployment, so while they can deploy a new VM, it can NOT deploy a *new* resource group, only a VM to the already existing RG1, since it is a contributor at the sub1 level which is 1 level above RG1, giving it inherited role permissions.
upvoted 3 times

🗨️ 👤 **Wassel_Laouini** 12 months ago

is just me or the information given about User didn't serve any purpose? the questions are only about User1
upvoted 1 times

🗨️ 👤 **Amir1909** 1 year, 1 month ago

Given answer is right
upvoted 1 times

🗨️ 👤 **18c2076** 1 year, 1 month ago

Azure provides the following Azure built-in roles for authorizing access to App Configuration data using Microsoft Entra ID:
Reader: Use this role to give read access to the App Configuration resource. This does not grant access to the resource's access keys, nor to the data stored in App Configuration.

In short: Reader role is sufficient to view the configurations - just not the data that lives inside them.
upvoted 1 times

🗨️ 👤 **etrop** 9 months ago

Try it. once I created a function I was not able to view the configuration with that user. It showed some fields, but not their values and even the fields it got all wrong. This is because reader is not good enough to see configuration which is a data level thing.
upvoted 1 times

🗨️ 👤 **1828b9d** 1 year, 2 months ago

This question was in exam 01/03/2024
upvoted 3 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago

Correct
Yes
Yes
No
upvoted 1 times

🗨️ 👤 **User65567473** 1 year, 2 months ago

Was on exam 11/2 /2024
upvoted 5 times

🗨️ 👤 **MGJG** 1 year, 8 months ago

YYN
3.- Microsoft.Resources/subscriptions/resourceGroups/read Gets or lists resource groups.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>
upvoted 1 times

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

People here are not paying attention to a clever wording of the question. "User1" and "User" are 2 different users. Read the question again. User1 is independent and User is a part of Group1.
So YYN is true.
upvoted 2 times

🗨️ 👤 **jackill** 1 year, 8 months ago

Regarding the sentences "User is a member of Group1." and "You assign User the Virtual Machine Contributor role for Sub1 and Sub2.". It is very strange the presence of "User" user... usually all the questions have a number in the users names (User1, User2, ...). It could be a typo... but also in this case (User -> User1) the correct response will be YYN, because User1 is always User Access Administrator at MG1 level that contains Sub1 and RG1. And also having User1 the Virtual Machine Contributor role, does not give him permission to create a resource group as requested by the third statement (it requires the Microsoft.Resources/subscriptions/resourceGroups/write permission).
upvoted 4 times

You have an Azure subscription that contains the resources shown in the following table.

Name	Description
share1	File share in storage1
storage1	Storage account
User1	Azure AD user

You need to assign User1 the Storage File Data SMB Share Contributor role for share1.

What should you do first?



- A. Enable identity-based data access for the file shares in storage1.
- B. Modify the security profile for the file shares in storage1.
- C. Select Default to Azure Active Directory authorization in the Azure portal for storage1.
- D. Configure Access control (IAM) for share1.

Correct Answer: D

Community vote distribution



D (52%)

A (48%)

-   **macrawat**

Highly Voted



 2 years, 1 month ago



It should be A,
I just created a storage account,
then created a file share,
went to IAM,
and it says : To give individual accounts access to the file share (Kerberos), enable identity-based authentication for the storage account.
upvoted 120 times
-   **c75e123** 4 months, 2 weeks ago



Still in 2024, is A correct



3. In the File share settings section, select Identity-based access: Not configured.



4. Under Microsoft Entra Domain Services select Set up, then enable the feature by ticking the checkbox.

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-domain-services-enable?tabs=azure-portal#enable-microsoft-entra-domain-services-authentication-for-your-account>
upvoted 2 times
-   **yettie79** 2 years, 1 month ago

A is correct I am getting the same message when I go to IAM on File Share.
'To give individual accounts access to the file share (Kerberos), enable identity-based authentication for the storage account'
upvoted 10 times
-   **riquesg** 2 years ago

Correct. Did the same. Very tricky. But this is the right answer.
upvoted 2 times
-   **garmatey** 1 year, 11 months ago

but its not asking how to give access, its asking what to do first. So dont you need to configure the access control before enabling identity-based data access for the file shares in storage1?
upvoted 4 times
-   **Indy429** 1 year, 4 months ago

I also thought it was A. Then I freaked and started doubting when I saw the Vote Distribution being 50-50 between A & D. Thanks for testing and confirming for us. Correct answer should be A then!
upvoted 5 times
-   **Slimus** 2 years ago

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview>
How it works
Azure file shares use the Kerberos protocol to authenticate with an AD source.
You can enable identity-based authentication on your new and existing storage accounts using one of three AD sources: AD DS, Azure AD DS, or Azure AD Kerberos (hybrid identities only). Only one AD source can be used for file access authentication on the storage account, which

applies to all file shares in the account. Before you can enable identity-based authentication on your storage account, you must first set up your domain environment.

upvoted 3 times

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

Selected Answer: A

After arguing with ChatGPT here is the answer:

The correct steps to assign User1 the Storage File Data SMB Share Contributor role for share1 are:

1. Enable identity-based data access for the file shares in storage1.
 2. Configure Access control (IAM) for share1 and add User1 as a role assignment with the Storage File Data SMB Share Contributor role.
- So the correct answer is A.

upvoted 22 times

  **AndreLima** 1 year, 11 months ago

kkkkkkkkkkkkkkkk

upvoted 2 times

  **maxsteele** 1 year, 7 months ago

lol you cant trust ChatGPT to be truthful.


upvoted 20 times

  **4f45fce** Most Recent 2 weeks, 1 day ago

Selected Answer: A

chatGpt's answer is A

upvoted 1 times

  **rmacjj** 3 weeks, 5 days ago

Selected Answer: D

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions?tabs=azure-portal>

To assign an Azure role to a Microsoft Entra identity, using the Azure portal, follow these steps:

1. In the Azure portal, go to your file share, or create an SMB file share.
2. Select Access Control (IAM).
3. Select Add a role assignment
4. In the Add role assignment blade, select the appropriate built-in role from the Role list.
5. Leave Assign access to at the default setting: Microsoft Entra user, group, or service principal. Select the target Microsoft Entra identity by name or email address. The selected Microsoft Entra identity must be a hybrid identity and cannot be a cloud only identity. This means that the same identity is also represented in AD DS.
6. Select Save to complete the role assignment operation.

upvoted 1 times

  **kriChe27** 1 month, 1 week ago

Selected Answer: A

The correct answer is A. Enable identity-based data access for the file shares in Storage1

Enable identity-based data access for the file shares in Storage1:

This step is necessary to allow Azure AD identities to access the file shares. Without enabling identity-based data access, you cannot assign Azure AD roles like the Storage File Data SMB Share Contributor role to users for accessing file shares.

upvoted 1 times

  **kriChe27** 1 month, 1 week ago

Modify the security profile for the file shares in Storage1:

This option is not relevant to the task. Modifying the security profile does not enable identity-based access or allow role assignments. Security profiles typically involve settings related to encryption, access protocols, and other security configurations.

Select Default to Azure Active Directory authorization in the Azure portal for Storage1:

While this option is related to enabling Azure AD authorization, it is not the first step. You need to enable identity-based data access first before you can configure Azure AD authorization settings.

upvoted 1 times

  **AndrewChedid** 1 month, 1 week ago

Selected Answer: D

Go to Azure Portal

Create a new storage account

Create a new File Share

Go to the File Share > IAM > Add Role Assignment > Storage File Data SMB Share Contributor

upvoted 1 times

  **Ponpon3185** 1 month, 3 weeks ago

Selected Answer: D

Tested and "Identity-based access: Not configured"

upvoted 1 times

  **netloony** 1 month, 3 weeks ago

Selected Answer: D

Just tested it, create storage, selected IAM and gave the user the role.



upvoted 1 times

  **Ponpon3185** 1 month, 4 weeks ago

Selected Answer: D

D is ok tested with a pay as you go

upvoted 2 times

  **vrn1358** 3 months ago

Selected Answer: D

Today, Feb 2025, you i could add Storage File Data SMB Share Contributor role for a user without enable identity-based data access for the file shares in storage1.

D is correct

upvoted 2 times

  **Bravo_Dravel** 3 months, 1 week ago

Selected Answer: A

C. Select Default to Azure Active Directory authorization in the Azure portal for storage1: While this step is necessary, it comes after enabling identity-based data access. Without enabling identity-based access first, this setting alone won't work.

upvoted 1 times

  **youngjanpawel** 4 months ago

Selected Answer: D

By the way - If I need wait for moderator approval my comment. Why comments with wrong answers are visible? I see a lot of new comments (1-6 months ago) "YEA I HAD A CHAT WITH CHAT GPT THE ANSWER IS 100% A" - Hollllyyy and the price is higher and higher....

upvoted 1 times

  **youngjanpawel** 4 months ago


Selected Answer: D

Correct answer is D

I tried the same way like macrawat however in my case that works - inside created file share "share1" I was able to grant access from IAM to user. State of identity-based access is "not configured" as on screenshot from microsoft doc

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-domain-services-enable?tabs=azure-portal>

upvoted 2 times

  **MaDota** 3 months, 3 weeks ago

Really? see the documentation that you sent, what's the first thing being configured?

upvoted 4 times

  **danlo** 4 months, 3 weeks ago

Selected Answer: A

Just repro in a lab with a new storage account.

Identity-based access can be enabled in two steps for a particular share in this storage account. This allows individual users to use their Active Directory or Microsoft Entra account to gain access to a specific file share.

Step 1: Enable an identity source

upvoted 1 times

  **Mark74** 5 months ago

Selected Answer: A

A for me is correct



upvoted 1 times

  **JPA210** 6 months ago

Selected Answer: A

Definetly A is the correct answer. That is the first step.

upvoted 1 times

  **Yoooom** 6 months, 2 weeks ago

Selected Answer: A

The answer is A

upvoted 1 times

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the User Access Administrator role for VNet1.
- C. Remove User1 from the Security Reader and Reader roles for Subscription1.
- D. Assign User1 the Contributor role for VNet1.

Correct Answer: B

Community vote distribution

B (97%)

- msramzan

Highly Voted

2 years, 1 month ago

many time repeated question

upvoted 26 times
- Shadowner

Highly Voted

2 years, 1 month ago

Selected Answer: B

B is indeed correct.
Only User Access Administrator role and Owner role can assign permissions.

upvoted 11 times
- 58b2872

Most Recent

4 months ago

Selected Answer: B

isn't repeated too much !!!

upvoted 1 times
- RajeshwaranM

4 months, 1 week ago

Selected Answer: B

B is the answer , Many time repeated questions.

upvoted 1 times
- Mark74

5 months ago

Selected Answer: B

B for me is correct

upvoted 1 times
- minura

7 months ago

Selected Answer: B

you need to assign the User Access Administrator role.

upvoted 1 times
- [Removed]

8 months ago

Selected Answer: B

B is corerct



upvoted 1 times
- No_Restaurant9617

8 months, 3 weeks ago

"How many stocks does this question in stock? 1,2,3,4,5 + 5!"

I swear they had to show us this question 5 times already lol

upvoted 2 times

  **No_Restaurant9617** 8 months, 3 weeks ago

Answer is B. Assign User1 the User Access Administrator role for VNet1.



"Only User Access Administrator role and Owner role can assign permissions."

upvoted 1 times

  **joemiller19762023** 1 year, 2 months ago

This question comes up a good bit on the site lol.

upvoted 3 times

  **Hi_09** 1 year, 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

  **BluAlien** 1 year, 3 months ago

Selected Answer: A

Yes you can configure Access control to user1 for share1 without any problem, but... when you try to open the file share in storage account with user1 you got the error:

You do not have permissions to list the data using your user account with Microsoft Entra ID...

upvoted 1 times

  **Elaine12345** 1 year, 4 months ago

sorry link bevor was wrong:

<https://www.iorad.com/player/2078214/Enable-identity-based-authentication-for-Azure-AD-on-your-storage-account--Set-permissions-to-Reader#trysteps-13>

upvoted 1 times

  **Elaine12345** 1 year, 4 months ago

<https://ior.ad/8IDA?iframeHash=viewsteps>

upvoted 1 times

  **Studyingengineer** 1 year, 5 months ago

Selected Answer: B

Repetitive question. This one must be simply on my exam next week :D

upvoted 3 times

  **GoldenDisciple2** 1 year, 8 months ago

I hope that the AZ-104 is just different variations of this question 60 times.

upvoted 7 times

  **oopspruu** 1 year, 8 months ago

This question has appeared too many times. It better be on the exam now lol

upvoted 3 times

  **GoldenDisciple2** 1 year, 8 months ago

I know right. lol I hope it's on the exam at least 10 times.

upvoted 1 times

  **TonySuccess** 1 year, 10 months ago

I used to be a question, but now I am the answer

upvoted 6 times

  **GoldenDisciple2** 1 year, 8 months ago

LMAO hilarious

upvoted 2 times

HOTSPOT -

You have an Azure AD tenant named adatum.com that contains the groups shown in the following table.


Name	Type	Member of
Group1	Security	None
Group2	Security	Group1

Adatum.com contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You assign an Azure Active Directory Premium P2 license to Group1 as shown in the following exhibit.

Assign license

 Got feedback?

Users and groups

Assignment options

Review + assign

Azure Active Directory Premium P2

Azure Active Directory Premium P1

OffOn

Azure Active Directory Premium P2

OffOn

Microsoft Azure Multi-Factor Authentication

OffOn

Microsoft Defender for Cloud Apps Discovery

OffOn

Group2 is NOT directly assigned a license.

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
You can assign User1 the Microsoft Defender for Cloud Apps Discovery license.	<input type="radio"/>	<input type="radio"/>
You can remove the Azure Active Directory Premium P2 license from User1.	<input type="radio"/>	<input type="radio"/>
User2 is assigned the Azure Active Directory Premium P2.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements

You can assign User1 the Microsoft Defender for Cloud Apps Discovery license.

You can remove the Azure Active Directory Premium P2 license from User1.

User2 is assigned the Azure Active Directory Premium P2.

Yes

No

☒

☐

☐

☐

☐

☒

☒

Correct Answer:

- ExamHelp22

Highly Voted

1 year, 12 months ago

YNN

1) Y, You can assign users MS Defender for Cloud Apps on a per user basis.

2) N, You cannot remove the P2 license as User1 is in Group1.

3) N, nested group assignments don't work

upvoted 131 times
- RickySmith

1 year, 8 months ago

I agree with this. I tested it on my trial dev tenant. i assigned a user only the AADP1 license from the E5 Deve license by a group. After it was assigned for a while, I went in and assigned the user the same license directly and onlswitched off a bunch of sub licenses at random. Checked after a day and the user was assigned the cumulative of the 2, so in the question, 1 is definitely Y.

The orrect answers should be as below.

1)Y. Additional licenses can be assigned on to of a group assignment with a cumulatve result.

2)N. The licenses is assigned by group, so without removing the group, the license cannot be removed. tested this and everything is greyed out at a user level.

3)N. License assignments are restricted to only the first level of the group.

upvoted 13 times
- nmshrwt

1 year, 4 months ago

question clearly states license is 'NOT' ASSIGNED DIRECTLY VIA GROUP BASED LICENSING'

upvoted 3 times
- Exam124352345

4 months, 1 week ago

N,N,N Tested laboratorio.

upvoted 1 times
- Soudenho

6 months, 1 week ago

Yes, you can still assign Microsoft Defender for Cloud Apps to a user even if it's turned off at the resource group level. However, the user will not be monitored until the service is enabled for the resource group or subscription they belong to.

upvoted 1 times
- DJHASH786

9 months, 1 week ago

Answer is NNN, tested in LAB

upvoted 9 times
- Exilic

Highly Voted

1 year, 11 months ago



OpenAI

"No: User1 is a member of Group1, which has been assigned the Azure Active Directory Premium P2 license, but not the Microsoft Defender for Cloud Apps Discovery license. Since Group1 does not have the Microsoft Defender for Cloud Apps Discovery license assigned, User1 cannot be assigned that license either.

No: User1 is a member of Group1, which has been directly assigned the Azure Active Directory Premium P2 license. Since User1 inherits the license from Group1, the Azure Active Directory Premium P2 license cannot be removed from User1 individually. It can only be removed by removing the license assignment from Group1.

No: User2 is a member of Group2, which is not directly assigned any licenses. Therefore, User2 does not inherit the Azure Active Directory Premium P2 license or any other license assigned to Group2. To assign the Azure Active Directory Premium P2 license to User2, it would need to be directly assigned to User2 or to a group that User2 is a member of."

upvoted 57 times

  **o0o0** 1 year, 8 months ago

You are are not wrong in the explanation. However, the first two questions use the verb "CAN". Based, on that, I want to ask you, what happens if I remove "USER1" from "GROUP1".

Moreover, the Microsoft Defender for Cloud Apps Discovery license can be assigned to one USER.

Obviously USER2 can not get any license because of the netted groups.

Base on the above, I will go for:



Yes-Yes-No.

upvoted 3 times

  **hebbo777** 1 year, 5 months ago



question given you a scenario to work on it not can and doing your out of the box workaround!

upvoted 2 times

  **Yodao** 1 year, 11 months ago

You are correct because defender is already off for assignment .

upvoted 3 times

  **xian05** 1 year, 8 months ago

Much confusion on question 1.

But if the license could not be assigned, the licensed would not be available or greyed out.

Which it isn't.



Does anybody have the same experience?

upvoted 1 times

  **maxsteele** 1 year, 7 months ago

you cant trust AI sources. They are not reliable sources of factual information

upvoted 10 times

  **ggogel** 1 year, 5 months ago

How can this have 41 upvotes?! Answers of generative AI, such as Chat GPT, are not reliable! It's called AI hallucination. Ask it a question to a difficult technical problem and the answer will most likely contain errors.

upvoted 10 times

  **cd4199f** Most Recent 2 months, 3 weeks ago

NYN

1. The option is off in the license Section.

2. Yes, if a license is assigned to a group in Azure AD, it is automatically assigned to all its members.

3. No, User2 will NOT receive the Azure AD P2 license.



Reason: Nested Group Licensing is NOT Supported in Azure AD

Licenses do NOT inherit through nested groups in Azure AD.

If Group1 is assigned an Azure AD P2 license, only its direct members receive the license.

Group2 (being a member of Group1) does NOT inherit the license, and neither do its members (like User2).

upvoted 2 times

  **Abhisk127** 3 months, 1 week ago



1) Y, You can assign users MS Defender for Cloud Apps on a per user basis.

2) N, You cannot remove the P2 license as User1 is in Group1.

3) N, nested group assignments don't work

This sounds correct because license is on the group and the question only says about the user, so meaning directly from user properties but as you say its tricky question but I think this is correct, per user you can assign that license and you can't remove a license assigned via a group from the users properties. If you want to remove you must remove them from the group itself and nested group won't work for licensing.

upvoted 3 times

  **sca88** 5 months, 3 weeks ago



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

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced>

So it should be NYN.

Please, before anwer and write explanation, please read the OFFICIAL Microsoft Documentation, not the Copilot or Chat Gpt answer. There are a lot of confusion here. Let's try to have a clean discussion, always reporting official Microsoft documentation link

upvoted 3 times



  **Chuong0810** 6 months ago

#1-NO. Azure AD Premium P2 include Microsoft Defender for Cloud Apps Discovery.It is included in Microsoft 365 E3 and Microsoft Entra ID P1 licenses

#2-YES. There are 2 method to remove P2 lic from User1: 1. Remove User1 from Group1. 2. Directly remove the P2 license from User1

#3-NO. nested group assignments don't work.

upvoted 2 times

  **jamesf** 6 months, 2 weeks ago

NNN

#1 No - Microsoft Defender for Cloud Apps Discovery license is OFF.

#2 No - Since the license is assigned to a group, you cannot remove the license from user1 directly. Instead, you remove the license by removing User1 from group1.

#3 No - License assignments are restricted to only the first level of the group.

upvoted 1 times

  **[Removed]** 8 months ago


WRONG

No

No

No

upvoted 3 times

  **CheMetto** 9 months, 3 weeks ago

The link of youtube isn't correctly. You need to trust what he is saying, but you can check it by yourself. Create your tenant for free as an azure developer. I've in my test tenant E5 for developerSo:

I created an user named "test user"

I created a group named "test license"

i assigned this license (E5 developer) to the group named "test license" where i turned off Microsoft defender for cloud apps. I wait few minutes so then user appear to the license tab where services enable are 65 of 66 (Microsoft defender for cloud apps is the only one turned off).

After that, i assign directly to the user the same license, with different service option (i keep everything turned on).

The result show:

User has 2 assignment, directly and inherited from test license. The service enabled are 66 of 66 (so microsoft defender for cloud apps is correctly assigned).

My answer are Y N N

upvoted 1 times

  **Jedi_sg2000** 9 months, 3 weeks ago

NNN is the answer!

upvoted 1 times

  **Jedi_sg2000** 9 months, 3 weeks ago

1 - the option is greyed out.. you are unable to do it

upvoted 1 times

  **varinder82** 11 months, 2 weeks ago

Final Answer : YNN

upvoted 1 times

  **Joseeph** 11 months, 3 weeks ago

N,N,N,

Gracias nchebbi, porque estas preguntas están resueltas en el video, donde hicieron el laboratorio. <https://youtu.be/np-6s3N-1iQ?t=201>

upvoted 2 times

  **ssky** 1 year ago

1. All Microsoft Cloud services that require user-level licensing are supported. This support includes all Microsoft 365 products, Enterprise Mobility + Security, and Dynamics 365.

2. Group-based licensing is currently available through the Azure portal and through the Microsoft Admin center.

3. Microsoft Entra ID automatically manages license modifications that result from group membership changes. Typically, license modifications are effective within minutes of a membership change.

A user can be a member of multiple groups with license policies specified. A user can also have some licenses that were directly assigned, outside of any groups. The resulting user state is a combination of all assigned product and service licenses. If a user is assigned same license from multiple sources, the license will be consumed only once.

upvoted 1 times

  **L3w1s** 12 months ago

As per this article <https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced>

The Microsoft 365 admin center doesn't currently support group-based licensing. If a user inherits a license from a group, this license appears in the Office admin portal as a regular user license. If you try to modify that license or try to remove the license, the portal returns an error message. Inherited group licenses can't be modified directly on a user.

So 2) No

upvoted 1 times

  **Anirban91** 1 year ago

what is the correct answer?



upvoted 1 times

  **Amir1909** 1 year, 1 month ago

Yes
No
No
upvoted 1 times

  **bhagyashree11** 1 year, 2 months ago

This is very frustrating, why examtopics didnt added correct answers. For every question there is conflict answers in comment
upvoted 9 times

  **GlixRox** 11 months ago
because the answers are *free*
upvoted 2 times

  **Amir1909** 1 year, 2 months ago

Yes
No
No
upvoted 1 times

HOTSPOT

-

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

Name	User type	On-premises sync enabled
User1	Member	No
User2	Member	Yes
User3	Guest	No

You need to modify the JobTitle and UsageLocation attributes for the users.

For which users can you modify the attributes from Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

JobTitle: ▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3

UsageLocation: ▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3

Answer Area**Correct Answer:**

JobTitle: ▼

- User1 only
- User1 and User2 only
- User1 and User3 only**
- User1, User2, and User3

UsageLocation: ▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3**

 **JeremyChainsaw** Highly Voted 1 year, 9 months ago

Users syncing from an On Prem AD to AAD cannot have the job title altered in AAD. it would need to be done in local AD , as AADC by default synchronizes the jobTitle property. Usage location is set only on the cloud side for all users, and Guest users can have their job titles set as well as cloud native (AAD) users.

Source - I've been the AD and AAD admin for years at several organizations.

upvoted 61 times

 **maxsteele** 1 year, 7 months ago

so the correct answer is:

1 and 3

and

1,2, and 3

is that correct?

upvoted 25 times

- LPaul

Highly Voted

1 year, 6 months ago

If You read the question carefully the key word will be <On-Premises Sync Enable>, when Status is "YES" that means the user is in the On-prem AD . it also means you cant change in On Azure AD , When the status is "NO" that means the Users is at AZURE AD . so the answer will be User 1 and User3 only for Jobtitle

upvoted 28 times
- RanPo

7 months, 4 weeks ago

the best explanation so far

upvoted 2 times
- op22233

1 year ago

Thank you for the understanding you brought.

upvoted 2 times
- chandiochan

Most Recent

2 months, 1 week ago

JobTitle modification

User1 (Cloud-only) → Can be modified in Azure AD.

User2 (On-Prem Sync) → Cannot be modified in Azure AD.

User3 (Guest User) → Cannot be modified in Azure AD.

✓ Correct Answer: "User1 only"

"UsageLocation" modification

User1 (Cloud-only) → Can be modified in Azure AD.

User2 (On-Prem Sync) → Can be modified in Azure AD (not synced from on-prem AD).

User3 (Guest User) → Can be modified in Azure AD.

✓ Correct Answer: "User1, User2, and User3"

upvoted 1 times
- JustinYoo

4 months, 3 weeks ago

You can update their attributes directly in the Microsoft Entra admin center if you are updating Microsoft Entra ID attributes, such as Usage Location.

upvoted 1 times
- [Removed]

8 months ago

CORRECT

upvoted 2 times
- deathazul

1 year, 2 months ago

The Answer is correct only the user that is with the on-premise synchronization active can't modified the job title vault because came from the onpremise active directory

upvoted 1 times
- GrossmanAirOne

1 year, 4 months ago

What are you all using your AZ-104 cert for? Increase in pay or your company requires you to have it as they use it for their msft partner solution designation program?

upvoted 3 times
- BhunB

1 year ago

10k/year raise

upvoted 2 times
- 18c2076

1 year, 1 month ago

the answer here is almost always due to company only benefit.

upvoted 1 times
- SQL_Student

1 year, 4 months ago

User 1 does not have cloud sync enabled so I guess that means that this user is a cloud only user..

upvoted 1 times
- STEVE_MEKA

1 year, 7 months ago

Nice question

upvoted 2 times
- Mehedi007

1 year, 9 months ago

User 1 & 3 only: "You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory." <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-manage-user-profile-info#profile-categories>

User 1, 2, 3: <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-manage-user-profile-info#add-or-change-profile-information>



upvoted 10 times
- antropaws



1 year, 9 months ago



"You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory".

Since User1 and User3 have On-Premises sync enabled, I'd say:

Box 1: User1 and User3 only.
Box 2: User1, User2, and User3.
upvoted 2 times

  **antropaws** 1 year, 9 months ago
Disregard.
upvoted 2 times



  **shiraghami** 1 year, 8 months ago
But User 1 and User 3 don't have On-Premises sync enabled
upvoted 4 times



  **cvalladares123** 1 year, 9 months ago
This question is planned in a very bad way:



1. JobTitle should be modified for ALL users since the second is hosted in Azure and his main identity solution is not an On-premise tool --> "You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory". Then, as account authority source is AD, answer should be User 1, 2 and 3



2. User 1, User 2 and User 3 is the correct answer



Check source --> <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-manage-user-profile-info>
upvoted 4 times

  **Pakawat** 1 year, 10 months ago
Found this Q in the exam, 3/7/23
upvoted 7 times



  **efayed** 1 year, 10 months ago
<https://www.examttopics.com/discussions/microsoft/view/38424-exam-az-104-topic-2-question-32-discussion/>
upvoted 10 times



  **fessebook** 1 year, 9 months ago
Not exactly the same question.
upvoted 2 times



  **alexvv89** 1 year, 7 months ago
I believe it's pretty much the same questions.
JobTitle: User1 and User3
UsageLocation: all Users
upvoted 2 times



  **Codelawdepp** 1 year, 8 months ago
So correct solution is:
JobTitle: User1 (Member and AzureAD Source) and User3 (Guest and Microsoft Account) only

UsageLocation: all users (User1, User2 and User3)
upvoted 3 times

  **fongode** 1 year, 10 months ago
JobTitle can't be changed in AD in hybrid setup
upvoted 4 times

  **antropaws** 1 year, 9 months ago
Where does it say so?
upvoted 1 times

  **rteinformatica** 1 year, 9 months ago
I checked it in the laboratory. It cannot be changed. Only the location, of the two concepts that ask
upvoted 2 times

  **xian05** 1 year, 8 months ago
The question states: For which users can you modify the attributes from Azure AD?
Not from AD, but AAD.
upvoted 1 times

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

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-MgUser cmdlet for each external user.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (97%)

- iamchoy

Highly Voted

1 year, 7 months ago

Selected Answer: B

The `New-MgUser` cmdlet is part of the Microsoft Graph PowerShell module, and it's used for creating new users in Azure AD. However, when creating guest users (or B2B users), you typically would invite them rather than create them like regular members.

The cmdlet you'd want to use for inviting external guest users is `New-AzureADMSInvitation` if you're using the AzureAD module or a related command in the Microsoft Graph module.

Given the provided solution, the answer is:

B. No

upvoted 22 times
- Rams786

Highly Voted

1 year, 7 months ago

This question was on my exam on 22 Sep 2023. scored 900 i answered B

upvoted 5 times
- Ponpon3185

Most Recent

1 month, 4 weeks ago

Selected Answer: B

New-MgInvitation : <https://learn.microsoft.com/en-us/entra/external-id/bulk-invite-powershell>

upvoted 1 times
- 58b2872

4 months ago

Selected Answer: B

No for sure, there is no URL of redirection and the command is wrong

upvoted 2 times
- RajeshwaranM

4 months, 1 week ago

Selected Answer: B

B is the correct answer

upvoted 1 times
- [Removed]

8 months ago

Selected Answer: B



B is corerct

upvoted 1 times
- Amir1909

1 year, 2 months ago

No is correct

upvoted 2 times



  **vsvoid** 1 year, 3 months ago

Selected Answer: A

Although invitation url is not in the csv file, we can still create the user by specifying url when running the script like here

<https://learn.microsoft.com/en-us/entra/external-id/bulk-invite-powershell#send-bulk-invitations>

upvoted 1 times

  **vsvoid** 1 year, 3 months ago

Sorry wrong question, please ignore the above

upvoted 1 times

  **VV11_SS22** 1 year, 8 months ago

answer is actually "B - No" because they are guest users and should be invited not created, therefore make use of Bulk invite - <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite>

upvoted 1 times

  **binhdortmund** 1 year, 9 months ago



Do we have a similar question and the answer is no due to missing RedirectURL in the CSV?

upvoted 3 times

  **fead** 1 year, 8 months ago

yeah, that was to be created from AZ portal

upvoted 2 times

  **MHguy** 1 year, 9 months ago



new-mguser seems only for creating new users, not guest:

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/new-mguser?view=graph-powershell-1.0&preserve-view=true>

for the guest under microsoft graph is that one: New-MgInvitation

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0&preserve-view=true>

upvoted 3 times

  **conip** 1 year, 8 months ago



but ...

-UserType

A string value that can be used to classify user types in your directory, such as Member and Guest. Returned only on \$select. Supports \$filter (eq, ne, not, in, and eq on null values). NOTE: For more information about the permissions for member and guest users, see [What are the default user permissions in Azure Active Directory](#)



<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/new-mguser?view=graph-powershell-1.0>

upvoted 1 times

  **Pakawat** 1 year, 10 months ago

Found this Q in the exam, 3/7/23

upvoted 3 times

  **tech07** 1 year, 10 months ago

Selected Answer: B

New-AzureADMSInvitation or New-MgInvitation can be used to invite users, Not New-MgUser

<https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0#users>



upvoted 3 times

  **marlonbenfica** 1 year, 10 months ago

Correct answer: B (NO).

Since there is a .csv file with the data, just import it in bulk.

upvoted 2 times



  **fongode** 1 year, 10 months ago

Answer is correct. New-MgUser is for Microsoft Graph and not for GuestInvite

See also

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/new-mguser?view=graph-powershell-1.0>

upvoted 1 times

  **pubalaji** 1 year, 10 months ago

Are you saying the correct answer is Option B?

upvoted 3 times

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

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-MgInvitation cmdlet for each external user.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Community vote distribution

A (89%)

11%

- iamchoy

Highly Voted

1 year, 7 months ago

Selected Answer: A

The New-MgInvitation cmdlet is part of the Microsoft Graph PowerShell module. It's used to create an invitation to an external user. When the invited user redeems their invitation, a guest user is created in the directory.

If you use a PowerShell script that loops through each external user in the CSV file and runs the New-MgInvitation cmdlet for each of them, it will send out invitation emails to each of those external users. Once an external user accepts the invitation, they'll be added to the Azure AD tenant as a guest user.

So, using the New-MgInvitation cmdlet in a PowerShell script for each external user does meet the goal of creating a guest user account in contoso.com for each of the 500 external users.

The answer is:

A. Yes

upvoted 29 times
- Shark006

1 year, 6 months ago

The cmdlet New-MgInvitation requires the Redirection URL.

"The URL the user should be redirected to once the invitation is redeemed. Required."

Reference:

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>

So the answer is:

B. No

upvoted 16 times
- Ponpon3185

1 month, 4 weeks ago

Wrong: <https://learn.microsoft.com/en-us/entra/external-id/bulk-invite-powershell> so Answer is B with a portal Bulk Invite May be

upvoted 1 times
- Batiste2023

1 year, 5 months ago

As you run the command from a script, you can hardcode a redirection URL into it.

A is correct, I would say!

upvoted 8 times
- SDiwan

1 year, 3 months ago

the correct answer is "A". We can assume that invitation url is present in the powershell script. also, it mentions the command is used for "each" user, so assuming there is a loop and this command runs for each user inside the loop.

upvoted 2 times

  **tech07** Highly Voted 1 year, 10 months ago

Selected Answer: A

New-AzureADMSInvitation or New-MgInvitation can be used to invite users, Not New-MgUser
<https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msolinet-cmdlet-map?view=graph-powershell-1.0#users>
upvoted 7 times

  **Ponpon3185** Most Recent 1 month, 3 weeks ago



Selected Answer: B

To my mind no cause not speak about URLRedirection : <https://learn.microsoft.com/en-us/entra/external-id/b2b-quickstart-invite-powershell>
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: A

it's A
upvoted 2 times

  **60ties** 9 months, 3 weeks ago

Selected Answer: A

As per this link: "<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>"

The "InviteRedirectUrl" requirement is a Boolean. So can be included (as True) or ignored (as False).

So A is the correct answer
upvoted 3 times

  **Dil_12345** 11 months, 1 week ago


The New-MgUser cmdlet creates a new user account in Azure AD, not a guest user account. To create a guest user account, you need to use the New-AzureADMSInvitation cmdlet, which sends an invitation email to the external user and adds them to the tenant as a guest.
upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

A. YES - using a PowerShell script with the New-MgInvitation cmdlet is an effective way to meet the requirement of creating guest user accounts for 500 external users in the contoso.com Azure AD tenant. This approach leverages the power of automation and Microsoft's API to accomplish the task efficiently and effectively.
upvoted 1 times

  **tashakori** 1 year, 1 month ago

Yes is correct
upvoted 1 times



  **MatAlves** 1 year, 2 months ago

CSV doesn't need to contain the -InviteRedirectUrl. It can be added later.

<https://learn.microsoft.com/en-us/entra/external-id/bulk-invite-powershell#send-bulk-invitations>
upvoted 1 times

  **e004a35** 1 year, 3 months ago

The CSV is missing a Redirect URL and the New-MgInvitation command requires it. Correct answer is No.
upvoted 1 times

  **vsvoid** 1 year, 3 months ago

Selected Answer: A

Although invitation url is not in the csv file, we can still create the user by specifying url when running the script like here

<https://learn.microsoft.com/en-us/entra/external-id/bulk-invite-powershell#send-bulk-invitations>
upvoted 2 times



  **ggogel** 1 year, 5 months ago

There simply is no clear answer to this question!

If you use the CSV in PowerShell, you would need another Cmdlet Import-Csv to read the CSV file. Then, you could iterate over the email addresses and specify the same redirection URL for every guest.

On the other hand, there is the same question about using Azure Portal Bulk Import. I could also argue that I can simply open the file in Excel and set a redirection URL for every user.

So it really comes down to how you interpret the question. Suppose you can just use the existing CSV and the given Cmdlet or Azure Bulk Import, then the answer is always FALSE. If you can add one extra step or Cmdlet, then it is always TRUE.
upvoted 4 times

  **ggogel** 1 year, 5 months ago

After reading the question again, it says: "you create a PowerShell script". In my opinion, this implies that we can use other Cmdlets. So I would lean towards "YES" here.
upvoted 4 times

  **clg003** 1 year, 5 months ago

Selected Answer: A

Yes with New-MgIInvitation the -InviteRedirectUrl flag is not required. You can also put one in with the command line.

"-InviteRedirectUrl Required: False"

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>
upvoted 3 times

  **ggogel** 1 year, 5 months ago

In the text explaining the parameter, it says "Required". In the tables, it says "Required: False" for every parameter, even the mail address.
upvoted 1 times


  **bhadrisn** 1 year, 4 months ago

Selected Answer : B
For "InvitedUserEmailAddress" also it states that
Required: False
But this is essential. So the Answer should be "B-No" where without a redirect URL you cannot invite an external user
upvoted 1 times

  **ziggy1117** 1 year, 6 months ago

Selected Answer: B

needs redirection URL
upvoted 3 times

  **amsioso** 1 year, 6 months ago

By portal you need to include the Redirection URL in the csv.
<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite>
Making it with Powershell yo dont need to include in the csv the Redirection URL.
If we can change New-AzureADMSInvitation for New-MgIInvitation in the PowerShell script then the answer is A.
<https://learn.microsoft.com/en-us/entra/external-id/bulk-invite-powershell?source=recommendations#send-bulk-invitations>
upvoted 2 times

  **amsioso** 1 year, 6 months ago

Seem like Yes
<https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0#users>
But we need to install the M Graph PowerShell SDK
<https://learn.microsoft.com/en-us/powershell/microsoftgraph/migration-steps?view=graph-powershell-1.0>
<https://learn.microsoft.com/en-us/powershell/microsoftgraph/installation?view=graph-powershell-1.0>
upvoted 1 times

  **Shark006** 1 year, 7 months ago

Selected Answer: B

The question is: You need to CREATE a guest user account in contoso.com for each of the 500 external users.

The command provided as an answer to this question is New-MgIInvitation, it INVITES guest users and do NOT create users. Answer is B: No.

Reference: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>
upvoted 1 times

  **Shark006** 1 year, 6 months ago

The answer is B but the justification is wrong after reconsideration.
"The URL the user should be redirected to once the invitation is redeemed. Required."
Reference:
<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>
upvoted 6 times

  **Vestibal** 1 year, 7 months ago

Selected Answer: B

La respuesta correcta es la B.

In this quickstart, you'll use the New-MgIInvitation command to add one guest user to your Azure tenant.

Habla de un usuario, en singular. Además, la documentación oficial los ejemplos es de un usuario, no de forma masiva como es la pregunta.
<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-invite-powershell>
<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/bulk-invite-powershell>
upvoted 1 times

You have an Azure subscription named Subscription1 that contains virtual network named VNet1. VNet1 is in a resource group named RG1.

A user named User1 has the following roles for Subscription1:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Assign User1 the Contributor role for VNet1.
- B. Assign User1 the Network Contributor role for VNet1.
- C. Assign User1 the User Access Administrator role for VNet1.
- D. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.

Correct Answer: C

Community vote distribution

C (100%)

vsvoid Highly Voted 1 year, 3 months ago

Selected Answer: C

This question has already appeared multiple times
upvoted 10 times

Vinny Most Recent 2 months, 3 weeks ago

Selected Answer: C

Kitne baar repeat hoga yeh Q.
upvoted 1 times

58b2872 4 months ago

Selected Answer: C

repeated many times
upvoted 2 times

Alex2259ggf 4 months, 1 week ago

Selected Answer: C

This question is repeated many times
upvoted 2 times

[Removed] 8 months ago

Selected Answer: C

C is corerct
upvoted 1 times

No_Restaurant9617 8 months, 3 weeks ago

"How many stocks does ExamTopic has this question in stock?
1... 2.. 3... 4... 5... + 5!"

This has to be the 5 time this question with the same answer has appeared.

Answer: C. Assign User1 the User Access Administrator role for VNet1.
upvoted 2 times

ELearn 9 months, 3 weeks ago

Selected Answer: C

C. Assign User1 the User Access Administrator role for VNet1.
upvoted 1 times

TedM2 1 year, 6 months ago

Selected Answer: C

Three of the answers involve assigning a Contributor role. Contributor does not include the ability to assign rights, permissions, or roles. Therefore the correct answer has to be C, assign the User Access Admin role.

upvoted 4 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: C

To allow User1 to assign the Reader role for VNet1 to other users, User1 needs to have permissions related to Azure RBAC (Role-Based Access Control).

Among the listed options:

A. Assign User1 the Contributor role for VNet1. - The Contributor role allows a user to manage everything except access.

B. Assign User1 the Network Contributor role for VNet1. - This role provides permissions to manage networking resources, not role assignments.

C. Assign User1 the User Access Administrator role for VNet1. - This role provides permissions to manage user access to Azure resources, which means User1 can assign roles to other users for VNet1.

D. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1. - This does not directly provide User1 with permissions to manage user access.

The correct action is:

C. Assign User1 the User Access Administrator role for VNet1.

upvoted 1 times

  **Vokuhila** 1 year, 8 months ago

Selected Answer: C

Assigning roles to users is at least User Access Administrator

upvoted 1 times

  **AntaninaD** 1 year, 8 months ago

Selected Answer: C

Network Contributor - Lets you manage networks, but not access to them.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>

User Access Administrator - Lets you manage user access to Azure resources.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>

Contributor - Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

T2Q71 - similar question with another possible solution - Assign User1 the Owner role for VNet1.

upvoted 3 times

You have an Azure subscription named Subscription1 that contains virtual network named VNet1. VNet1 is in a resource group named RG1.

User named User1 has the following roles for Subscription1:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- B. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- C. Assign User1 the Network Contributor role for VNet1.
- D. Assign User1 the User Access Administrator role for VNet1.

Correct Answer: D

Community vote distribution

D (100%)

  **[Removed]** 8 months ago

Selected Answer: D

D is corerct

upvoted 1 times

  **3c5adce** 1 year ago



To ensure that User1 can assign the Reader role for VNet1 to other users, you need to give User1 the necessary permissions at the appropriate scope. In this scenario, the user needs permissions specifically related to VNet1.

Option C. Assigning User1 the Network Contributor role for VNet1 is the correct approach. This role grants the user permissions to manage Azure networking resources, including the ability to assign roles such as Reader to other users for the specific virtual network VNet1.

So, the correct answer is:

C. Assign User1 the Network Contributor role for VNet1.



upvoted 1 times

  **vsvoid** 1 year, 3 months ago

Selected Answer: D

Owner and User Access Administrator can assign roles


upvoted 4 times

  **TedM2** 1 year, 6 months ago

Selected Answer: D

Three of the answers involve assigning a Contributor role. Contributor does not include the ability to assign rights, permissions, or roles. Therefore the correct answer has to be D, assign the User Access Admin role.

upvoted 4 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: D

To allow User1 to assign the Reader role for VNet1 to other users, User1 needs to have permissions related to Azure RBAC (Role-Based Access Control).

Among the listed options:

A. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1. - The Contributor role allows a user to manage everything except access.

B. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1. - Again, the Contributor role doesn't grant User1 the ability to assign roles to others.

C. Assign User1 the Network Contributor role for VNet1. - This role provides permissions to manage networking resources, not role assignments.

D. Assign User1 the User Access Administrator role for VNet1. - This role provides permissions to manage user access to Azure resources, which means User1 can assign roles to other users for VNet1.

The correct action to meet the requirement is:

D. Assign User1 the User Access Administrator role for VNet1.

upvoted 2 times

 **AntaninaD** 1 year, 8 months ago

Selected Answer: D

Network Contributor - Lets you manage networks, but not access to them.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>

User Access Administrator - Lets you manage user access to Azure resources.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>

Only User Access Administrator or Owner could assign roles to other users.

upvoted 1 times

HOTSPOT

-

You have an Azure Storage account named storage1 that uses Azure Blob storage and Azure File storage.

You need to use AzCopy to copy data to the blob storage and file storage in storage1.

Which authentication method should you use for each type of storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Blob storage:

Azure AD only
Shared access signatures (SAS) only
Azure AD and shared access signatures (SAS)

File storage:

Azure AD only
Shared access signatures (SAS) only
Azure AD and shared access signatures (SAS)

Answer Area

Correct Answer:

Blob storage:

Azure AD only
Shared access signatures (SAS) only
Azure AD and shared access signatures (SAS)

File storage:

Azure AD only
Shared access signatures (SAS) only
Azure AD and shared access signatures (SAS)

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

First: Azure AD & SAS
Second: SAS

Source: <https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#authorize-azcopy>
upvoted 35 times



 **hank00r** 1 year, 4 months ago

The link you provided states:
"You can provide authorization credentials by using Microsoft Entra ID, or by using a Shared Access Signature (SAS) token".



So it should be Azure AD & SAS for both Questions. Am I getting it wrong?
upvoted 23 times

  **Bravo_Dravel** 3 months, 3 weeks ago

True, both you can use either SAS (Shared Access Signature) or Azure AD (Azure Active Directory) for authorization
upvoted 2 times

  **ggogel** 1 year, 3 months ago



Yes, this must have been changed. The following doc clearly states that Entra ID can be used to authorize access to file shares when using azcopy.
<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>
upvoted 8 times

  **SDiwan** 1 year, 3 months ago

No, if you are targetting copy to the whole "file share" then SAS is the only option. Entra ID can be used , if you are copying a fileor files to a specific folder inside file file share. So, SAS only is correct for 2nd question
upvoted 2 times

  **tableton** 1 year, 1 month ago

But I think the whole file share is not mentioned in the question:
"You need to use AzCopy to copy data to the blob storage and file storage in storage1."
So EntraID could be used to azcopy to file share
upvoted 5 times

  **suddin1** 11 months, 2 weeks ago

I agree, this is what microsoft says here,
" Note


The examples in this article show the use of a SAS token to authorize access. However, for commands that target files and directories, you can now provide authorization credentials by using Microsoft Entra ID and omit the SAS token from those commands. You'll still have to use a SAS token in any command that targets only the file share or the account (For example: 'azcopy make https://mystorageaccount.file.core.windows.net/myfileshare' or 'azcopy copy 'https://mystorageaccount.file.core.windows.net'. "
<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-files>
upvoted 7 times

  **Sameer9371** 1 year, 8 months ago

you are absolutely right
upvoted 3 times


  **[Removed]** Highly Voted  1 year, 4 months ago

Currently supported method of authorization
Blob storage: Microsoft Entra ID & SAS
Blob storage (hierarchical namespace): Microsoft Entra ID & SAS
File storage: SAS only
upvoted 11 times

  **heartfilia42** 1 year, 3 months ago

Sorry, but with the official doc :<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

I don't see anywhere taht you cannot use Azure AD to access File Storage as well as Blob Storage ?
upvoted 4 times

  **Thisisacat** 9 months, 1 week ago

I think for both the answer is 3rd option
upvoted 3 times

  **kriChe27** Most Recent  1 month, 1 week ago

For Azure Blob storage, AzCopy supports two authentication methods:
Azure AD Authentication:
Azure Active Directory (Azure AD) allows you to use your organizational credentials to authenticate and authorize access to Azure Blob storage. This method is secure and integrates with your organization's identity management.
You can use Azure AD to grant permissions to users, groups, or service principals.

Shared Access Signatures (SAS):
SAS tokens provide a way to grant limited access to your Azure Blob storage without sharing your account key.
You can specify the permissions, start time, expiry time, and IP range for the SAS token.

For Azure File storage, AzCopy primarily supports:
Shared Access Signatures (SAS):
Similar to Blob storage, SAS tokens allow you to grant limited access to your Azure File storage.
You can define the permissions, start time, expiry time, and IP range for the SAS token.
upvoted 1 times

  **Jakub4444** 2 months ago

As of February 2025, according to the latest official Microsoft documentation, AzCopy supports the following authentication methods for Azure Blob Storage and Azure File Storage:

1. Azure Blob Storage:

Supported Authentication Methods:

Microsoft Entra ID (formerly Azure Active Directory or Azure AD): Allows for secure, role-based access control.
Shared Access Signature (SAS) Tokens: Provide time-limited and permission-specific access.

2. Azure File Storage:

Supported Authentication Methods:

Microsoft Entra ID: Enables secure access with role-based permissions.

Storage Account Key: Utilizes the account key for authentication.

SAS Tokens are not supported for Azure File Storage with AzCopy.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-files>

upvoted 4 times

  **sca88** 5 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-files>

"The examples in this article show the use of a SAS token to authorize access. However, for commands that target files and directories, you can now provide authorization credentials by using Microsoft Entra ID and omit the SAS token from those commands. You'll still have to use a SAS token in any command that targets only the file share or the account (For example: 'azcopy make

<https://mystorageaccount.file.core.windows.net/myfileshare>' or 'azcopy copy 'https://mystorageaccount.file.core.windows.net'.")

So because the question doesn't talk about specific file or folder the answer provided is correct: 1) AD & SAS

2) ONLY SAS

upvoted 1 times

  **JPA210** 6 months ago

this kind of questions are tricky, because it is not explicit if it is going to copy only some fiiles or the entire share.

The examples in this article show the use of a SAS token to authorize access. However, for commands that target files and directories, you can now provide authorization credentials by using Microsoft Entra ID and omit the SAS token from those commands. You'll still have to use a SAS token in any command that targets only the file share or the account.

upvoted 1 times

  **jamesf** 6 months, 2 weeks ago

The answer is incorrect now because File storage supports Microsoft Entra ID after 11 Jun 2024.

The correct answer is SAS and Microsoft Entra ID for both blob storage and file storage.

There is a registration process to follow to use MS Entra ID for File with AzCopy.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

upvoted 7 times

  **155e6a0** 7 months ago

The answer is incorrect now because File storage supports Microsoft Entra ID after 6/12/2024.

The correct answer is SAS and Microsoft Entra ID for both blob storage and file storage.

There is a registration process to follow to use MS Entra ID for File with AzCopy.



<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

upvoted 3 times

  **[Removed]** 8 months ago

CORRECT

upvoted 2 times

  **Op0m0p** 9 months, 3 weeks ago

It can be authorized with credentials for FileShare as well..

The examples in this article show the use of a SAS token to authorize access. However, for commands that target files and directories, you can now provide authorization credentials by using Microsoft Entra ID and omit the SAS token from those commands. You'll still have to use a SAS token in any command that targets only the file share or the account (For example: 'azcopy make

<https://mystorageaccount.file.core.windows.net/myfileshare>' or 'azcopy copy 'https://mystorageaccount.file.core.windows.net'.

upvoted 3 times



  **varinder82** 11 months, 3 weeks ago

Final Answer:

First: Azure AD & SAS

Second: SAS

upvoted 2 times

  **3c5adce** 11 months, 4 weeks ago

Validated by ChatGPT 4 -

Blob Storage: Azure AD and Shared Access Signatures (SAS)

File Storage: Shared Access Signatures (SAS) only

upvoted 1 times

  **3c5adce** 11 months, 3 weeks ago

Changing my answer

Blob storage: Azure AD and shared access signatures (SAS)

File storage: Azure AD only

upvoted 2 times

  **ssky** 1 year ago

for commands that target files and directories, you can now provide authorization credentials by using Microsoft Entra ID and omit the SAS token from those commands. You'll still have to use a SAS token in any command that targets only the file share or the account

upvoted 4 times

  **tashakori** 1 year, 2 months ago



Correct

upvoted 1 times

  **Ziolupo** 1 year, 2 months ago



Entra ID is now available to authorize Azcopy on Azure file share.

upvoted 5 times

  **allyou** 1 year, 2 months ago

<https://learn.microsoft.com/fr-fr/azure/storage/common/storage-ref-azcopy-copy>

upvoted 2 times

  **allyou** 1 year, 2 months ago

<https://learn.microsoft.com/en-us/training/modules/configure-storage-tools/4-use-azcopy>

upvoted 1 times

  **edurakhan** 1 year, 2 months ago

This link:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

clearly states:

"You can provide AzCopy with authorization credentials by using Microsoft Entra ID. That way, you won't have to append a shared access signature (SAS) token to each command."

The question is kind of confusing - "which SHOULD you use". You COULD use both, but I am assuming Microsoft Entra ID (Azure AD) SHOULD be the right way for both.

upvoted 1 times

HOTSPOT

-

You have an Azure AD tenant that contains a user named External User.

External User authenticates to the tenant by using external195@gmail.com.

You need to ensure that External User authenticates to the tenant by using contractor@gmail.com.

Which two settings should you configure from the Overview blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

The screenshot shows the 'External User' Overview blade in the Azure AD portal. The 'Identities' section is highlighted with a black box, showing the email address 'mail'. The 'My Feed' section includes three tiles: 'Account status' (Enabled), 'Sign-ins', and 'B2B collaboration' (Invitation state: Accepted). The 'B2B collaboration' tile is also highlighted with a black box.

Correct Answer:

The screenshot shows the 'External User' Overview blade in the Azure AD portal. The 'Identities' section is highlighted with a black box, showing the email address 'mail'. The 'My Feed' section includes three tiles: 'Account status' (Enabled), 'Sign-ins', and 'B2B collaboration' (Invitation state: Accepted). The 'B2B collaboration' tile is also highlighted with a black box.

Vestibal 1 year, 7 months ago

If the user wants to sign in using a different email:

- Select the Edit properties icon.
- Scroll to Email and type the new email.
- Next to Other emails, select Add email. Select Add, type the new email, and select Save.
- Select the Save button at the bottom of the page to save all changes

On the Overview tab, under My Feed, select the "Reset redemption" status link in the B2B collaboration tile.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/reset-redemption-status#use-the-microsoft-entra-admin-center-to-reset-redemption-status>

upvoted 44 times

  **PhiloUK** 10 months, 1 week ago

This is right, you can easily confirm this on azure portal.

upvoted 1 times

  **090200f** 11 months ago

more over , we're unable to click on identities link/button. so Edit prop and B2B are the answers

upvoted 2 times

  **Babustest** 1 year, 7 months ago

I totally agree. MS document clearly lists these steps.

upvoted 2 times

  **devops_devops** Highly Voted  1 year, 3 months ago

This question was in exam 15/01/24

upvoted 14 times



  **70ec7c1** Most Recent  1 month, 2 weeks ago

Testing on 03/20/2025. "Reset redemption" is now under B2B Invitation. B2B Collaboration now has link to convert to internal user.

There is no longer a way to directly reach "mail" via Identities. You have to go through "Edit properties" and then to "Contact information"

Given all these changes, highly doubtful that this question will come out in its current form.

upvoted 1 times



  **jamesf** 6 months, 2 weeks ago

"Edit properties"

"B2B collaboration"

<https://learn.microsoft.com/en-us/entra/external-id/reset-redemption-status>

upvoted 2 times

  **lykeman26** 6 months, 3 weeks ago

The question says "Which two settings should you configure from the Overview blade?". I believe "Edit Properties" isn't one. So I think the answer is correct - Identities and B2B Collab.

upvoted 2 times

  **[Removed]** 8 months ago

CORRECT

Edit properties

Identities

B2B collaboration

upvoted 2 times

  **Felas** 1 year ago

Then, the correct answer would be:

"Edit properties".

"B2B collaboration"

?

upvoted 2 times

  **1828b9d** 1 year, 2 months ago

This question was in exam 01/03/2024

upvoted 4 times

  **Amir1909** 1 year, 2 months ago

Edit properties

B2B

upvoted 1 times

  **31c21da** 1 year, 3 months ago

The question is "Which two settings should you configure", it doesn't focus on how you approach that setting, so I recommend question just need us to click the 2 settings: email and redemption.

upvoted 3 times

  **SkyZeroZx** 1 year, 4 months ago

Click in "edit properties" and "Reset redemption Status"

upvoted 2 times

  **[Removed]** 1 year, 4 months ago

This is not correct, if I click on identities I cannot edit the UPN. To edit it, I need to actually go to Edit properties, modify that, and then resent the B2B invitation.

upvoted 2 times

  **[Removed]** 1 year, 4 months ago

<https://learn.microsoft.com/en-us/entra/external-id/reset-redemption-status>

upvoted 1 times

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

1. Edit Identities (new email address)
2. Resend invitation to the new email address.

upvoted 2 times

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

"Which two settings should you configure from the Overview blade?"
Read carefully question very important, right?

upvoted 1 times

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

Select the Edit properties icon.
Scroll to Email and type the new email.
Next to Other emails, select Add email. Select Add, type the new email, and select Save.
Select the Save button at the bottom of the page to save all changes.

Source: <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/reset-redemption-status>

upvoted 2 times

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

Yes it should be 'Edit Properties' option. In the answer image, it is shown as 'identities' attribute, which is not correct.

upvoted 4 times

🗨️ 👤 **Stu444555** 1 year, 8 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/reset-redemption-status>

upvoted 4 times

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

So this source shows that the first step is to do this:
Browse to Identity > Users > All users.

Which can be done from the Overview tab by simply clicking on Identities as noted by the given answer.

Then it states:

"On the Overview tab, under My Feed, select the Reset redemption status link in the B2B collaboration tile."

So the given answer of "Identities" and "B2B Tile" are correct

upvoted 5 times

🗨️ 👤 **BluAlien** 1 year, 3 months ago

No, the Identity referred from the Microsoft article is related to Microsoft Entra Admin Center, here there is the Identity | Users | All Users blade. In Azure Portal you must select User from the Users Blade, the Identity showed in the overview page is totally useless..

So "Edit Properties" and "Reset redemption Status".

upvoted 2 times

You have an Azure subscription that contains the resources shown in the following table.

Name	Description
RG1	Resource group
RG2	Resource group
storage1	Storage account in RG1
Workspace1	Azure Synapse Analytics workspace in RG2

You need to assign Workspace1 a role to allow read, write, and delete operations for the data stored in the containers of storage1.

Which role should you assign?

- A. Storage Account Contributor
- B. Contributor
- C. Storage Blob Data Contributor
- D. Reader and Data Access

Correct Answer: C

Community vote distribution

C (96%)

4%

Babustest

Highly Voted

1 year, 7 months ago

Selected Answer: C

Storage Blob Data Contributor Read, write, and delete Azure Storage containers and blobs.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-blob-data-contributor>

upvoted 27 times

SkyZeroZx

Highly Voted

1 year, 4 months ago

Selected Answer: C

A : No has permissons to delete and is a general role ()
B : Too general
C : Apply requirement , Read , write and delete (<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-blob-data-contributor>
)
D : Impossible to delete

upvoted 9 times

adilkhan

Most Recent

3 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

ayufitri

4 months, 3 weeks ago

Selected Answer: C

C because

Focus on the keyword *container*

Storage Account Contributor: This role grants full management permissions to a storage account, including creating, updating, and deleting data, containers, and storage account settings. This is too broad for the scenario since the requirement is specific to container-level data operations.

Contributor : Similar to A, it offers permissions beyond just the data-level operations.

Storage Blob Data Contributor: This role allows read, write, and delete operations specifically for data in blob containers, without granting full management access to the storage account itself.

Reader and Data Access: (The reason is obvious) This role grants read-only access to resources and data.

upvoted 4 times

🗨️ 👤 **Omer87** 7 months, 3 weeks ago

Selected Answer: C

Storage Blob Data Contributor
upvoted 2 times

🗨️ 👤 **[Removed]** 8 months ago

Selected Answer: C

C is correct
upvoted 3 times

🗨️ 👤 **alsmk2** 8 months, 4 weeks ago

Selected Answer: C

Question refers to data IN a container, so by proxy that means Storage BLOB Data Contributor is the best answer.
upvoted 3 times

🗨️ 👤 **ajay01avhad** 9 months, 1 week ago

C:For the requirement to allow Workspace1 to perform read, write, and delete operations on the data within storage1, the Storage Blob Data Contributor role is the correct choice.
upvoted 2 times

🗨️ 👤 **SofiaLorean** 11 months, 3 weeks ago

For ChatGPT: To allow read, write, and delete operations for the data stored in the containers of storage1 for Workspace1, you should assign the role:

C. Storage Blob Data Contributor

This role provides the necessary permissions for full access to the blobs, including read, write, and delete operations within Azure Storage Blob containers.

Here's a brief overview of why the other roles are not suitable:

A. Storage Account Contributor: This role provides management access to the storage account, which includes operations such as creating and managing storage accounts and setting access policies, but it doesn't necessarily grant access to the data within the blobs.

B. Contributor: This role has a wide scope and provides full access to manage all Azure resources but does not grant specific data access permissions for storage blobs.

D. Reader and Data Access: This role allows read access to the storage account's data but does not include write or delete permissions. Therefore, the most appropriate role for the scenario is Storage Blob Data Contributor.

upvoted 1 times

🗨️ 👤 **applepie89** 11 months, 3 weeks ago

Selected Answer: C

Storage Account Contributor : Permits management of storage accounts. Provides access to the account key, which can be used to access data via Shared Key authorization.

Storage Blob Data Contributor : Read, write, and delete Azure Storage containers and blobs. To learn which actions are required for a given data operation

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-blob-data-contributor>

upvoted 3 times

🗨️ 👤 **3c5adce** 11 months, 4 weeks ago

Given that the requirement is to allow read, write, and delete operations for data stored in the containers of storage1, the correct role to assign is:

C. Storage Blob Data Contributor

This role specifically targets the data within the blob containers, providing the necessary permissions for read, write, and delete operations without extending unnecessary broader access to other aspects of the Azure environment.

upvoted 1 times

🗨️ 👤 **bobothewiseman** 1 year, 1 month ago

Selected Answer: C

Storage Blob Data Contributor

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-blob-data-contributor>

upvoted 4 times

🗨️ 👤 **nachito** 1 year, 1 month ago

Selected Answer: C

I think the key of the answer is in the question "read, write and delete operations FOR THE DATA stored in the containers"

So the mentioned operations are about the data.. and the Storage Account Contributor doesnt have permissions on the data, its permissions are about properties and metadata and not the data itself.

So the answer is C

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#storage-account-contributor>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#storage-blob-data-contributor>

upvoted 7 times


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

C is correct
upvoted 1 times

  **AAlmani** 1 year, 2 months ago

Selected Answer: C

The required data actions / operations: for the data stored in the containers of storage1. (not the whole storage account)
so, Storage Blob Data Contributor meet the goal
upvoted 4 times

  **tripleaholic** 1 year, 6 months ago

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-blob-data-contributor>
The "contributor" in option B is not specific too general .
"Reader and Data Access" in option D is not a role.
option A: Storage Account Contributor can't perform delete operation.
option C: Storage Blob Data Contributor role can also perform data action in storage account.
upvoted 3 times

  **binhdortmund** 1 year, 7 months ago

Correct answer is C due to delete-operation
upvoted 4 times

You have an Azure subscription named Subscription1 that contains virtual network named VNet1. VNet1 is in a resource group named RG1.

A user named User1 has the following roles for Subscription1:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- B. Assign User1 the Contributor role for VNet1.
- C. Assign User1 the Owner role for VNet1.
- D. Assign User1 the Network Contributor role for RG1.

Correct Answer: C

Community vote distribution

C (100%)

- ki01**

Highly Voted

1 year, 4 months ago

Selected Answer: C

i feel like i answered this question about 10 times today already. no wonder there are near 600 questions in this dump.... considering how much ET raised their prices over the past years one would expect some quality control

upvoted 21 times
- Alex2259ggf**

4 months, 1 week ago

it keeps popping up

upvoted 2 times
- shrsrm95**

Highly Voted

1 year, 8 months ago

Selected Answer: C

user access admin is beyond the scope for A, B, and D - so the answer must be C by logical deduction. open to hearing your thoughts though!

upvoted 8 times
- kavikumar**

Most Recent

1 month, 4 weeks ago

Selected Answer: C

When ever I see this question I'm very happy.One less of the count of 600

upvoted 2 times
- 58b2872**

4 months ago

Selected Answer: C

this is cheating, you repeated this question many times !!!!!!!

upvoted 1 times
- VitaliiKurishko**

5 months, 3 weeks ago

I like this question, 10 more times and I will love it)

upvoted 2 times
- kijoksip**

1 year, 1 month ago

Why this question is so often?

upvoted 4 times
- bgcarter**

1 year, 3 months ago

there would be a whole lot less questions in this cumbersome exam dump if we removed the many repetitions of this same question.

upvoted 4 times
- manasa_3011**

1 year, 6 months ago

Option C

This question is repeated many times
upvoted 4 times

  **samehpalass** 1 year, 8 months ago

c Owner or user access administrator to assign role to other users
upvoted 3 times

You have an Azure AD tenant that contains the groups shown in the following table.

Name	Type	Security
Group1	Security	Enabled
Group2	Mail-enabled security	Enabled
Group3	Microsoft 365	Enabled
Group4	Microsoft 365	Disabled

You purchase Azure Active Directory Premium P2 licenses.

To which groups can you assign a license?



- A. Group1 only
- B. Group1 and Group3 only
- C. Group3 and Group4 only
- D. Group1, Group2, and Group3 only
- E. Group1, Group2, Group3, and Group4


Correct Answer: B

Community vote distribution

B (51%)

D (47%)

  iamchoy

Highly Voted 

1 year, 7 months ago

Selected Answer: B

Azure AD licenses can be assigned to user accounts. When you want to assign licenses to a group, the intention is to assign those licenses to the members of the group.

You can assign licenses to Microsoft 365 groups and security groups, but not to mail-enabled security groups. Furthermore, the group should be security-enabled to get the licenses assigned.

From the given list:

Group1: Security group (Security Enabled) - You can assign licenses.

Group2: Mail-enabled security group (Security Enabled) - You cannot assign licenses to mail-enabled security groups.



Group3: Microsoft 365 group (Security Enabled) - You can assign licenses.

Group4: Microsoft 365 group (Security Disabled) - You cannot assign licenses to security-disabled groups.

The correct answer is:

B. Group1 and Group3 only.



upvoted 47 times

  Fryether1

8 months, 3 weeks ago

I just tried it in my tenant and I was able to assign a license to a mail enabled security group without issue. I think it's only distribution lists and non-security enabled groups that you can't.

upvoted 9 times

  cpaljchc4



2 months, 1 week ago

"If you have security groups, mail enabled groups, or Microsoft 365 groups, you can assign or unassign licenses for those groups on the Licenses page in the Microsoft 365 admin center. We refer to this as group-based licensing."




not sure if it was not able in the past, but i found this here.

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-group-licenses?view=o365-worldwide>

upvoted 3 times



  **2d153f5** 5 months, 3 weeks ago
That's it.
upvoted 2 times



  **LovelyGroovey** 1 year, 2 months ago
Thank you! Your explanation is so clear and I understand better now
upvoted 1 times



  **SivaPannier** Highly Voted  1 year, 8 months ago
Answer is B:
"The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE."



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




I could not find much information on the possibility of adding it to 'mail enabled' group.
upvoted 45 times

  **[Removed]** 1 year, 6 months ago
The link is here:<https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>
upvoted 2 times

  **[Removed]** 1 year, 6 months ago
in your comment link, it mentioned: "Mail-enabled security groups are used for granting access to resources such as SharePoint, and emailing notifications to those users."
upvoted 2 times



  **edurakhan** 11 months ago
mail-enabled security group is a security group too.
I have just created a mail-enabled security group and assigned several licenses... just test it, you will see
upvoted 7 times

  **Jedi_sg2000** 11 months, 3 weeks ago
u r rite!
upvoted 1 times

  **joejoe15152** Most Recent  13 hours, 35 minutes ago
Selected Answer: D
You can assign a license to a group only if:



The group is a Security or Microsoft 365 group
The group has Azure AD Security Enabled = Enabled

Mail-enabled security groups and security-enabled Microsoft 365 groups are supported
upvoted 1 times



  **kriChe27** 1 month, 1 week ago
Selected Answer: D
you can assign Azure Active Directory Premium P2 licenses to Group-2, which is a mail-enabled security group. Azure AD supports assigning licenses to both security groups and mail-enabled security groups1.


Here is the updated list of groups to which you can assign licenses:

Group-1: Security type group, Security Enabled
Group-2: Mail-Enabled Security type group, Security Enabled
Group-3: Microsoft 365 type group, Security Enabled
You cannot assign licenses to Group-4 because it is a Microsoft 365 type group with security disabled
upvoted 2 times

  **vrn1358** 1 month, 2 weeks ago
Selected Answer: D
Just read the first paragraph here:

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-group-licenses?view=o365-worldwide>
upvoted 2 times

  **1d6a499** 2 months, 1 week ago
Selected Answer: D
Mail enabled security group is also a security group.
upvoted 1 times

  **cpaljchc4** 2 months, 1 week ago
Selected Answer: D
Tested in Lab 21 Feb 2025,
mail-enabled security group is also under security group tab which can be assigned group based licensing.


I think what matters is just security enabled or disabled.
upvoted 1 times

  **Nathan12345** 2 months, 2 weeks ago

Selected Answer: B

As stated, the licenses can be assigned only to security groups and MS 365.

Mail-enabled are distributed so cannot be assigned.
upvoted 1 times

  **0703448** 2 months, 3 weeks ago

Selected Answer: B

The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE.
upvoted 2 times

  **Jay_D_Lincoln** 3 months ago

Selected Answer: B

License Assignment Requirements for Groups:

- ✔ Security Groups (Security enabled) – Supported
- ✔ Microsoft 365 Groups (Security enabled) – Supported
- ✘ Microsoft 365 Groups (Security disabled) – Not Supported
- ✘ Mail-Enabled Security Groups – Not Supported
- ✘ Distribution Lists – Not Supported

upvoted 1 times

  **mmp6428** 3 months, 2 weeks ago

Selected Answer: D

the ChatGPT's answer
upvoted 1 times

  **7Zayin** 3 months, 4 weeks ago

Selected Answer: D

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-group-licenses?view=o365-worldwide>
upvoted 1 times

  **Kong2408** 3 months, 4 weeks ago

Selected Answer: D

<https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing> , Licenses can be assigned to any security group in Microsoft Entra ID. Security groups can be synced from on-premises, by using Microsoft Entra Connect. You can also create security groups directly in Microsoft Entra ID (also called cloud-only groups), or automatically via the Microsoft Entra dynamic group feature. So i think "Mail-enabled security group" is one of the security group
upvoted 1 times



  **RajeshwaranM** 4 months, 1 week ago

Selected Answer: B

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-group-licenses?view=o365-worldwide>
upvoted 1 times

  **RajeshwaranM** 4 months, 1 week ago

Sorry I selected the answer wrongly Refer to the below Microsoft documentation, We can assign the license to a mail-enabled security group So the answer is : D
<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-group-licenses?view=o365-worldwide>
upvoted 1 times

  **Pisagid** 4 months, 1 week ago

Selected Answer: D

If you have security groups, mail enabled groups, or Microsoft 365 groups, you can assign or unassign licenses for those groups on the Licenses page in the Microsoft 365 admin center. We refer to this as group-based licensing.

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-group-licenses?view=o365-worldwide>
upvoted 3 times

  **minura** 4 months, 2 weeks ago

Selected Answer: B

Answer is B:
The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE.
upvoted 1 times

  **Armandez** 5 months ago

Selected Answer: D

Given this information, Group2 (Mail-Enabled Security) is eligible for license assignment. Therefore, the correct groups for license assignment are Group1, Group2, and Group3. This aligns with option D: "Group1, Group2, and Group3 only."

Key Takeaway:

When assigning licenses in Azure AD, ensure that the groups are security-enabled. This includes standard security groups, mail-enabled security groups, and Microsoft 365 groups with security enabled.

upvoted 3 times

HOTSPOT

-

You have an Azure AD tenant.

You need to create a Microsoft 365 group that contains only members of a marketing department in France.

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

(

device.managementType
device.organizationalUnit
user.department
user.usageLocation

-eq "Marketing")

and
or
typeof

(user.country

-and
-eq
-in
-match

"France")

Correct Answer:

(

device.managementType
device.organizationalUnit
user.department
user.usageLocation

-eq "Marketing")

and
or
typeof

(user.country

-and
-eq
-in
-match

"France")

AntaninaD Highly Voted 1 year, 8 months ago
(user.department -eq "Marketing") -and (user.country -eq "France")

parentheses could be used to determine order
<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#operator-precedence>
upvoted 34 times

Vokuhila Highly Voted 1 year, 8 months ago
(user.department -eq "Marketing") -and (user.country -eq "France")
upvoted 10 times

RanPo Most Recent 7 months, 4 weeks ago
It was in my exam at 29.8.24
upvoted 1 times

[Removed] 7 months, 4 weeks ago
CORRECT
upvoted 2 times

3c5adce 11 months, 4 weeks ago
(user.department -eq "Marketing") and (user.country -eq "France")
upvoted 1 times

1828b9d 1 year, 2 months ago
This question was in exam 01/03/2024
upvoted 2 times

bnicolas 1 year, 2 months ago
"-eq" AND "-match" would work.

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

Correct

upvoted 1 times

  **tfdestroy** 1 year, 4 months ago

(user.department -eq "Marketing") and (user.country -eq "France")



- user.department -eq "Marketing": This part checks if the user's department attribute in Azure AD is equal to "Marketing".

- and: This operator combines the two conditions.

- user.country -eq "France": This part checks if the user's country attribute in Azure AD is equal to "France".

Therefore, the rule will only add users to the group who meet both conditions: they must be in the "Marketing" department and have their country set to "France".

upvoted 2 times

  **river1999991** 1 year, 5 months ago

The given answer is correct.

upvoted 2 times

  **pinyonet** 1 year, 6 months ago

(user.department -eq "Marketing") -and (user.country -eq "France")

upvoted 2 times

  **rikinetysix** 1 year, 7 months ago

The given answer is correct.

upvoted 3 times

HOTSPOT

-

You have an Azure AD tenant.

You need to modify the Default user role permissions settings for the tenant. The solution must meet the following requirements:

- Standard users must be prevented from creating new service principals.
- Standard users must only be able to use PowerShell or Microsoft Graph to manage their own Azure resources.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

NOTE: Each correct answer is worth one point.

The screenshot shows the 'Default user role permissions' settings in the Azure AD portal. The settings are organized into sections: 'Default user role permissions', 'Guest user access', 'Administration portal', 'LinkedIn account connections', and 'Show keep user signed in'. The 'Default user role permissions' section includes three toggle switches: 'Users can register applications' (Yes), 'Restrict non-admin users from creating tenants' (No), and 'Users can create security groups' (Yes). The 'Guest user access' section includes a radio button selection for 'Guest user access restrictions', with 'Guest users have limited access to properties and memberships of directory objects' selected. The 'Administration portal' section includes a toggle switch for 'Restrict access to Azure AD administration portal' (No). The 'LinkedIn account connections' section includes a radio button selection for 'Allow users to connect their work or school account with LinkedIn', with 'Yes' selected. The 'Show keep user signed in' section includes a toggle switch for 'Show keep user signed in' (Yes).

Default user role permissions
Learn more ⓘ

Users can register applications ⓘ ☒ Yes

Restrict non-admin users from creating tenants ⓘ ☐ No

Users can create security groups ⓘ ☒ Yes

Guest user access
Learn more ⓘ

Guest user access restrictions ⓘ ☐ Guest users have the same access as members (most inclusive)
☒ Guest users have limited access to properties and memberships of directory objects
☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Administration portal
Learn more ⓘ

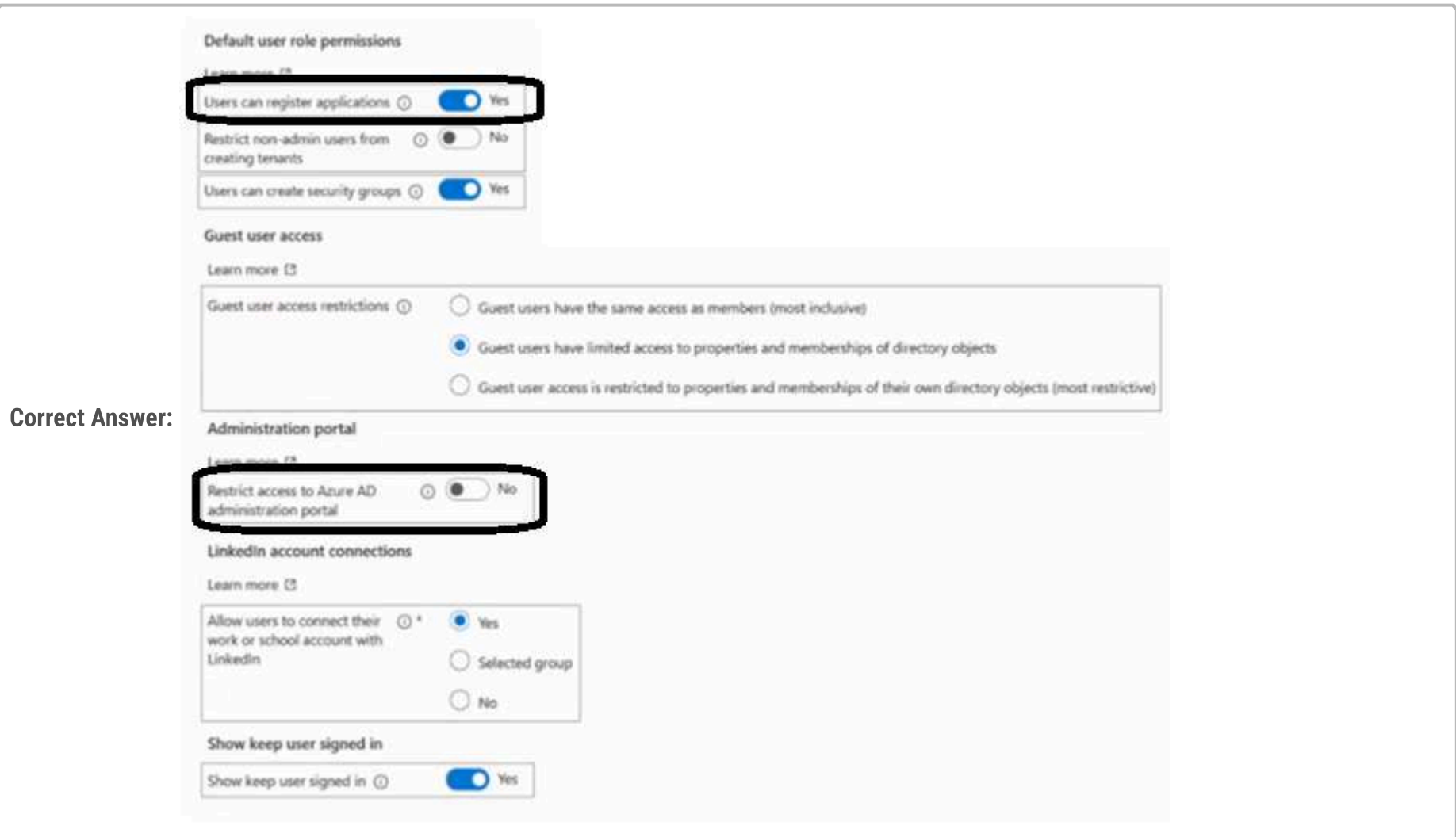
Restrict access to Azure AD administration portal ⓘ ☐ No

LinkedIn account connections
Learn more ⓘ

Allow users to connect their work or school account with LinkedIn ⓘ * ☒ Yes
☐ Selected group
☐ No

Show keep user signed in

Show keep user signed in ⓘ ☒ Yes



Correct Answer:

- AntaninaD

Highly Voted

1 year, 8 months ago

Register applications:
Setting this option to No prevents users from creating application registrations.

Restrict access to Azure AD administration portal:
What does this switch do?
No: lets non-administrators browse the Azure AD administration portal.
Yes: Restricts non-administrators from browsing the Azure AD administration portal. Non-administrators who are owners of groups or applications are unable to use the Azure portal to manage their owned resources.
What does it not do?
It doesn't restrict access to Azure AD data using PowerShell, Microsoft GraphAPI, or other clients such as Visual Studio.
It doesn't restrict access as long as a user is assigned a custom role (or any role).

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions>
upvoted 28 times
- Jay_D_Lincoln

3 months ago

What is your answer? It is not making sense

upvoted 2 times
- Z_MU

4 months ago

What about that option, should we disable "Users can create security groups"?
Is security groups considered as security principal?

upvoted 1 times
- josola

1 year, 6 months ago

Although I agree with your answer, the setting is already "Yes" in "Restrict access to Azure administration portal," meaning that there is no need to change that setting. It looks like that the question has it backwards.

upvoted 2 times
- MatAlves

1 year, 3 months ago

No, the "Restrict Access to Azure AD" is set to "No".

upvoted 6 times
- testtaker09

Highly Voted

10 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 5 times
- nicolase

Most Recent

1 month, 2 weeks ago

Desactivar "Users can register applications"

Activar "Restrict non-admin users from creating tenants"

upvoted 1 times
- [Removed]

7 months, 4 weeks ago

CORRECT

upvoted 2 times

  **RajeshwaranM** 4 months, 1 week ago

Restrict nonadmin users from creating tenants Is it a correct answer? I'm not sure about Could anyone put the answer with clear details? Answer
upvoted 1 times

  **cpaljchc4** 2 months, 1 week ago

From my understanding from the forum,

1. set the User can register applications: From Yes -> No
2. Set Restrict Access to Azure AD: From No -> Yes

But I didn't have Lab questions last time when I took in Dec 2024, so I didn't see this question.
upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago

Partially Correct - only adjust the "Users can register applications" to No to prevent the creation of new service principals. For managing resource access through PowerShell or Microsoft Graph, ensure that proper RBAC policies are in place. If there are specific settings related to PowerShell or Microsoft Graph access that can be toggled in your environment, these would typically be managed directly in the Azure subscription or resource management panels rather than Azure AD tenant settings.

upvoted 2 times

  **Amir1909** 1 year, 2 months ago

Correct
upvoted 1 times

  **river1999991** 1 year, 5 months ago

The given answer is correct.
upvoted 3 times

  **markb258** 1 year, 7 months ago



why isnt it to restrict user to their own directory objects?
upvoted 3 times

  **alsmk2** 9 months ago

Because the question is for STANDARD users, and that option refers to GUEST users.
upvoted 1 times

  **Cfernandes** 1 year, 7 months ago

Acho correto
upvoted 1 times

  **ajdann** 1 year, 8 months ago

I believe its correct
upvoted 1 times

HOTSPOT -

You have an Azure subscription named Sub1 that contains the blob containers shown in the following table.

Name	In storage account	Contains blob
cont1	storage1	blob1
cont2	storage2	blob2
cont3	storage3	blob3

Sub1 contains two users named User1 and User2. Both users are assigned the Reader role at the Sub1 scope.

You have a condition named Condition1 as shown in the following exhibit.

```
(
  (
    ! (ActionMatches { 'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read' })
  )
  OR
  (
    @Resource[Microsoft.Storage/storageAccounts/blobServices/containers:name] StringEquals 'cont1'
  )
)
```

You have a condition named Condition2 as shown in the following exhibit.

```
(
  (
    ! (ActionMatches { 'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write' })
  )
  OR
  (
    @Resource[Microsoft.Storage/storageAccounts/blobServices/blobs:path] StringLike '*2*'
  )
)
```

You assign roles to User1 and User2 as shown in the following table.

User	Role	Scope	Role assignment condition
User1	Storage Blob Data Reader	sub1	Condition1
User2	Storage Blob Data Owner	storage1	Condition2

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 read blob2.	<input type="radio"/>	<input type="radio"/>
User1 can read blob3.	<input type="radio"/>	<input type="radio"/>
User2 can read blob1.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
User1 can read blob2.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can read blob3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can read blob1.	<input checked="" type="radio"/>	<input type="radio"/>

- sugarbubbles

Highly Voted

1 year, 8 months ago

Answer is NNY

The conditions are difficult to read, but they mean (according to reference 1):

 - a. If the user performs a reading operation, then he may only read from "cont1"
 - b. If the user performs a writing operation, then he may only write to blobs like "*2"

Given that, then:

 - 1- User 1 can read Blob2 - No, because he is reading, then the condition a. applies, and he is not reading cont1
 - 2- User 1 can read Blob3 - No, because he is reading, then the condition a. applies, and he is not reading cont1
 - 3- User 2 can read blob 1 - Yes. He is not writing, so the condition b. does not apply. He has permissions granted by the role on the scope he is reading - Storage Blob Data Owner on storage1, which contains blob1

References:

 - 1. <https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-format>
 - 2. <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 151 times
- Stunomatic

6 months, 2 weeks ago

- 1- No because condition 1 applied on cont2
 - 2- user 1 can read blob3 because its exist in cont3 not cont1 therefore no condition applied only default condition which is read.
 - 3. Y

upvoted 1 times
- [Removed]

1 year, 7 months ago

ANSWER IS NNY

condition1 - read action cannot perform since it encloses a parenthesis and exclamation point which indicate not. It also include OR which if the resource name string is equal to "cont1" then it cannot read it, again because it all enclose to a !(condition).

so, USER1 CAN READ BLOB2? No. because it falls to a condition that it cannot not read.

USER1 CAN READ BLOB2? No. Again because it falls to a condition that it cannot not read.

USER2 CAN READ BLOB1? Yes. condition2 says that it cannot write or if it contains string like "2" (wild card search with * asterisk). it all surpasses all the condition into false.

note:

user1 has a reader role but it also has a condition1 which prevent it to read.

user2 is the owner so it has read and write permission, but it also has a condition2 which prevent it to write. but it can read.

upvoted 22 times
- Batiste2023

1 year, 6 months ago



Please consult the syntax reference on this topic: Exclamation marks just introduce the ACTION section of a condition - they do not imply a negation (although that's what I, too, first thought...).



To summarize the syntax: each condition includes




 - an ACTION part that determines which action is to be limited by the condition and
 - an EXPRESSION part that says under which circumstances the action is allowed (expression evaluates to TRUE) or not (evaluates to FALSE).



Source: <https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-format#simple-condition>

In the light of this, the correct answers are
N: the expression evaluates to FALSE
N: the expression evaluates to FALSE
Y: the action mentioned in the condition does not apply to what the question asks about.
upvoted 13 times

  **Aniruddha_dravyakar** 1 year, 7 months ago
I agree Joshua thanks
upvoted 2 times

  **QL112233** 1 year, 3 months ago
Human language, reader role cannot read unless it's blob one, writer role cannot write unless it's blob 2
upvoted 8 times



  **HoT77777** Highly Voted  1 year, 8 months ago
Based on the documentation is NNY
upvoted 28 times

  **Ycheqri** 1 year, 8 months ago
Totally agree with this answer.
Explanation:
In a nutshell the two conditions can be read as such:
- condition 1: user 1 can read only blobs from container cont1
- condition 2: user 2 can write only to blobs with path matching the pattern *2*.



user 1 has azure blob data reader but restricted to read only blobs in container .



user 2 has azure blob data owner and doesn't have any read restrictions (the condition is targeting write action). That means He can read all blobs from all containers in storage account.

Documetation:
<https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-format>
upvoted 9 times



  **Ycheqri** 1 year, 8 months ago
Forgot to mention the authorized read container for user 1.



user 1 has azure blob data reader but restricted to read only blobs in container Cont1.
upvoted 1 times



  **Aniruddha_dravyakar** 1 year, 7 months ago
There is OR condition
upvoted 6 times


  **Lapiduse** 1 year, 8 months ago
This is not an answer
upvoted 2 times

  **70ec7c1** Most Recent  1 month, 2 weeks ago
Answer is YYY:
upvoted 1 times


  **70ec7c1** 1 month, 2 weeks ago
User1 has Reader role and Condition1 applied at the subscription level. RBAC roles are additive. In other words, it is the union of all the roles. This means that even if we have restricted to only cont1 in the Storage Blob Data Reader Role, User1 still has the original Reader role provided. The read access to cont2 and cont3 are not restricted at the Reader role and per the additive rule, this role is not negated. Thus, User1 can read all containers and their blobs per the Reader role at the sub1. So User1 can read both blob2 in cont2 and blob3 in cont3. User2 has the Reader role at the sub1 scope and the Storage Blob Data Owner with condition at the storage1 scope. Once again, both roles are additive. So, User2 can read all containers, and now additional, can write to storage1 containers so long as the blob path is like "*2*"
upvoted 1 times

  **iamsks** 1 month, 3 weeks ago
N
N
Y
upvoted 1 times


  **krish_76** 2 months, 3 weeks ago
Answer is NNY
Tested in Azure environment
Condition 1 beats both option of reading any blob and cont1 - N
Condition 1 applies again - so user 1 cannot read blob 3 - N
Condition 2 applies for User - He can read blob1 as he is the owner of storage1 which has the blob inside - Y
upvoted 1 times

-  **Priyanshu_Ji** 4 months, 2 weeks ago


As per the conclusive evidences i am able to see here, i concluded, the answer should be NNY. Request @examtopics to either update the correct answer. or justify your answer please.

upvoted 2 times
-  **GreenTick** 5 months, 1 week ago


whoever create this question must be put in prison. this question is very simple to answer, but was made difficult by all the wordings, half baked table and scrambled facts.

upvoted 2 times
-  **sca88** 5 months, 3 weeks ago

Should be NNY

upvoted 1 times
-  **behradcld** 8 months ago

ChatGPT says NNN which I beleive based on explanation it provided


upvoted 1 times
-  **[Removed]** 8 months ago

WRONG

No

No

Yes

upvoted 2 times
-  **azmlan** 9 months, 1 week ago


Answer is NNY

The first part !(ActionMatches('Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read')) is checking if the action being performed is NOT the "read blob" action (Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read).


The OR means that if the first part evaluates to false (i.e. the action IS "read blob"), then it will evaluate the second part of the condition.

The second part @Resource[Microsoft.Storage/storageAccounts/blobServices/containers:name] StringEquals 'cont1' is checking if the name of the storage container is equal to "cont1".

So in plain language, this condition allows any action EXCEPT reading blobs, OR it allows reading blobs ONLY from a container named "cont1".


upvoted 2 times
-  **ximim58473** 10 months ago

The answer is NNY


upvoted 1 times
-  **OscarFRltz** 10 months, 1 week ago

Tested:


NNY

upvoted 1 times
-  **testtaker09** 10 months, 3 weeks ago

was in the exam today 17/06/2024


upvoted 1 times
-  **robsoneuclides** 11 months, 1 week ago

NNY the image is wrong

upvoted 2 times
-  **Miccc** 11 months, 2 weeks ago

Answer is NNN

The condition has OR check, not AND

upvoted 5 times
-  **3c5adce** 11 months, 4 weeks ago

Based on the documentation is NNY

upvoted 1 times

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

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-MgUser cmdlet for each user.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Community vote distribution

B (88%)

12%

- rajneeshverma2020

Highly Voted

1 year, 4 months ago

This question is repeated multiple times, can admin remove duplicates
upvoted 9 times
- Babustest

Highly Voted

1 year, 7 months ago

Selected Answer: B

'New-MgInvitation' is the command to add external users to the organization.
<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>
upvoted 7 times
- Kalaiarasu

Most Recent

7 months ago

New-MgInvitation cmdlet for inviting external users ..
upvoted 2 times
- [Removed]

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times
- ProfesorF

10 months ago

ive seen this question like 10 times wow
upvoted 1 times
- AlbertKwan

10 months, 3 weeks ago

Selected Answer: A

Voting for A to test if admin actually reads my comment here.
upvoted 2 times
- Cfernandes

1 year ago

Resposta é B
Este cmdlet é usado para convidar um novo usuário externo para o seu diretório.
referencia: <https://learn.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0>
upvoted 1 times
- Vestibal

1 year, 6 months ago

Selected Answer: B

Instead use the New-AzureADMSInvitation cmdlet which is used to invite a new external user to your directory.

Reference:
<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation>

New-MgUser —> <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/new-mguser?view=graph-powershell-1.0>
upvoted 4 times

  **bryant12138** 1 year, 6 months ago

Selected Answer: B

should do the invite cmdlet rather than the create one
upvoted 3 times

HOTSPOT -

You purchase a new Azure subscription.

You create an Azure Resource Manager (ARM) template named deploy.json as shown in the following exhibit.

```

1  {
2    "$schema":
3    "https://schema.management.azure.com/schemas/2019-04-
4    01/deploymentTemplate.json#",
5    "contentVersion": "1.0.0.0",
6    "parameters": {
7      "obj1": {
8        "type": "object",
9        "defaultValue": {
10          "propA": "one",
11          "propB": "two",
12          "propC": "three",
13          "propD": {
14            "propD-1": "sub",
15            "propD-2": "sub"
16          }
17        },
18      "part1": {
19        "type": "string",
20        "allowedValues": [
21          "centralus",
22          "eastus",
23          "westus" ],
24        "defaultValue": "eastus"
25      },
26      "variables": {
27        "var1": [
28          "westus",
29          "centraus",
30          "eastus"
31        ]
32      },
33      "resources": [
34        {
35          "type": "Microsoft.Resources/resrouceGroups",
36          "apiVersion": "2018-05-01",
37          "location": "eastus",
38          "name": "[concat('RGS', copyIndex())]",
39          "copy": {
40            "name": "copy",
41            "count": 2
42          }
43        },
44        {
45          "type": "Microsoft.Resources/resourceGroups",
46          "apiVersion": "2018-05-01",
47          "location": "[last(variables('var1'))]",
48          "name": "[concat('ResGrp', '8')]"
49        },
50        {
51          "type": "Microsoft.Resources/resourceGroups",
52          "apiVersion": "2018-05-01",
53          "location": "[parameters('part1')]",
54          "name": "[concat('RGroup', length(parameters('obj1')))]"
55        }
56      ],
57      "outputs": {}
58    }

```

You connect to the subscription and run the following command.

New-AzDeployment -Location westus -TemplateFile "deploy.json"

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
Three resource groups are created when you run the script.	<input type="radio"/>	<input type="radio"/>
A resource group named RGroup5 is created.	<input type="radio"/>	<input type="radio"/>
All the resource groups are created in the East US Azure region.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Three resource groups are created when you run the script.	<input type="radio"/>	<input checked="" type="radio"/>
	A resource group named RGroup5 is created.	<input type="radio"/>	<input checked="" type="radio"/>
	All the resource groups are created in the East US Azure region.	<input checked="" type="radio"/>	<input type="radio"/>

- trferreiraBR

Highly Voted

1 year, 7 months ago

NNY - I run the ARM template in a lab environment. Before go to the explanation, it's valid to say that there are some errors in the script format and I have to fix it to run successfully.

1- It's N, because it creates 4 Resource Groups and not 3 Resource Groups (RGS0, RGS1, RGroup4 and ResGrp8);
1.1: The Resource Group named with "[concat('RGS', copyIndex())]", creates RGS0 and RGS1;
1.2: The Resource Group named with "[concat('ResGrp', '8')]", creates ResGrp8;
1.3: The Resource Group named with "[concat('RGroup', length(parameters('obj1')))]", creates RGroup4 (As we can see, obj1 parameter has a length of 4 'propA', 'propB', 'propC' and 'propD');
2 - It's N, because it doesn't create a resourcer group named RGroup5;
3 - It's Y, because all resource groups were created in the East US Azure Region.

upvoted 96 times
- c75e123

4 months, 2 weeks ago

Correct: N N Y
For the first two answers see above.

The last answer:
In the first two resource groups objects, "eastus" is in parameter "location" definded.
For the last group, take a look into "par1" in the parameters, the default value is also "eastus."

upvoted 1 times
- Archangel0007

1 year, 6 months ago

for the third one u give the input parameter as westus so it has to be No right ?

upvoted 1 times
- trferreiraBR

1 year, 6 months ago

No. It's is different! When you specify the location with a template, the location tells Azure Resource Manager where to store the deployment data.

"For subscription level deployments, you must provide a location for the deployment. The location of the deployment is separate from the location of the resources you deploy. The deployment location specifies where to store deployment data. Management group and tenant deployments also require a location. For resource group deployments, the location of the resource group is used to store the deployment data."

References:
<https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azdeployment?view=azps-10.4.1#description>

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-to-subscription?tabs=azure-cli#deployment-location-and-name>

upvoted 17 times
- Highgate

8 months, 3 weeks ago



Excellent answer



upvoted 1 times
- fomedad



1 year, 6 months ago



Why The Resource Group named with "[concat('RGS', copyIndex())]", creates RGS0 and RGS1?



upvoted 4 times



  **ubiquituz** 1 year, 4 months ago
because of the "copy" and "count" property
copy...means the 1st created resource group should be duplicated
count...how manytimes should it be duplicated..."2" (twice)
and [concat('RGS', copyIndex())] means the name of the created RGs should be derived from joining (concat) the words (string) "RGS" with
the copyindex number of each created RG (ie 1st created RG...copyindex number "0", 2nd created RG copyindex number "1")....as we all know
counting in prog lang. often begin with 0, 1, 2 and not 1
upvoted 8 times



  **ubiquituz** 1 year, 4 months ago
count: how many instance of the RG should exist...sorry my english isnt too good
upvoted 2 times




  **pharsat** 1 year, 6 months ago
Count property
upvoted 4 times



  **nsss** 1 year, 5 months ago
If it doesn't run successfully because of the errors, shouldn't you just say no to all? You are not supposed to assume that the errors are fixed
when running it.
upvoted 3 times



  **ggogel** 1 year, 5 months ago
Just from looking at it, I can see at least one error, which is the reference of "par1", written as "part1".
upvoted 2 times




  **nuel_12** 1 year, 3 months ago
microsoft willfully put it like that because the is default value for location which is "EAST US" if a location is not specify or empty it will
default to that or wrong specification
upvoted 1 times

  **c5ad307** 1 year, 3 months ago
You can also assume that it is a transcription error. Just consider both possibilities when taking the exam and read carefully
upvoted 3 times



  **forkie** Highly Voted  1 year, 7 months ago
NNY,
1: No, to my count there will be 4 resources deployed
2: No, the length(parameters('obj1')) count will result in 4, as there are top-level properties.
3: Yes, the -location parameter given only effects what region the deployment would happen in, the resourcses location are defined by the
template, and in this case the first two get an explicit eastus, the second refers to the last item in the list which is eastus and the third gets the
default value of it which is again eastus
upvoted 8 times



  **neolisto** 1 year, 6 months ago
1: there is a typo mistake in 1-st RG but I still wondering, how did you get 4 resource groups?
upvoted 1 times



  **Indy429** 1 year, 4 months ago
There's 3 RGs in the template for East-US. Hence, if you create 1 RG for West-US, it would be the 4th RG
upvoted 1 times



  **[Removed]** Most Recent  8 months ago
WRONG

No
No
Yes
upvoted 2 times

  **AlbertKwan** 10 months, 3 weeks ago
NNN - because in Line 35, the text "resrouceGroup" is wrong.
upvoted 4 times

  **varinder82** 11 months, 3 weeks ago
Final Answer: 'Yes No No
upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago
ChatGPT4 says Yes No No
upvoted 1 times

  **semse27** 11 months, 1 week ago
mine says no no yes
upvoted 2 times

- 3c5adce** 11 months, 4 weeks ago

Went through comments - most popular answer is NNY
upvoted 2 times
- devilish84** 12 months ago

There is a mistake on line 17, it should be part (referred on line 53). If you try to deploy the file above it won't work. If you change line 53 part1 -> part. You will have the following results:

Name=RGroup4, Location=East US
Name=RGS1, Location=East US
Name=ResGrp8, Location=East US
Name=RGS0, Location=East US

Therefore:

Question Number 1: NO (Notify line number 41, RGS0 and RGS1 will be created). Plus 2 other resource.
Question Number 2: NO (obj1 contains only 4 parameters, propA-D)
Question Number 3: YES
upvoted 4 times
- mercerc1** 4 months, 3 weeks ago

I typed out this JSON by hand in VS code (which makes mistakes easier to see). There are numerous mistakes/typos in the code (3 or 4 I think). Once I fixed those, I ran the command as shown in the question. It created four resource groups all in 'East US'. The names are:
ResGrp8
RGroup4
RGS0
RGS1
Therefore the answer is indeed NNY like devilish84 said.
upvoted 1 times
- 5faef8c** 1 year ago

NNN as written because of syntax errors, it fails until all are fixed

Fixing:
"location": "[parameters('part1')]" to
"location": "[parameters('par1')]"
"type": "Microsoft.Resources/resrouceGroups" to
"type": "Microsoft.Resources/resourceGroups"

Yields:
No – It creates 4 – RGS0, RGS1, ResGrp8, RGroup4 (len of PropA-D)
No – See above
Yes – tested in Lab
upvoted 2 times
- foves65810** 1 year ago

NNY
N: Two copies + two groups (total 4)
N: RGS 0, RGS 1, ResGrp 8, RGroup 4
Y: Location eastus, last() takes last value from array so eastus, deaefaultvalue eastus
upvoted 1 times
- prshntdxt7** 1 year, 1 month ago

lot of confusion around these Yes-No questions. Folks who don't know the correct answer kindly refrain providing your inputs here. Neither the ChatGPT plethora of knowledge is needed here. please, don't add to confusion, this az-104 is the only exam on ET where i see people creating a mess.
upvoted 2 times
- bobothewiseman** 1 year, 1 month ago

Answer is NNN
1st box : 4 resource groups (RGS0, RGS1, RGroup4 and ResGrp8)
2nd box: RGS0, RGS1, RGroup4 and ResGrp8
3rd box: all resources groups were created in West US
the location specified in the deployment command acts as the target deployment location for the entire deployment process, and all resources defined within the ARM template will be deployed to that specified location, regardless of any location properties defined within the individual resource definitions in the template.

<https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azdeployment?view=azps-10.4.1#description>
<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-to-subscription?tabs=azure-cli#deployment-location-and-name>
upvoted 2 times
- nguyendh** 2 months, 1 week ago

Nice catch! I think your answer and explanation is correct.
upvoted 1 times
- Amir1909** 1 year, 1 month ago

No

No

Yes

upvoted 1 times

  **adilkhan** 1 year, 3 months ago

answer is N N Y

upvoted 2 times

  **SkyZeroZx** 1 year, 4 months ago

N : Because resource first has a copy property then create groups size is 4

N : Is obvious not exist RGroup 5 for the conditions

Y : All resource is create East accordint the ARM

upvoted 3 times



  **alonedave** 1 year, 5 months ago

YNY

There is a typo on the par1 reference to the 4th RGS, so only three RGs would be deployed.

The other three would be deployed on East US

upvoted 1 times

  **ggogel** 1 year, 5 months ago

With that typo, the template would not execute.

upvoted 1 times

  **Isumby10** 1 year, 5 months ago

bro stop killing the excitement of learning.. you are literally creating a whole discussion just for a TYPO?? ????????????????????

upvoted 3 times

  **AlbertKwan** 10 months, 3 weeks ago

Obviously you are wishful that the compiler/interpreter has intelligence to correct typos...

upvoted 1 times

  **esetyanto** 1 year, 6 months ago

N - spelling mistake on first resource group

N - RGroup4

N - spelling mistake on the param

upvoted 5 times

Your on-premises network contains a VPN gateway.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.



What should you configure?


- A. Azure AD Application Proxy
- B. private endpoints
- C. a network security group (NSG)
- D. Azure Peering Service

Correct Answer: B

Community vote distribution

B (100%)

 **Batiste2023**

Highly Voted 

 1 year, 6 months ago



Selected Answer: B

Correct, that's what private endpoints are for.

"A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network."

<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview>

upvoted 5 times

 **Batiste2023** 1 year, 6 months ago



Ok, the following question seems to complicate things a bit - same scenario, different solution...


Here is what MS says about the difference about private endpoints and service endpoints:
"What is the difference between Service Endpoints and Private Endpoints?
- Private Endpoints grant network access to specific resources behind a given service providing granular segmentation. Traffic can reach the service resource from on premises without using public endpoints.
- A Service Endpoint remains a publicly routable IP address. A Private Endpoint is a private IP in the address space of the virtual network where the private endpoint is configured."

<https://learn.microsoft.com/en-us/azure/private-link/private-link-faq#what-is-the-difference-between-service-endpoints-and-private-endpoints->

From what I read here, both service endpoints and private endpoints seem a viable solution to the requirements stated.

upvoted 3 times

 **RajeshwaranM**



Most Recent 

 4 months, 1 week ago

Selected Answer: B

Repeated question. Admin, kindly remove this question from being repeated.

upvoted 1 times



 **[Removed]** 6 months ago

Selected Answer: B

B is correct



from VM1 to storage1 = private endpoints
between VNet1 and VNet2 = peering



upvoted 2 times



 **[Removed]** 8 months ago



Selected Answer: B

B is corect
upvoted 1 times

  **Pdutz** 10 months ago
Correct, private endpoint
upvoted 1 times

  **testtaker09** 10 months, 3 weeks ago
was in the exam today 17/06/2024
upvoted 4 times

  **090200f** 11 months ago
private endpoint
upvoted 2 times

  **Navigator** 1 year, 3 months ago
B is perfect
upvoted 1 times

Your on-premises network contains a VPN gateway.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A. Azure AD Application Proxy
- B. service endpoints
- C. a network security group (NSG)
- D. Azure Firewall

Correct Answer: B

Community vote distribution

B (100%)

- Kenz30**

Highly Voted

4 months, 3 weeks ago

Selected Answer: B

keywords-
when you see backbone - remember endpoints
upvoted 10 times
- serbanvadi**

Most Recent

2 months, 1 week ago

Selected Answer: B

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>
upvoted 1 times
- Sickcnt**

8 months, 1 week ago

Hey, Cloud network engineer here.

Yes both Private endpoint + Service endpoint is good.

Difference between them is that private endpoint will have its own private IP in your VNET

Service Endpoint is still a public IP (towards for exapmle a Storage Account) But Microsoft would know to route it in its Microsoft Backbone network
upvoted 4 times
- ProfesorF**

10 months ago

sometimes it is prive endpoints
upvoted 1 times
- Josh219**

9 months ago

so both are correct ?
Private endpoints and Service endpoints?
upvoted 1 times
- asdfgqwer**

1 year, 2 months ago

500 and 400 repeated



upvoted 2 times

  **tfdestroy** 1 year, 4 months ago

Selected Answer: B

- A. Azure AD Application Proxy
- B. service endpoints
- C. a network security group (NSG)
- D. Azure Firewall

upvoted 1 times

  **Libny** 1 year, 4 months ago

No doubts here

upvoted 1 times

  **Batiste2023** 1 year, 6 months ago

Selected Answer: B

Correct.

"Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network."

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

upvoted 4 times

Your on-premises network contains a VPN gateway.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A. Azure Application Gateway
- B. service endpoints
- C. a network security group (NSG)
- D. Azure Peering Service

Correct Answer: B

Community vote distribution

B (100%)

- 01111010

Highly Voted

1 year, 5 months ago

Selected Answer: B

B. service endpoints - assures traffic goes over MS bon(er)
upvoted 6 times
- Ahkhan

Most Recent

1 year, 5 months ago

This question was on my exam today on 11/14/2023.
upvoted 2 times
- PERCY23

1 year, 5 months ago

And wat was your answer
upvoted 1 times
- lebeyic620

1 year, 1 month ago

And did you pass?
upvoted 1 times
- victorlie

9 months, 3 weeks ago

It seems not, cause he´s still here
upvoted 2 times
- gbemxods

8 months, 3 weeks ago

ACCOUNT IS A BOT
upvoted 2 times

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Type
MG1	Management group
RG1	Resource group
VM1	Virtual machine

You create a user named Admin1.

To what can you add Admin1 as a co-administrator?

- A. RG1
- B. MG1
- C. Sub1
- D. VM1

Correct Answer: C

Community vote distribution

C (100%)

- Gabsyfire**

Highly Voted

1 year, 6 months ago

The correct answer is: C. Sub1

You can add Admin1 as a co-administrator to the Sub1 subscription.

You cannot add Admin1 as a co-administrator to the RG1 resource group, MG1 management group, or VM1 virtual machine.

Co-administrators have full access to all resources in a subscription, including the ability to create, read, update, and delete resources.

To add Admin1 as a co-administrator to Sub1:

In the Azure portal, navigate to Sub1.
Click Access control (IAM).
Click Assign role.
Select the Co-Administrator role.
Select Admin1 in the Select drop-down list.
Click Assign.
Once the role has been assigned, Admin1 will have full access to all resources in Sub1.

Note: Co-administrators can only be assigned at the subscription scope. You cannot assign co-administrators to resource groups, management groups, or virtual machines.

upvoted 44 times
- Batiste2023**

Highly Voted

1 year, 6 months ago

Selected Answer: C

Answer is correct.

A new question about a legacy topic. Co-Administrators where a thing before Azure RBAC was introduced - and will be deprecated from Aug 31, 2024...

Co-administrators have full access to all resources in a subscription, including the ability to create, read, update, and delete resources.

upvoted 16 times
- 2d153f5**

Most Recent

5 months, 3 weeks ago

Co-admin is a role that no longer exists in Azure as of August 2024. This question is obsolete.

upvoted 3 times
- sukaysukay**

7 months, 3 weeks ago

As of August 31st 2024, classic Azure Role has retired, which includes retirement of co-administrator role.

upvoted 2 times
- [Removed]**

8 months ago

Selected Answer: C


C is corerct

upvoted 1 times

  **3c5adce** 11 months, 4 weeks ago



Sub1 (Subscription): This is the correct level to add Admin1 as a co-administrator. Adding a co-administrator at the subscription level allows that user to manage everything within the subscription.

upvoted 2 times

  **Amir1909** 1 year, 2 months ago

C is correct

upvoted 1 times

  **Wojer** 1 year, 3 months ago

from 15 February 2024 you will not be able to add new Co-Administrator

upvoted 3 times

  **Tilakarasu** 1 year, 3 months ago

When you try adding co-admin role to VM you get a notification saying " Co-admin can be added in Sub level"

upvoted 1 times

  **nchebbi** 1 year, 5 months ago

The correct answer is C: Sub1, however this is a leagacy question, Co-Administrator and Service Administrator roles are used with classic ressources: Classic resources and classic administrators will be retired on August 31, 2024. Remove unnecessary Co-Administrators and use Azure RBAC for fine-grained access control.

ref: <https://learn.microsoft.com/en-us/azure/role-based-access-control/classic-administrators>

upvoted 4 times

HOTSPOT -

You have a Microsoft Entra tenant that contains the groups shown in the following table.

Name	Type	Has an assigned license
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

The tenant contains the users shown in the following table.

Name	Member of	Has a direct assigned license
User1	None	Yes
User2	Group1	No
User3	Group4	Yes
User4	None	No

Which users and groups can you delete? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users:

▼

User4 only
User1 and User4 only
User2 and User4 only
User1, User2, User3, and User4

Groups:

▼

Group2 only
Group2 and Group3 only
Group2 and Group4 only
Group1, Group2, Group3, and Group4

Answer Area

Users:

	▼
User4 only	
User1 and User4 only	
User2 and User4 only	
User1, User2, User3, and User4	

Correct Answer:

Groups:

	▼
Group2 only	
Group2 and Group3 only	
Group2 and Group4 only	
Group1, Group2, Group3, and Group4	

  **techtest848** Highly Voted 1 year, 4 months ago

Tested and verified answers are

Users = User1, User2, User3, User4 (can delete all users whether a license is assigned directly or via inheritance from a group membership)

Groups = Group 2 and Group 4 (Groups with active license assignments cannot be deleted. You get an error)

upvoted 87 times

  **Bravo_Dravel** 3 months ago

Correct tested in the lab

All users can be deleted but deleting a group with assigned license getting the error "Customer ran into error with Failed to delete group.

Details: The group has an active license. So it cannot be deleted.."

upvoted 2 times

  **Z_MU** 4 months ago



How can you delete group4 if it has user3 with direct assigned license?

upvoted 2 times

  **kinamee** 2 months ago



the user3 will not be deleted even if you delete the group4

upvoted 1 times

  **Giovachia2016** 1 year, 3 months ago



Correct. Tested in Lab too.

upvoted 7 times

  **Alandt** 1 year, 4 months ago

Please be clear in your answer. What is your answer now?

upvoted 2 times

  **rodrod** 6 months, 1 week ago

He gave a very clear answer. It just can't be clearer... Read again

upvoted 4 times

  **SkyZeroZx** Highly Voted 1 year, 4 months ago

User : User 1, User2 , User 3 and User 4

(Explain : You can deleted all users with licence then what happend ? Only free the licence and storage en some part)

Group : Group 2 and Group 4 (Groups with active license assignments cannot be deleted. You get an error)

<https://techcommunity.microsoft.com/t5/microsoft-365-admin-center/reclaiming-licenses-from-deleted-users/m-p/116488>

upvoted 11 times

  **SysC** Most Recent 3 weeks, 4 days ago

Why was the answer from 'User1, User2, User2, and User4'? changed to 'User1 and User4'? Which answer is the right one?

upvoted 1 times

  **SysC** 3 weeks, 2 days ago

To make it clearer, what is the difference between this question and question 108? In question 108, User1, User2, User3, and User4 can be selected.

upvoted 1 times

  **LinuxLewis** 5 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced#deleting-a-group-with-an-assigned-license>Important

Licenses that a user inherits from a group can't be removed directly. Instead, you have to remove the user from the group from which they're



inheriting the license.



So I would also think:



Users 1 and 4
Groups 2 and 4
upvoted 3 times



  **[Removed]** 8 months ago
WRONG

Users: User1, User2, User3, and User4
Groups: Group 2 and Group 4 only
upvoted 3 times

  **3c5adce** 11 months, 3 weeks ago
Validated by ChatGPT4 :
Users = User1, User2, User3, User4 (can delete all users whether a license is assigned directly or via inheritance from a group membership)
Groups = Group 2 and Group 4
upvoted 2 times

  **bobothewiseman** 1 year, 1 month ago
User : User 1, User2 , User 3 and User 4 . you can delete all users
Group : Group 2 and Group 4
upvoted 1 times

  **bnicolas** 1 year, 2 months ago
We can delete all users and Group 2 and 4
upvoted 2 times

  **yukkki** 1 year, 4 months ago
these answers are correct.
upvoted 1 times

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location
VM1	Virtual machine	East US
storage1	Storage account	West US

You need to ensure that data transfers between storage1 and VM1 do NOT traverse the internet

What should you configure for storage1?

- A. data protection
- B. a private endpoint
- C. Public network access in the Firewalls and virtual networks settings
- D. a shared access signature (SAS)

Correct Answer: B

Community vote distribution

B (100%)

- Yumperboy**

Highly Voted

1 year, 4 months ago

Correct Answer: B

To ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network without going out to the public internet, you should use a private endpoint.

A private endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet. Any traffic between your virtual machine and the storage account will traverse over the VNet and stay on the Microsoft backbone network, without ever leaving it.

Link: <https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

upvoted 11 times
- RajeshwaranM**

Most Recent

4 months, 1 week ago

Selected Answer: B

Repeated questions, Admin kindly review and remove it

upvoted 1 times
- [Removed]**

8 months ago

Selected Answer: B

B is corerct

upvoted 1 times
- testtaker09**

10 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 3 times
- edurakhan**

11 months ago

Selected Answer: B

Definitely B

upvoted 1 times
- Pechu200**

1 year, 2 months ago

correct Amswer :B

upvoted 1 times
- Mysystemad**

1 year, 3 months ago

B it's ok

upvoted 1 times
- SkyZeroZx**

1 year, 4 months ago

Selected Answer: B

Correct Answer: B

To ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network without going out to the public internet, you should use a private endpoint.

A private endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet. Any traffic between your virtual machine and the storage account will traverse over the VNet and stay on the Microsoft backbone network, without ever leaving it.

Link: <https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

upvoted 4 times

HOTSPOT

-

You have a Microsoft Entra tenant that is linked to the subscriptions shown in the following table.

Name	Management group	Parent management group
Sub1	Tenant Root Group	<i>Not applicable</i>
Sub2	MG1	Tenant Root Group
Sub3	MG2	Tenant Root Group

You have the resource groups shown in the following table.

Name	Subscription	Description
RG1	Sub1	Contains a storage account named storage1
RG2	Sub2	Contains a web app named App1
RG3	Sub3	Contains a virtual machine named VM1

You assign roles to users as shown in the following table.

User	Role	Scope
User1	Contributor	MG2
User2	Storage Account Contributor	storage1
User3	User Access Administrator	Tenant Root Group



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 resize VM1.	<input type="radio"/>	<input type="radio"/>
User2 can create a new storage account in RG1.	<input type="radio"/>	<input type="radio"/>
User3 can assign User1 the Owner role for RG3.	<input type="radio"/>	<input type="radio"/>

Answer Area			
	Statements	Yes	No
Correct Answer:	User1 can resize VM1.	<input checked="" type="radio"/>	<input type="radio"/>
	User2 can create a new storage account in RG1.	<input type="radio"/>	<input checked="" type="radio"/>
	User3 can assign User1 the Owner role for RG3.	<input checked="" type="radio"/>	<input type="radio"/>



-   **alsmk2** Highly Voted 8 months, 2 weeks ago

YNY

1. User 1 is a contributor of MG2, which cointains sub 3 and VM1.

2. User 2 is a SA Cont on storage 1 only. Can only modify tht.

3. User 3 is a UA Admin at tenant group level. Can assign roles to anything below.



upvoted 32 times
-   **sabrinakloud** Highly Voted 6 months ago

YES: user 1 is contributor to the scope MG2, which is linked to sub3 and contains RG3 and VM1. contributor role can resize vm in its scope.

NO: User2 is storage account contributor to the storage1 scope only not RG1.

YES: User3 is user access admin to the scope tenant root group that contains all the subscriptions and therefore sub3 that contains RG3, so he can assign roles to any users and to user1

upvoted 10 times

  **2d153f5** 5 months, 2 weeks ago

Great!

upvoted 1 times

  **allinict_111** Most Recent 5 months, 1 week ago

No, User1 cannot resize vm1 based on their current role and scope.

User1 has the Contributor role, but their scope is limited to the Azure AD Tenant. Since vm1 is located in RG3, which is under Subscription3, User1 does

No, User2 cannot create a new storage account in RG1.

User2 has the Storage Account Contributor role with a scope limited to storage1. This means User2 can manage storage accounts within storage1, but does not have the permissions to create or manage storage accounts in other resource groups, including RG1.

Yes, User3 can assign User1 the Owner role for RG3.

User3 has the Access Administrator role with a scope of the Tenant Root Group, which generally includes the ability to manage access and permissions across the entire tenant, including all subscriptions and resource groups within it. This role allows User3 to assign roles to other users for specific resources like RG3.

upvoted 2 times

  **c4ecedc** 6 months ago

1. NO: User1 has the role of contributor for the MG2 level, VM1 is located in MG1

2. NO: User2 has the role of "Storage Account Contributor" only for the storage1 resource, therefore he will not be able to create a new storage account in the resource group

3. YES: User 3 has the role "User Access Administrator" in the root of the administration group, therefore he can give access to any user

upvoted 1 times

  **amircoka** 3 months, 1 week ago



User1 has contributor role for MG2, which contains Sub3. VM1 is located in RG3 which is also part of Sub3, so User1 has inherited Contributor role on VM1.

So it should be YES for first question.

2nd - No

3rd - Yes

upvoted 2 times

  **Sifon_n** 6 months, 1 week ago

Y, N, Y

upvoted 1 times

  **[Removed]** 8 months ago



CORRECT

upvoted 2 times

  **[Removed]** 7 months, 1 week ago

according to the scopes

upvoted 1 times

  **RanPo** 8 months, 1 week ago

agreed

upvoted 1 times

Your on-premises network contains a VPN gateway.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A. a network security group (NSG)
- B. private endpoints
- C. Microsoft Entra Application Proxy
- D. Azure Virtual WAN

Correct Answer: *B*

Community vote distribution

B (100%)

- webbrowser

7 months ago

The answer is B

upvoted 2 times
- behradclld

7 months, 4 weeks ago

Selected Answer: B

100% correct. I like this question :) Good luck with your exam!

upvoted 2 times
- [Removed]

8 months ago

Selected Answer: B

B is corerct

upvoted 1 times
- RanPo

8 months, 1 week ago

these kind of question seen all the times, might need to shrink them

upvoted 3 times

You have a Microsoft Entra tenant.

You plan to perform a bulk import of users.

You need to ensure that imported user objects are added automatically as the members of a specific group based on each user's department. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.


- A. Create groups that use the Assigned membership type.
- B. Create an Azure Resource Manager (ARM) template.
- C. Create groups that use the Dynamic User membership type.
- D. Write a PowerShell script that parses an import file.
- E. Create an XML file that contains user information and the appropriate attributes.
- F. Create a CSV file that contains user information and the appropriate attributes.

Correct Answer: CF

Community vote distribution


CF (80%)

DF (20%)

-  **ELearn** Highly Voted 8 months, 1 week ago


Solution Analysis:
Dynamic User Membership Type:

Azure AD offers dynamic group membership, which automatically adds users to groups based on attributes such as department, job title, etc. By using the Dynamic User membership type, you can create rules (e.g., department equals 'Sales') that automatically manage group membership. This minimizes ongoing administrative effort as users are automatically added/removed from groups based on attribute changes. This solution directly aligns with the requirement to minimize administrative effort and automatically handle group membership.
Importing User Information:

When performing a bulk import of users, you need a structured format to provide user details such as names, departments, etc. A CSV file is a common format for importing user data into Azure AD. Azure AD supports bulk importing users using a CSV file, which can include attributes necessary for dynamic membership rules (e.g., department).
upvoted 6 times
-  **ELearn** 8 months, 1 week ago


Detailed Steps:
Create Groups with Dynamic User Membership:
By setting up groups with dynamic membership rules based on the department attribute, you ensure users are automatically placed in the correct group upon import.
Create a CSV File for Bulk Import:
A CSV file containing user information, including the department attribute, will allow Azure AD to import users with the necessary data to match the dynamic membership rules.
Correct Actions:
C. Create groups that use the Dynamic User membership type.

This allows automatic group membership based on user attributes, reducing manual management.
F. Create a CSV file that contains user information and the appropriate attributes.

This facilitates the bulk import of users with necessary attributes (e.g., department) into Azure AD.
Conclusion:
Using Dynamic User membership for groups and a CSV file for importing users allows for automated and efficient user management in Azure AD, fulfilling the requirement of minimal administrative effort.
upvoted 4 times
-  **Ponpon3185** Most Recent 1 month, 4 weeks ago



Selected Answer: DF

Would say D & F cause with just a CSV file you cannot make a Bulk. Question don't speak about Azure portal, so a script is needed to my mind.
upvoted 1 times

 **Ponpon3185** 1 month, 4 weeks ago

Selected Answer: CF

To make a bulk import (question not speak about Azure portal), you need CSV File...and a PS Script
upvoted 1 times

  **Mark74** 4 months, 3 weeks ago

Selected Answer: CF

CF for me
upvoted 3 times

  **behradcld** 7 months, 4 weeks ago



Selected Answer: CF

I would say CDF but there is no third answer so the best choices are CF.
upvoted 3 times

  **[Removed]** 8 months ago



Selected Answer: CF

C & F are correct
upvoted 3 times

  **ELearn** 8 months, 1 week ago



Selected Answer: CF

vote: C&F
upvoted 4 times

  **siheom** 8 months, 1 week ago



Selected Answer: CF

vote CF
upvoted 2 times



  **michael1msc** 8 months, 1 week ago

Selected Answer: DF

As you don't have option to upload csv to Azure the only option is PowerShell + CSV.
upvoted 3 times

  **pasangawa** 8 months, 1 week ago

I have to disagree with this. you can upload the csv on the portal.
All users > Users > Bulk create....there's the upload there when you download the template
upvoted 1 times

  **6c05b3d** 8 months, 2 weeks ago

ChatGPT: Correct answer: CF.
C. Dynamic groups automatically include members based on specified attributes (like department) that are evaluated using rules. In this scenario, you would create dynamic user groups and define a membership rule based on the department attribute. This eliminates the need for manual assignment or scripting as users are automatically added to the appropriate group based on their department.
F. The bulk import of users in Microsoft Entra ID (formerly Azure AD) is typically done using a CSV file. The CSV file allows you to specify user attributes, including the department. Once the users are imported with the department attribute correctly populated, they will automatically be added to the relevant dynamic groups based on the membership rules you set.
upvoted 2 times

You have an Azure subscription that contains a storage account named storage1.

You need to ensure that the access keys for storage1 rotate automatically.



What should you configure?



- A. a backup vault
- B. redundancy for storage1
- C. lifecycle management for storage1
- D. an Azure key vault
- E. a Recovery Services vault



Correct Answer: D



Community vote distribution



D (100%)

-   **exa104az** Highly Voted 8 months, 2 weeks ago

D: Use Azure Key Vault for Key Management
Azure Key Vault is a service that helps manage secrets, keys, and certificates. You can store and manage your storage account keys securely in Key Vault and use its features to automate key rotation.
upvoted 17 times
-   **behradcd** Most Recent 7 months, 4 weeks ago

Selected Answer: D
simple as cake
upvoted 1 times
-   **[Removed]** 8 months ago

Selected Answer: D
D is corerct
upvoted 1 times
-   **6c05b3d** 8 months, 2 weeks ago

Selected Answer: D
D: To ensure that the access keys for your storage account rotate automatically, you should configure Azure Key Vault with Azure Storage account key rotation.
upvoted 3 times
-   **alsmk2** 8 months, 2 weeks ago

Selected Answer: D
Correct
upvoted 3 times

You have an Azure subscription that contains the Microsoft Entra identities shown in the following table.

Name	Type
User1	User
Group1	Security group
Group2	Microsoft 365 group

You need to enable self-service password reset (SSPR).



For which identities can you enable SSPR in the Azure portal?


- A. User1 only
- B. Group1 only
- C. User1 and Group1 only
- D. Group1 and Group2 only
- E. User1, Group1, and Group2

Correct Answer: D

Community vote distribution

D (47%)	C (33%)	8%	7%
---------	---------	----	----



  **hnk**

Highly Voted 

 7 months, 3 weeks ago



Selected Answer: D

The correct answer is D, you can not assign SSPR to individual users it has to be a group. It can be a Security Group or a M365 Group.
upvoted 20 times



  **Escaruncho** 1 month ago

I'd go with this one, and here's the reason why:
https://www.youtube.com/watch?v=L8s_ILoHfzU



Notice that when he adds an object for SSPR, it asks for "Select group". It seems you can also add an user this way but my guess is Microsoft "likes" the group options better.
In the end, it's just one more of those unfortunate questions.
upvoted 1 times

  **Jay_D_Lincoln** 3 months ago



What is your source?
upvoted 1 times

  **d72bae5** 5 months, 2 weeks ago



I agree, D is the answer. I tested and I agree with hnk
upvoted 2 times

  **pheztux** 6 months, 2 weeks ago



You can assign SSPR to individual users. Also, MS Entra let you assign SSPR to ANY type of Group but you can only select one Group, so it means the answer is E (You can assign SSPR to M365, Security Groups and users)
upvoted 3 times

  **feralberti** 6 months, 2 weeks ago



Hi, can you describe how to enable SSPR to individual users? i cannot find the way to do this without having to create a group with just one user?
upvoted 2 times

  **Sunth65** 5 months ago

<https://youtu.be/rA8TvhNcCvQ>
upvoted 1 times

  **Sunth65** 5 months ago

<https://youtu.be/Lu1VT13GvyE>
upvoted 1 times

  **cris_exam** 3 months ago

NO you cannot configure SSPR to individual users.

The links above btw, both show how you can ONLY enable SSPR for Groups or ALL Users, NOT individual user.

Correct Answer D.

upvoted 1 times

🗄️ 👤 **alsmk2** Highly Voted 👍 8 months, 2 weeks ago

Selected Answer: C

Correct.

It could be E also, but only if the 365 group was security enabled, and it doesn't mention that in the question.

upvoted 8 times

🗄️ 👤 **Josh219** 5 months ago

you have to stick to the information given in question and answer it.

Its Option C

upvoted 2 times

🗄️ 👤 **SabitaN** Most Recent 🕒 1 month ago

Selected Answer: C

In the Azure portal, you can enable Self-Service Password Reset (SSPR) for both individual users and security groups, but not for Microsoft 365 groups.

upvoted 1 times

🗄️ 👤 **932cb77** 1 month, 1 week ago

Selected Answer: E

The answer is E Yes you can assign SSPR to individual users via azure portal.

Go to the Azure Portal

Navigate to Azure Active Directory → Password reset

Under "Properties", set:

"Self service password reset enabled" = Selected

Under "Select users or groups", you can:

Select individual users (like user1@contoso.com)

Or select groups

upvoted 1 times

🗄️ 👤 **KennethYY** 1 month ago

can assign to all user but not individual users

upvoted 1 times

🗄️ 👤 **Jakub4444** 2 months ago

Selected Answer: B

Yes, Microsoft Entra's Self-Service Password Reset (SSPR) can be enabled for individual users and security groups, but not directly for Microsoft 365 groups.

Important Considerations:

Security Groups: SSPR can be enabled for security groups, applying the configuration to all members within those groups.

Microsoft 365 Groups: SSPR cannot be directly enabled for Microsoft 365 groups. To apply SSPR settings to users within a Microsoft 365 group, you would need to add those users to a security group and then enable SSPR for that security group.

Individual Users: While there's no direct method to enable SSPR for individual users without using groups, you can achieve this by creating a security group specifically for those users and enabling SSPR for that group.

https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr?utm_source=chatgpt.com

upvoted 2 times

🗄️ 👤 **serbanvadi** 2 months, 1 week ago

Selected Answer: D

When you're comfortable with the process and the time is right to communicate the requirements with a broader set of users, you can select a group of users to enable for SSPR. Or, you can enable SSPR for everyone in the Microsoft Entra tenant.

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#enable-self-service-password-reset>

upvoted 2 times

🗄️ 👤 **vrn1358** 3 months ago

Selected Answer: E

Entra ID has 3 options for SSPR,

1- none

2-Group

3- All

so we can set SSPR for users and groups

upvoted 1 times

🗄️ 👤 **cris_exam** 3 months ago

Selected Answer: D

Correct Answer D.

You can Enable SSPR for Groups (both Security and M365) OR ALL users, but not individual users.
upvoted 1 times

  **Bravo_Dravel** 3 months ago

Selected Answer: D



I checked this <https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/3-implement-azure-ad-self-service-password-reset> and found that to enable self-service password reset (SSPR) for a single user, you must specify a security group.

I tested it in the lab, and it also allows an M365 group to be selected for SSPR.
Correct Answer is Security Group or a M365 Group
upvoted 3 times

  **Mitko_V_Milkov** 3 months ago

Selected Answer: C

The key word here is "enable". You can assign SSPR only to individual user, who you then can put in a group. However, in Azure you can ENABLE either to selected users or users grouped in a security group. Therefore, for me the answer is C.
upvoted 1 times

  **ZK2000** 3 months, 4 weeks ago

Selected Answer: C



Imo this should be C, as the question states that the subscription only contains the listed user and groups.
The article bellow states that we can either enable SSPR for all users (which is only User1 in this case) or for a security group. M365 group is not mentioned.

<https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/3-implement-azure-ad-self-service-password-reset>
upvoted 1 times

  **SHAHIN_STA** 4 months ago

Selected Answer: C

You can assign SSPR to individual users and Security Groups, but Microsoft 365 Groups are not supported. Correct answer: C. User1 and Group1 only.
upvoted 2 times

  **58b2872** 4 months ago



Selected Answer: D

You cannot enable Self-Service Password Reset (SSPR) for an individual user; it must be done for a group. Currently, you can only enable one Microsoft Entra group for SSPR using the Microsoft Entra admin center.

References:

Tutorial: Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset Self-service password reset (SSPR) can only be enabled for security groups in Microsoft Entra ID. It cannot be enabled for Microsoft 365 groups. The self-service group management features do not apply to mail-enabled security groups or distribution lists.



References:
upvoted 1 times

  **58b2872** 4 months ago

You cannot enable Self-Service Password Reset (SSPR) for an individual user; it must be done for a group. Currently, you can only enable one Microsoft Entra group for SSPR using the Microsoft Entra admin center.

References:

Tutorial: Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset
upvoted 1 times

  **58b2872** 4 months ago

Selected Answer: C

To enable ****Self-Service Password Reset (SSPR)**** in Azure, the following conditions apply:

****Who can SSPR be enabled for?****

- **Individual Users (e.g., User1)**:**
 - SSPR can be enabled for specific users in Azure AD.
- **Security Groups (e.g., Group1)**:**
 - SSPR can be enabled for security groups, and all members of the group will inherit the SSPR policy.
- **Microsoft 365 Groups (e.g., Group2)**:**
 - SSPR ****cannot**** be enabled for Microsoft 365 groups. Azure AD does not support enabling SSPR for Microsoft 365 groups.



****Analysis of Options**:**

- **User1**: Eligible for SSPR.
- **Group1 (Security group)**: Eligible for SSPR.
- **Group2 (Microsoft 365 group)**: **Not eligible** for SSPR.

Correct Answer:

C. User1 and Group1 only.

upvoted 1 times

  **58b2872** 4 months ago

just to correct myself... it is wrong, the solution is D "You cannot enable Self-Service Password Reset (SSPR) for an individual user; it must be done for a group. Currently, you can only enable one Microsoft Entra group for SSPR using the Microsoft Entra admin center.

References:

Tutorial: Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset"

upvoted 3 times

  **MarthaMounir** 4 months ago

Selected Answer: C

User1: Individual user accounts can have Self-Service Password Reset (SSPR) enabled directly.

Group1: Security groups can be selected to enable SSPR for all their members.

Group2: Microsoft 365 groups are not supported for SSPR configuration.

upvoted 2 times

  **matthieudumont** 4 months, 1 week ago

Selected Answer: C

Vous pouvez activer SSPR pour User1 (utilisateur individuel).

Vous pouvez également activer SSPR pour un groupe de sécurité comme Group1.

Vous ne pouvez pas activer SSPR pour un groupe Microsoft 365 comme Group2.

upvoted 2 times

DRAG DROP -

You have a Microsoft Entra tenant.

You need to ensure that when a new Microsoft 365 group is created, the group name is automatically formatted as follows:

<Department><Group name>

Which three actions should you perform in sequence in the Microsoft Entra admin center? 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
Set Add suffix to Attribute .		
Create a group naming policy.		
Set Add prefix to Attribute .	>	
Set Add suffix to String .	<	
Set Add prefix to String .		
Set Select type to Department .		
Customize the company branding.		

	Answer Area
Correct Answer:	Create a group naming policy.
	Set Add prefix to Attribute .
	Set Select type to Department .

 **ELearn** Highly Voted 8 months, 1 week ago

To ensure that when a new Microsoft 365 group is created, the group name is automatically formatted as <Department><Group name>, you need to configure a group naming policy in Microsoft Entra (formerly Azure AD). This can be achieved by setting a prefix based on the department attribute.

- 1- Create a group naming policy: This is the first step to establish the framework for naming groups.
- 2- Set Add prefix to Attribute: This step specifies that the prefix will be an attribute rather than a static string.
- 3- Set Select type to Department: Finally, you specify that the 'Department' attribute will be used as the prefix.

upvoted 12 times

 **eduardovzermeno** Most Recent 7 months ago


<https://learn.microsoft.com/es-mx/entra/identity/users/groups-naming-policy>

upvoted 2 times

 **[Removed]** 8 months ago



CORRECT



upvoted 2 times



 **Jacky_1** 8 months, 2 weeks ago

Answer is correct. Tested it in my tenant.

upvoted 4 times

  **Shakka** 8 months, 2 weeks ago
Tested in Azure, Given Answer is correct
upvoted 1 times

  **Alawi1990** 8 months, 2 weeks ago
Create a group naming policy.
Set Add prefix to Attribute.
Set Add suffix to String.
upvoted 4 times

  **alsmk2** 8 months, 2 weeks ago
I think the last option should be Set Select type to Department.

I've not tested it, but that would seem most logical.
upvoted 5 times

HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Microsoft Entra ID P2
User2	Group2	None
User3	None	Microsoft Entra ID P2
User4	None	None

The tenant contains the groups shown in the following table.

Name	Member of	Assigned license
Group1	None	None
Group2	Group3	Microsoft Entra ID P2
Group3	Group4	None
Group4	None	Microsoft Entra ID P2

Which users and groups can be deleted? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users: ▼

- User4 only
- User3 and User4 only
- User2 and User4 only
- User1, User2, User3, and User4

Groups: ▼

- Group1 only
- Group4 only
- Group1 and Group3 only
- Group1, Group2, Group3, and Group4

Answer Area**Correct Answer:**

Users: ▼

- User4 only
- User3 and User4 only
- User2 and User4 only
- User1, User2, User3, and User4**

Groups: ▼

- Group1 only
- Group4 only
- Group1 and Group3 only**
- Group1, Group2, Group3, and Group4

 **ELearn** Highly Voted 8 months, 2 weeks ago

the given answers are correct:

1st box: you can delete all users (user1,2,3&4) whether a license is assigned directly or via inheritance from a group membership

2nd box: Groups with active license assignments cannot be deleted. so only group 1 & 3 can be deleted
upvoted 20 times

 **jairoaquinterov** 2 months, 3 weeks ago

Group 2 is member of Group 3, and this group have active license assignments, then group 3 can not delete.
upvoted 1 times

  **Elsayed2030** 4 months, 2 weeks ago

You can delete all the users - licensed or not
You can only delete Group 1. Ideally you could delete Group 3 too but Group 2 is a member of Group 3 and Group 2 cannot be deleted as it is licensed. Group 4 cannot be deleted as it is licensed.
upvoted 2 times

  **Jay_D_Lincoln** 3 months ago

nested grouping is not supported in entra id when it comes to licensing. so you can delete group3Licenses are assigned at the tenant or user level, not at the group level – While Group4 has a license assigned, it does not mean that Group3 is bound to it in a way that would prevent deletion.
Nested group membership does not prevent deletion – Even though Group3 is a member of Group4, this does not restrict its deletion unless it has specific administrative restrictions applied.
upvoted 1 times

  **Armandez** 5 months ago

Discrepancy in the Answer:
The inclusion of User1 and User3 as deletable users in the given answer directly contradicts the standard rules for users with assigned licenses.
The inclusion of Group1 and Group3 aligns with the analysis, so that part is correct
upvoted 2 times

  **IPERSONIC** Highly Voted  6 months ago

Users:

User1 and User3 have the Microsoft Entra ID P2 license.
User2 and User4 have no license.
Only users without a license (User2 and User4) can be deleted directly without removing a license first.

Groups:

Group1 has no license and no membership dependencies.
Group2 has a Microsoft Entra ID P2 license and is a member of Group3.
Group3 has no license but is a member of Group4.
Group4 has a Microsoft Entra ID P2 license.
Based on Microsoft Entra guidelines, only Group1 can be deleted, as it has no license or membership dependencies.

Correct Answer

Users: User2 and User4 only

Groups: Group1 only

This aligns with Microsoft's current guidelines on license and membership requirements for deletion
upvoted 9 times

  **gt1405** Most Recent  8 months ago

Box1 : User1, User2, User3, and User4

Box2 : Group1 only

upvoted 7 times

  **gt1405** 8 months ago

Box1 : User1, User2, User3, and User4

Box2 : Group1 and Group3 only

upvoted 4 times

  **[Removed]** 8 months ago

CORRECT

upvoted 3 times

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Resource group	Type	Location
app1	RG1	Container app	East US
Vault1	RG1	Azure Key Vault	East US
Vault2	RG1	Azure Key Vault	West US
Vault3	RG2	Azure Key Vault	East US

You plan to use an Azure key vault to provide a secret to app1.

What should you create for app1 to access the key vault, and from which key vault can the secret be used? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create a:

▼

Managed identity
Private endpoint
Service principal
User account

Use the secret from:

▼

Vault1 only
Vault1 and Vault2 only
Vault1 and Vault3 only
Vault1, Vault2, or Vault3

Answer Area

Correct Answer:

Create a:

▼

Managed identity
Private endpoint
Service principal
User account

Use the secret from:

▼

Vault1 only
Vault1 and Vault2 only
Vault1 and Vault3 only
Vault1, Vault2, or Vault3

[Removed]

Highly Voted

 8 months ago
WRONG

Create a: Managed Identity
Use the secret from: Vault1, Vault2, or Vault3
upvoted 25 times

happpieee 6 months ago
Secret can be assessed from cross region vault e.g. during failover
Source: <https://learn.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>
upvoted 1 times

Chuong0810

Highly Voted



 5 months, 4 weeks ago
You can use a Key Vault in a different resource group and region to provide secrets to your web application in a different resource group and region. Azure allows cross-resource group and cross-region access to Key Vaults, as long as you have the necessary access policies configured. And the answers:
Create a: Managed Identity
Use the secret from: Vault1, Vault2, or Vault3
upvoted 8 times



Stunomatic



Most Recent



 6 months, 2 weeks ago



Box 1: Correct, Managed Identity.
Box 2: The best for microsoft recommendations is vault1, vault3.
I think its about best practices ?
upvoted 2 times



  **rodrod** 6 months, 1 week ago
those test are NEVER about best practices (except if explicitly stated). it's always about what you CAN do. keep that in mind or you will fail your exam
upvoted 7 times



  **0378d43** 6 months, 3 weeks ago
Managed Identity and VAULT1 and 3 due to the location of the APP.
upvoted 2 times

  **akinz** 6 months, 3 weeks ago
my vault is in westus and my web application is in canadacentral, can my application use the key vault in westus to retrieve secret
Copilot said:
A web application in Canadacentral can use an Azure Key Vault in West US to retrieve secrets. Azure Key Vault is designed to be accessible from any region, allowing applications to securely retrieve secrets regardless of their geographic location.
upvoted 1 times

  **69b9d7c** 8 months, 1 week ago
Box 1: Correct, Managed Identity.
Box 2: The best for microsoft recommendations is vault1, vault3.
Unfortunately the question is confusing, but I will opt for what Microsoft recommends.
<https://learn.microsoft.com/en-us/azure/key-vault/general/best-practices>
upvoted 5 times



  **58b2872** 4 months ago
Vault1 and vault3 are correct... reducing latency
upvoted 1 times



  **pasangawa** 8 months, 1 week ago
for box 2, i'll vote for vault 1, 2 and 3.
though not best practice, i believe key vault can be access on resource group and region pair as long as configured properly.
upvoted 2 times

  **ELearn** 8 months, 1 week ago
regarding the key vault aspect(2nd answer) , What do they mean here?
what are the possibilities/options or which one is thew best option. we need to know instead of assuming ,in order for us to respond properly.

1st box: Managed Identity By creating a managed identity for app1, you can assign the necessary permissions to access the secrets in each key vault. The managed identity can be given access to multiple key vaults, regardless of their location or resource group.

2nd box: Confusing. we need to know what they mean here (either the best option , or all the possibilites/options)
upvoted 3 times



  **Dankho** 7 months ago
agreed, the question doesn't specify so I think all 3 vaults are possible.
upvoted 2 times



  **ELearn** 8 months, 1 week ago
Azure Key Vault allows secrets to be accessed from different regions and resource groups, provided that the necessary permissions are set up correctly. This means that app1 can access secrets from Vault1, Vault2, and Vault3, as long as it has the required access permissions to those key vaults.

Best Option: Vault1 — due to the same region and resource group, offering the best balance of performance and management simplicity.



Second Best: Vault3 — good for low latency but might need more attention for permissions and management due to being in a different resource group.

Third Option: Vault2 — feasible but not optimal due to being in a different region, which could lead to latency and additional costs.
upvoted 4 times

  **majejim435** 8 months, 2 weeks ago
*Correction: Vault2 is in different region
upvoted 2 times

  **majejim435** 8 months, 2 weeks ago
Managed Identity
Vault1, Vault2, or Vault3.

Vault3 is in a different region and therefore latency and costs is increased. However, it can be used without deploying an additional resources.
upvoted 3 times

  **majejim435** 8 months, 2 weeks ago
*Correction: Vault2 is in different region

upvoted 1 times

  **6c05b3d** 8 months, 2 weeks ago

Managed Identity and Vault1.

Managed Identity is often preferred for Azure resources like apps because it simplifies authentication and eliminates the need to manage credentials. It provides a secure way for the application to authenticate to Azure services.



Vault 1: app1 is located in the same resource group (RG1) and region (East US) as Vault1, so it should use the secret from Vault1 for best performance and accessibility.

upvoted 1 times

  **HardeWerker433** 8 months, 2 weeks ago

is this brokekey?

upvoted 1 times

  **Jacky_1** 8 months, 2 weeks ago

Managed id is right <https://learn.microsoft.com/en-us/azure/container-apps/manage-secrets?tabs=azure-portal#reference-secret-from-key-vault>

But I think it should be vault 1, 2 and 3. I cannot find anything about restrictions on resource group, or region. Another region can give some latency.

upvoted 2 times

You have a Microsoft Entra tenant named contoso.com.

You collaborate with an external partner named fabrikam.com.

You plan to invite users in fabrikam.com to the contoso.com tenant.

You need to ensure that invitations can be sent only to fabrikam.com users.

What should you do in the Microsoft Entra admin center?

- A. From Cross-tenant access settings, configure the Tenant restrictions settings.
- B. From Cross-tenant access settings, configure the Microsoft cloud settings.
- C. From External collaboration settings, configure the Guest user access restrictions settings.
- D. From External collaboration settings, configure the Collaboration restrictions settings.

Correct Answer: D

Community vote distribution

D (100%)

  **KAM2023** Highly Voted 8 months, 2 weeks ago

Selected Answer: D

Collaboration restrictions settings in Microsoft Entra (formerly Azure AD) are specifically designed to control which external domains can be invited as guests.

upvoted 12 times

  **Shakka** Highly Voted 8 months, 2 weeks ago

Correct

Sign in to the Microsoft Entra admin center:
Ensure you have the External Identity Provider Administrator role.
Navigate to External Collaboration Settings:
Go to Identity > External Identities > External collaboration settings.
Set Up an Allowlist:
Under Collaboration restrictions, select Allow invitations only to the specified domains (most restrictive).

upvoted 8 times

  **adilkhan** Most Recent 3 months, 3 weeks ago

Selected Answer: D

keywords to remember collaborate , external
upvoted 2 times

  **chrillelundmark** 4 months, 2 weeks ago

Selected Answer: D

<https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure>
upvoted 1 times

  **minura** 5 months ago

Selected Answer: D

The correct answer is D. From External collaboration settings, configure the Collaboration restrictions settings.

Why others are wrong

A. From Cross-tenant access settings, configure the Tenant restrictions settings
Tenant restrictions are not used to control guest user invitations. Instead, they manage access to resources between tenants, such as accessing applications or services in another tenant.

B. From Cross-tenant access settings, configure the Microsoft cloud settings
Microsoft cloud settings in Cross-tenant access are used for configuring collaboration across Microsoft clouds, like Azure Government or Microsoft 365 Global. It does not restrict guest invitations to specific domains.

C. From External collaboration settings, configure the Guest user access restrictions settings
Guest user access restrictions settings manage what external guest users can access after they are invited (e.g., whether they can see the tenant directory or access groups). They do not restrict who can be invited.
upvoted 2 times

  **[Removed]** 8 months ago

Selected Answer: D

D is corerct
upvoted 1 times

  **DJHASH786** 8 months, 2 weeks ago

D is correct answer.
upvoted 1 times

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains blob data.

You need to assign a role to a user named User1 to ensure that the user can access the blob data in storage1. The role assignment must support conditions.

Which two roles can you assign to User1? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Owner
- B. Storage Account Contributor
- C. Storage Account Backup Contributor
- D. Storage Blob Data Contributor
- E. Storage Blob Data Owner
- F. Storage Blob Delegator

Correct Answer: DE

Community vote distribution

DE (93%)

7%

alsmk2

Highly Voted

8 months, 2 weeks ago

Selected Answer: DE

Incorrect. Answer should be DE.
upvoted 10 times

Shakka

8 months, 2 weeks ago

Correct

Storage Blob Data Contributor: Grants read, write, and delete access to blob data.
Storage Blob Data Owner: Grants full access to blob data, including the ability to manage access permissions
upvoted 5 times

chrillelundmark

Most Recent

4 months, 2 weeks ago

Selected Answer: DE

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage>
upvoted 1 times

[Removed]

8 months ago

Selected Answer: DE

WRONG

D & E are correct
upvoted 1 times

6c05b3d

8 months, 2 weeks ago

Selected Answer: DE

Correct Answers:
D. Storage Blob Data Contributor
• Reason: This role allows the user to read, write, and delete blob data. It supports conditions, which means you can use Azure Role-Based Access Control (RBAC) to set conditions on the role assignment if necessary.
E. Storage Blob Data Owner
• Reason: This role allows the user to manage blob data including reading, writing, and deleting, and also managing the blob container and data. It supports conditions, making it possible to apply RBAC conditions on the role assignment.
upvoted 2 times

arunydav09

8 months, 2 weeks ago

Selected Answer: BD

Storage Account Contributor Role permits management of storage accounts. It provides access to the account key, which can be used to access data via Shared Key authorization.
Storage Blob Data Contributor Role permits Read, write, and delete Azure Storage containers and blobs.
upvoted 1 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 -

ADatum Corporation is consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Existing Environment -

Azure Environment -

ADatum has an Azure subscription that contains three resource groups named RG1, RG2, and RG3.

The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace1	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

Azure Key Vault -

The subscription contains an Azure key vault named Vault1.

Vault1 contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS#12	RSA	2048
Cert2	PKCS#12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vault1 contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment -

ADatum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

Name	Microsoft Entra role	Azure role
Admin1	Global Administrator	None
Admin2	Attribute Definition Administrator	None
Admin3	Attribute Assignment Administrator	None
User1	None	Reader for RG2 and RG3

The tenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes -

ADatum plans to implement the following changes:

- Configure a data collection rule (DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.
- In storage1, create a new container named cont2 that has the following access policies: o Three stored access policies named Stored1, Stored2, and Stored3 o A legal hold for immutable blob storage
- Whenever possible, use directories to organize storage account content.
- Grant User1 the permissions required to link Zone1 to VNet1.
- Assign Attribute1 to supported adatum.com resources.
- In storage2, create an encryption scope named Scope1.
- Deploy new containers by using Image1 or Image2.

Technical Requirements -

ADatum must meet the following technical requirements:

- Use TLS for WebApp1.
- Follow the principle of least privilege.
- Grant permissions at the required scope only.
- Ensure that Scope1 is used to encrypt storage services.
- Use Azure Backup to back up cont1 and share1 as frequently as possible.
- Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You need to implement the planned change for Attribute1.

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
Admin1 can assign Attribute1 to Group1.	<input type="radio"/>	<input type="radio"/>
Admin2 can assign Attribute1 to User1.	<input type="radio"/>	<input type="radio"/>
Admin3 can assign Attribute1 to Group2.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Admin1 can assign Attribute1 to Group1.	<input type="radio"/>	<input checked="" type="radio"/>
	Admin2 can assign Attribute1 to User1.	<input type="radio"/>	<input checked="" type="radio"/>
	Admin3 can assign Attribute1 to Group2.	<input type="radio"/>	<input checked="" type="radio"/>

- pasangawa**

Highly Voted

8 months ago

tried to test on lab and
box1. no.
box 2. no. need Attribute assignment Administrator to assign. admin2 is just Attribute definition Administrator
box 3 - No. Not sure if im doing it right but i can't find way to assign to a group, so it's a no unless someone points me to the right direction. if
M365 group assigned user, it works if assigning to user and not the group.
upvoted 7 times
- knarik**

1 month, 1 week ago

No No Yes

Users with Attribute Assignment Administrator role can assign and remove custom security attribute keys and values for supported Microsoft
Entra objects such as users, service principals, and devices
By default, Global Administrator and other administrator roles do not have permissions to read, define, or assign custom security attributes.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#attribute-assignment-administrator>
upvoted 1 times
- knarik**

1 month, 1 week ago

okay sorry nevermind, omitted the word Group
its NO NO NO
upvoted 1 times
- Adx_YT**

6 months, 1 week ago

No3:
You can add custom security attributes for the following Microsoft Entra objects:

Microsoft Entra users

Microsoft Entra enterprise applications (service principals)

<https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-overview#objects-that-support-custom-security-attributes>
upvoted 1 times

  **careTaker** Highly Voted 3 months ago

Box 1: No
Reference: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#attribute-assignment-administrator>
(read the note)

Box 2: No
Reference: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#attribute-definition-administrator>
(definition admin can not assign roles)

Box 3: No
Reference: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#attribute-assignment-administrator>
(Read the Actions column in that link table; It has only users and servicePrincipals; not groups)
upvoted 7 times

  **dilopezat** Most Recent 5 months, 1 week ago

NNN
Objects that support custom security attributes
You can add custom security attributes for the following Microsoft Entra objects:

- Microsoft Entra users
- Microsoft Entra enterprise applications (service principals)


https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-overview?wt.mc_id=knwlserapi_inproduct_azportal#what-are-custom-security-attributes-in-microsoft-entra-id

References:
https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-manage?wt.mc_id=knwlserapi_inproduct_azportal&tabs=admin-center#manage-access-to-custom-security-attributes-in-microsoft-entra-id
upvoted 2 times

  **sca88** 5 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-manage?tabs=admin-center>

So Attribute Definition can edit or add attribute for user and application, but CAN'T assign attribute to user and application. Assignment Admin, instead CAN assign Attribute to user and application. So answer should be correct: NNY
upvoted 4 times

  **swk1_az104** 3 months, 3 weeks ago



Based on the roles assigned to each administrator and the permissions required to manage custom security attributes in Microsoft Entra, here are my answers:

Admin1 (Global Admin) can assign Attribute1 to Group1: No


Global Administrators do not have permissions to read, define, or assign custom security attributes by default1.
Admin2 (Attribute Definition Admin) can assign Attribute1 to User1: No

The Attribute Definition Admin role can define and manage attribute definitions but cannot assign attributes to users or groups1.
Admin3 (Attribute Assignment Admin) can assign Attribute1 to Group2: Yes

The Attribute Assignment Admin role can assign custom security attributes to users and groups
upvoted 3 times

  **kam1122** 5 months, 2 weeks ago

Correct, only Attribute Assignment Admin able to assign
upvoted 1 times

  **sca88** 5 months, 3 weeks ago

Exam topic should not allow comments without documentation link...
upvoted 1 times


  **155e6a0** 7 months, 2 weeks ago

NNN is correct. Attribute Assignment Administrator CANNOT assign a custom security attribute to a M365 group. ChatGPT is wrong.
upvoted 2 times

  **[Removed]** 8 months ago

WRONG

No
No
No
upvoted 2 times

  **kjujuai** 8 months, 2 weeks ago

1. Global Admin does not have permission to assign Attribute
a. Note: Prerequisites
Manage custom security attributes for an application - Microsoft Entra ID | Microsoft Learn
2. Attribute Definition Assignment does not have permission to assign Attribute
a. Note: Prerequisites
Manage custom security attributes for an application - Microsoft Entra ID | Microsoft Learn
3. Microsoft 365 Group cannot be assigned an Attribute
a. Note: Objects that support custom security attributes
What are custom security attributes in Microsoft Entra ID? - Microsoft Entra | Microsoft Learn
upvoted 4 times

🗨️ 👤 **un4exa** 8 months, 1 week ago
NNN - <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#attribute-assignment-administrator> - only Microsoft entra objects users and sec principal or apps are eligible for Attributes and only Attribute Assignment Admin can assign for 2nd question definition Admin cannot assign but users are eligible for assignment
upvoted 1 times

🗨️ 👤 **kjujuai** 8 months, 2 weeks ago
1,2. <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/custom-security-attributes-apps?pivots=portal>
3. <https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-overview>
upvoted 2 times

🗨️ 👤 **arunyadav09** 8 months, 2 weeks ago
<https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-manage?tabs=admin-center>
<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

In Microsoft Entra ID, the Attribute Assignment Administrator role is needed to assign custom security attribute values to objects like users and applications, while the Global Administrator role does not have this permission by default.
Global Administrators can assign Attribute Assignment Administrator roles to themselves if needed.

Attribute Definition Administrator define and manage the definition of custom security attributes but it can not assign custom security attribute values to objects like users and groups & applications etc.

Hence NNY is right answer.
upvoted 2 times

🗨️ 👤 **DJHASH786** 8 months, 2 weeks ago
Shouldn't First option be Yes, since Admin 1 is global admin ?
upvoted 1 times

🗨️ 👤 **itismadu** 7 months ago
First time i see Global Admin does not have the ultimate rights . Microsoft must be

Attribute Assignment Administrator - <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#attribute-assignment-administrator>

By default, Global Administrator and other administrator roles do not have permissions to read, define, or assign custom security attributes. To work with custom security attributes, you must be assigned one of the custom security attribute roles.
upvoted 1 times

🗨️ 👤 **alsmk2** 8 months, 2 weeks ago
NYN

I'm not 100% on this, so do double check, but custom security attributes can only be assigned direct to users and service principals. I don't think you can assign them to a group.
upvoted 2 times

You have a Microsoft Entra tenant configured as shown in the following exhibit.

i

Default Directory | Overview

Microsoft Entra ID

+ Add

Manage tenants

What's new

Preview features

...

i

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview

Monitoring

Properties

Recommendations

Tutorials

Search your tenant

Basic information

Name

Default Directory

Tenant ID

c4d2baba-3de9-4dbe-abdb-2892387a97dd

Primary domain

sk230128outlook.onmicrosoft.com

License

Microsoft Entra ID Free

The tenant contains the identities shown in the following table.

Name	Type
User1	User account
Group1	Security group
Group2	Microsoft 365 group

You purchase a Microsoft Fabric license.

To which identities can you assign the license?

- A. User1 only
- B. User1 and Group1 only
- C. User1 and Group2 only
- D. User1, Group1, and Group2

Correct Answer: A

Community vote distribution

A (54%)

B (27%)

Other

- examprepboy

Highly Voted

7 months, 2 weeks ago

Selected Answer: A

Correct Answer is A Only
The Entra tenant is in FREE mode, so there is no P1 or P2 assigned.
Without this, all licence applying abilities are done by user mode ONLY.
When you get a Premium licence then you are allowed to assign by groups.
Tested in my lab
upvoted 23 times
- c75e123

4 months, 2 weeks ago

Correct!

You must have one of the following licenses for every user who benefits from group-based licensing:
Paid or trial subscription for Microsoft Entra ID P1 and higher.

<https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing#licensing-requirements>
upvoted 1 times

  **Sunth65** 5 months ago

<https://www.apps4rent.com/microsoft-entra-id-free-vs-p1-vs-p2-vs-governance.html>
upvoted 1 times

  **eduardovzermeno** 7 months ago

You're right: <https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing?context=azure%2Factive-directory%2Fusers-groups-roles%2Fcontext%2Fugr-context#licensing-requirements>
upvoted 3 times

  **Jo696** Highly Voted  7 months, 4 weeks ago

Selected Answer: B



I would think the answer is B, as it does not mention if Group 2 is security-enabled.
upvoted 5 times

  **serbanvadi** Most Recent  2 months, 1 week ago

Selected Answer: B

You can enable Microsoft Fabric for:
Your tenant - Use this option to enable Microsoft Fabric for everyone in the tenant.
A specific capacity - Use this option if you want to enable Microsoft Fabric for users in a specific capacity.
In both cases, you can use security groups to provide Microsoft Fabric access to a specified list of users.

<https://learn.microsoft.com/en-us/fabric/admin/fabric-switch>
upvoted 1 times

  **05e3903** 2 months, 1 week ago



Selected Answer: D

You can assign license to a user group M365 or security or a user in admin M365, so the correct answer is D: <https://learn.microsoft.com/en-ca/entra/identity/users/licensing-admin-center>
upvoted 1 times

  **vrn1358** 4 months, 1 week ago

Selected Answer: B

based on below refrence:
<https://learn.microsoft.com/en-us/fabric/admin/fabric-switch>
User1 and Group 1 is the answer
B
upvoted 1 times

  **amsioso** 4 months, 4 weeks ago

Selected Answer: A

Entra ID Free suppor only users asigment.
<https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing#licensing-requirements>
upvoted 2 times

  **minura** 5 months ago

Selected Answer: A

Microsoft Fabric licenses are per user licenses.
upvoted 1 times



  **[Removed]** 7 months, 3 weeks ago

Selected Answer: B

B is correct

User Accounts and Security Groups in a Microsoft Entra tenant can be assigned Microsoft Fabric licenses, while Microsoft 365 groups cannot be directly licensed.

To license members of a Microsoft 365 group, the licenses need to be assigned to the individual user accounts rather than the group itself.
upvoted 3 times

  **155e6a0** 7 months, 2 weeks ago

I even could not enable Microsoft Fabric with the Microsoft Entra ID Free license.
upvoted 1 times

  **155e6a0** 7 months, 2 weeks ago

Please post the link that supports your answer.
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: B

B is correct

User Accounts and Security Groups in a Microsoft Entra tenant can be assigned Microsoft Fabric licenses, while Microsoft 365 groups cannot be directly licensed.

To license members of a Microsoft 365 group, the licenses need to be assigned to the individual user accounts rather than the group itself.
upvoted 3 times

  **27f57ef** 8 months ago

In your tenant, you can enable Microsoft Fabric for:



The entire organization - In most cases your organization has one tenant, so selecting this option enables it for the entire organization. In organizations that have several tenants, if you want to enable Microsoft Fabric for the entire organization, you need to enable it in each tenant.

Specific security groups - Use this option to enable Microsoft Fabric for specific users. You can either specify the security groups that Microsoft Fabric will be enabled for, or the security groups that Microsoft Fabric won't be available for.

<https://learn.microsoft.com/en-us/fabric/admin/fabric-switch>
upvoted 2 times



  **adamtboyle** 8 months, 1 week ago

A. ChatGPT says Microsoft Entra ID Free licenses must be assigned on a per-user basis and cannot be assigned to security groups or Microsoft 365 groups. Microsoft Entra Premium P1 and P2 licenses can be assigned to groups and all users within the group will inherit the license.
upvoted 1 times

  **6c05b3d** 8 months, 2 weeks ago



Selected Answer: C

C. User1 and Group2 only
This assumes that Microsoft 365 groups are supported for license assignments, which they generally are, while security groups (Group 1) might not directly receive licenses themselves but can be used for grouping users for license assignments.
upvoted 5 times

  **Shakka** 8 months, 2 weeks ago



Selected Answer: D

I think its D, Correct me if I'm wrong
upvoted 1 times

  **alsmk2** 8 months, 2 weeks ago

Selected Answer: D

I think you can assign this to all three.
upvoted 2 times

  **alsmk2** 8 months, 2 weeks ago

Scrap that - only if the m365 group was security-enabled, which isn't mentioned. C is correct.
upvoted 1 times

You have an Azure subscription that contains a storage account named storage. The storage account contains a blob that stores images.

Client access to storage1 is granted by using a shared access signature (SAS).

You need to ensure that users receive a warning message when they generate a SAS that exceeds a seven-day time period.

What should you do for storage?

- A. Enable a read-only lock.
- B. Configure an alert rule.
- C. Add a lifecycle management rule.
- D. Set Allow recommended upper limit for shared access signature (SAS) expiry interval to Enabled.

Correct Answer: D

Community vote distribution


D (100%)

  **Shakka** Highly Voted 8 months, 2 weeks ago



Selected Answer: D

D Correct

Sign in to the Azure portal:
Ensure you have the necessary administrative privileges.
Navigate to the Storage Account:
Go to Storage accounts and select the storage account named storage.
Configure the SAS Expiration Policy:
In the storage account settings, go to Configuration.
Under Shared access signature (SAS) settings, find the SAS expiration policy.
Set the Recommended upper limit for SAS expiration to 7 day
upvoted 5 times

  **Brzzzzz4489** 6 months, 4 weeks ago

Question asks how to send a warning email if a condition is met, wouldn't that be an alert regardless of SAS expiration policy?
upvoted 1 times

  **RPINTO** 4 months, 1 week ago

A SAS expiration policy doesn't prevent a user from creating a SAS with an expiration that exceeds the limit recommended by the policy. When a user creates a SAS that violates the policy, they see a warning, along with the recommended maximum interval. If you've configured a diagnostic setting for logging with Azure Monitor, then Azure Storage writes a message to the 'SasExpiryStatus' property in the logs whenever a user uses a SAS that expires after the recommended interval; the message indicates that the validity interval of the SAS exceeds the recommended interval.

> <https://learn.microsoft.com/en-us/azure/storage/common/sas-expiration-policy?tabs=azure-portal#:~:text=A%20SAS%20expiration%20policy%20doesn%27t,SAS%20exceeds%20the%20recommended%20interval.>
upvoted 1 times

  **58b2872** Most Recent 4 months ago

Selected Answer: D

To ensure users receive warnings when generating SAS tokens that exceed a 7-day expiry, D. Set Allow recommended upper limit for shared access signature (SAS) expiry interval to Enabled is the correct choice.
upvoted 1 times

  **sca88** 5 months, 2 weeks ago

Selected Answer: D

<https://learn.microsoft.com/en-us/azure/storage/common/sas-expiration-policy?tabs=azure-portal>
upvoted 3 times

  **Sweden2022** 7 months ago

Selected Answer: D

D is correct.
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: D

D is corect
upvoted 1 times

  **KAM2023** 8 months, 2 weeks ago

Selected Answer: D

Correct
upvoted 3 times

  **DJHASH786** 8 months, 2 weeks ago

Correct Answer
upvoted 1 times

You have an Azure subscription named Subscription1 that contains the storage accounts shown in the following table:

Name	Account kind	Azure service that contains data
storage1	Storage	File
storage2	StorageV2 (general purpose v2)	File, Table
storage3	StorageV2 (general purpose v2)	Queue
storage4	BlobStorage	Blob

You plan to use the Azure Import/Export service to export data from Subscription1.

You need to identify which storage account can be used to export the data.

What should you identify?

- A. storage1
- B. storage2
- C. storage3
- D. storage4

Correct Answer: D

Community vote distribution



mlantonis Highly Voted 3 years, 11 months ago

Correct Answer: D

- Azure Import/Export service supports the following of storage accounts:
- ☞ Standard General Purpose v2 storage accounts (recommended for most scenarios)
 - ☞ Blob Storage accounts
 - ☞ General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments),

- Azure Import/Export service supports the following storage types:
- ☞ Import supports Azure Blob storage and Azure File storage
 - ☞ Export supports Azure Blob storage. Azure Files not supported.

Only storage4 can be exported.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements>
upvoted 225 times

c75e123 4 months, 2 weeks ago

Correct:
The following list of storage types is supported with Azure Import/Export service.

Import
Azure Blob Storage: Block blobs and Page blobs
Azure Files storage: Files

Export:
Azure Blob Storage: Block blobs, Page blobs, and Append blobs

Azure Files not supported
Export from archive tier not supported

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>
upvoted 3 times

suriyaswamy 3 years, 8 months ago

Very useful Info
upvoted 1 times

Babustest 1 year, 7 months ago

Thank you
upvoted 1 times



  **nfett** Highly Voted 4 years ago

From the provided link. I assume since they table in the question notes "Storage" its being disregarded as an invalid option. Thus the answer blob appears to be correct.
Standard General Purpose v2 storage accounts (recommended for most scenarios)
Blob Storage accounts
upvoted 10 times




  **careTaker** Most Recent 3 months ago



Selected Answer: D

Answer is still D today...
Reference: <https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service#inside-an-export-job> (read the note specific to export which is the question, import only supported in both blob and file; export supported only from blob)
upvoted 1 times

  **58b2872** 4 months ago

Selected Answer: D

Azure Import/Export service supports the following of storage accounts:
 Standard General Purpose v2 storage accounts (recommended for most scenarios)
 Blob Storage accounts
 General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments),



Azure Import/Export service supports the following storage types:
 Import supports Azure Blob storage and Azure File storage
 Export supports Azure Blob storage. Azure Files not supported.
upvoted 1 times

  **MackD** 4 months, 3 weeks ago

Selected Answer: A

This does not apply anymore:
<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service>

How does Import/Export work?
Azure Import/Export service allows data transfer into Azure Blobs and Azure Files by creating jobs. Use Azure portal or Azure Resource Manager REST API to create jobs. Each job is associated with a single storage account.
upvoted 1 times

  **CheMetto** 9 months, 1 week ago

Selected Answer: D

Azure import export support Standard general Purpose V2 and Premium Block Blob. However it support only file and blob, so B is excluded for this reason
upvoted 1 times

  **tashakori** 1 year, 1 month ago

D is right
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

D is correct
upvoted 1 times

  **Tilakarasu** 1 year, 3 months ago

Azure Import/Export service allows data transfer into Azure Blobs and Azure Files by creating jobs.
The jobs can be import or export jobs. An import job allows you to import data into Azure Blobs or Azure files whereas the export job allows data to be exported from Azure Blobs.
upvoted 1 times

  **oopspruu** 1 year, 8 months ago

Given answer is right. Notes below:
Azure Import/Export Supports: Standard General Purpose v2 storage accounts, Blob Storage Accounts, General Purpose v1 accounts. Types Supported: Import – Blob, Files, Export – Blob. Archive tier is not supported for Export.
upvoted 1 times

  **GoldenDisciple2** 1 year, 8 months ago

Just want clarification. I'm assuming that the answer can't be B because the Azure service contains data in file and table. Where as if it was only file without table then B would have been a good choice as well as D?
upvoted 1 times

  **eeperetz** 1 year, 8 months ago

You cannot export Azure Files with Azure Import/Export.
upvoted 1 times



  **Mehedi007** 1 year, 9 months ago

Selected Answer: D

"Block blobs, Page blobs, and Append blobs supported"



<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>

upvoted 1 times

  **NYTK** 1 year, 9 months ago

Came in exams 27/7/2023. I selected D

upvoted 6 times

  **itguyeu** 1 year, 10 months ago

I used free version access for this site and it helped me pass the exam. Some questions that I had on the exams, I took the exam more than once, are not available under the free tier access, but 80% of the questions came from here. I do recommend investing a bit of money and getting full access to this site. I didn't memorise answers but analysed them and studied as Microsoft does tweak them a bit.



This Q was on the exam.

upvoted 2 times

  **kmsalman** 1 year, 10 months ago

was on the exam on June 17 2023

upvoted 3 times



  **sadsad** 1 year, 10 months ago

When using the Azure Import/Export service to export data, the supported storage account types are as follows:

Standard General Purpose v2 Storage Accounts: The Azure Import/Export service supports exporting data from storage accounts of the Standard General Purpose v2 kind. These storage accounts provide a combination of storage capabilities for blobs, files, queues, and tables.

Blob Storage Accounts: Blob storage accounts, which are specialized storage accounts optimized for storing and serving large amounts of unstructured data, can also be used for exporting data using the Azure Import/Export service.

upvoted 2 times

  **guegue** 1 year, 11 months ago

Correct Answer: D

Refer to MS official documentation - <https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service#how-does-importexport-work>

upvoted 1 times

HOTSPOT -

You have Azure Storage accounts as shown in the following exhibit.

Home > Storage accounts

Storage accounts

+ Add

≡ Edit columns

↻ Refresh

🏷 Assign Tags

🗑 Delete

Subscription: All 2 selected - Don't see a subscription? Switch directories

Filter by home...

All subscriptions




All resource groups

All types

All locations

No grouping

3 items

<input type="checkbox"/>	NAME ↑	TYPE ↑	KIND ↑	RESOURCE... ↑	LOCATION ↑	SUBSCRIPTION ↑	ACCESS T...	REPLICAT...
<input type="checkbox"/>	 storageaccount1	Storage account	Storage	ContosoRG1	East US	Subscription 1	-	Read-access ge...
<input type="checkbox"/>	 storageaccount2	Storage account	StorageV2	ContosoRG1	Central US	Subscription 1	Hot	Geo-redundant...
<input type="checkbox"/>	 storageaccount3	Storage account	BlobStorage	ContosoRG1	East US	Subscription 1	Hot	Locally-redundant...

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can use [answer choice] for Azure Table Storage.

storageaccount1 only

storageaccount2 only

storageaccount3 only

storageaccount1 and storageaccount2 only

storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only

storageaccount2 and storageaccount3 only

storageaccount1 and storageaccount3 only

all the storage accounts

Correct Answer:

Answer Area

You can use [answer choice] for Azure Table Storage.

storageaccount1 only

storageaccount2 only

storageaccount3 only

storageaccount1 and storageaccount2 only

storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only

storageaccount2 and storageaccount3 only

storageaccount1 and storageaccount3 only

all the storage accounts

Box 1: storageaccount1 and storageaccount2 only

Box 2: All the storage accounts -



Note: The three different storage account options are: General-purpose v2 (GPv2) accounts, General-purpose v1 (GPv1) accounts, and Blob storage accounts.



- ☞ General-purpose v2 (GPv2) accounts are storage accounts that support all of the latest features for blobs, files, queues, and tables.
- ☞ Blob storage accounts support all the same block blob features as GPv2, but are limited to supporting only block blobs.
- ☞ General-purpose v1 (GPv1) accounts provide access to all Azure Storage services, but may not have the latest features or the lowest per



gigabyte pricing.
Reference:
<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-options>



  **mlantonis** Highly Voted 3 years, 11 months ago
Correct Answer:



Box 1: storageaccount1 and storageaccount2 only
Box 2: All the storage accounts
upvoted 190 times



  **JayBee65** 3 years, 11 months ago
Why do you say that?
upvoted 5 times



  **Energo** 2 years, 3 months ago
because he is the chosen one.
upvoted 67 times



  **Ark_Phoenix** 1 year, 8 months ago
You're God Damn right!!
Say it again!
upvoted 5 times



  **Juwizee** 1 year, 6 months ago
Its "mlantonis", He never miss!
upvoted 8 times



  **[Removed]** 9 months, 2 weeks ago
HE DUN MISS!
upvoted 1 times



  **Slimus** 1 year, 11 months ago
<https://images.squarespace-cdn.com/content/v1/5af21c03e17ba3f52f6d007b/1561741063599-OYAYQPVVN84F8TMRVKV/Table+comparing+Storage+Account+Types%2C+Services+and+Performance?format=1500w>
upvoted 4 times



  **fedztetz** Highly Voted 4 years, 4 months ago
Answer is correct.
- Storage account 1 & 2
- All storage accounts.
upvoted 178 times



  **JayBee65** 3 years, 11 months ago
Why do you say that?
upvoted 5 times



  **Saravana12g** 3 years, 7 months ago
Why do you ask that?
It's correct...
upvoted 11 times

  **Omar_Aladdin** 3 years, 7 months ago
Hey, What's the problem with asking. That's not acceptable
upvoted 49 times

  **Takloy** 3 years, 6 months ago
Hey! stop fighting! lol
upvoted 25 times

  **CloudHustler** 2 years, 7 months ago
y'all gotta do better than this
upvoted 10 times

  **garmatey** 1 year, 11 months ago
maybe to understand *why* it is correct...
upvoted 9 times

  **Shailen** 3 years, 10 months ago
Since question 1 is to store table storage which can't be done in blob storage account (blob storage is the premium storage which is either block blob, append blob or page blob). refer <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction#blob-storage-resources>
upvoted 27 times

- allinict_111

Most Recent

5 months, 1 week ago

No, a Blob storage account does not support Table storage. Blob storage accounts are specifically optimized for storing unstructured data such as text, binary data, documents, media files, backups, and more.

upvoted 1 times
- [Removed]

7 months, 3 weeks ago

CORRECT

upvoted 2 times
- varinder82

11 months, 3 weeks ago

Final Answer:
Box 1: storageaccount1 and storageaccount2 only
Box 2: All the storage accounts

upvoted 1 times
- 3c5adce

11 months, 4 weeks ago

ChatGPT4 says:
for Azure Table Storage: storageaccount2 and storageaccount3 / These are 'StorageV2' accounts, typically supporting table storage unless explicitly restricted.
for Azure Blob Storage: storageaccount2 and storageaccount3 / These 'StorageV2' accounts are suitable for blob storage.

upvoted 1 times
- 3c5adce

11 months, 4 weeks ago

Box 1: storageaccount1 and storageaccount2 only
Box 2: All the storage accounts

upvoted 1 times
- tashakori

1 year, 1 month ago

Given answer is Correct

upvoted 1 times
- devops_devops

1 year, 3 months ago

This question was in exam 15/01/24

upvoted 3 times
- Mehedi007

1 year, 9 months ago

Box 1: storageaccount1 and storageaccount2 only
Box 2: All the storage accounts

<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#types-of-storage-accounts>
<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#legacy-storage-account-types>

upvoted 2 times
- NYTK

1 year, 9 months ago

Came in exams 21/7/2023. I selected Storage acct1 &2 and all storage accounts.

upvoted 7 times
- Puja_Azure

1 year, 9 months ago

How was your exam. I will appear in 2 days.

upvoted 2 times
- neolisto

1 year, 6 months ago

Puja_Azure how you pass it mate?

upvoted 1 times
- Juanchooo

1 year, 11 months ago

Came in my exam today 17/05/23

upvoted 4 times
- keszi

2 years, 2 months ago

Question appeared on the exam 3/1/2023

upvoted 12 times
- B_M_A

2 years, 3 months ago

This came in my Exam today . Passed my exam. However want to bring it to those who are studying . In the answer area the Blob Storage was first followed by Azure Table.

upvoted 15 times
- Hongzu13

2 years, 3 months ago



This was on the exam today!

upvoted 7 times
- [Removed]

2 years, 3 months ago


definitely test

upvoted 1 times

  **Zetten** 2 years, 5 months ago

why is everyone ignoring the fact that storage 1 is read only?

upvoted 1 times

  **fabrideci** 2 years, 4 months ago

It is not, that's the replication mode only

upvoted 1 times

  **Alex2022_31** 2 years, 4 months ago

It's not read-only, this is the replication that is Read-only georedundant which means that you can read the replicas in the secondary zone where the data is replicated for high availability purpose

upvoted 11 times

You have Azure subscription that includes data in following locations:

Name	Type
container1	Blob container
share1	Azure files share
DB1	SQL database
Table1	Azure Table

You plan to export data by using Azure import/export job named Export1.

You need to identify the data that can be exported by using Export1.

Which data should you identify?

- A. DB1
- B. container1
- C. share1
- D. Table1

Correct Answer: B

Community vote distribution

B (100%)

- Anon6969

Highly Voted

4 years, 5 months ago

Blobs are only type of storage which can be exported.
upvoted 140 times

Holydud

2 years, 8 months ago

Was on exam 19 Aug 2022. Scored 870. Answered B
upvoted 21 times

rodrod

6 months, 1 week ago

how does it help to know if B is valid??
upvoted 2 times
- fedztedz

Highly Voted

4 years, 4 months ago

Answer is correct. B - Blob Container.
For Azure file share, it is tricky as it is mentioned Azure Files can be used for export and import. But I tested especially with file share and it doesn't work. Maybe work for storage account with type file or something. but not Azure file shares.
upvoted 80 times

ASalam

2 years, 6 months ago

1. Import and export support for blob storage.
2. Only import support for File storage but export not support. check the table of Supported storage types
<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>
upvoted 8 times

Bravo_Dravel

Most Recent

3 months, 1 week ago

Selected Answer: B

Azure Import/Export service supports exporting data from the following storage services:
1. Azure Blob Storage: You can export data from block blobs, page blobs, and append blobs.
2. Azure Files: Currently, the service supports importing data into Azure Files but does not support exporting data from Azure Files
upvoted 1 times

[Removed]

7 months, 3 weeks ago

Selected Answer: B

B is correct

only Blobs storage type can be exported
upvoted 1 times

[Removed]

8 months ago

Selected Answer: B

B is correct

only Blobs storage type can be exported
upvoted 1 times

  **tashakori** 1 year, 1 month ago

B is correct
upvoted 2 times

  **tfdestroy** 1 year, 4 months ago

Selected Answer: B

DB1: While Azure Import/Export can be used for some database scenarios with specific tools and services, the information available in the image doesn't indicate compatibility with SQL databases like DB1.

share1: Azure Import/Export supports exporting data from Azure Files shares like share1. However, the image specifically mentions "container1" which is a more likely target for data export in this context.

Table1: Azure Import/Export doesn't support exporting data from Azure Table Storage like Table1.

container1: Blob containers like container1 are the primary data target for Azure Import/Export jobs. The image explicitly lists container1 alongside other resources, making it the most likely candidate for data export.

Therefore, given the available information and the focus on "container1" within the image, the data you should identify for export with Export1 is B. container1.

upvoted 4 times

  **BillDilena** 1 year, 8 months ago

Selected Answer: B

Supported storage types for Export jobs: Block blobs, Page blobs, and Append blobs supported
<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements>



upvoted 3 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: B

"Block blobs, Page blobs, and Append blobs supported"
<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>



upvoted 1 times

  **NYTK** 1 year, 9 months ago

Came in exams 21/7/2023. Selected B
upvoted 3 times

  **Juanchooo** 1 year, 11 months ago

Came in my exam today 17/05/23
upvoted 4 times

  **Siraf** 1 year, 11 months ago

Answer is B:
Azure Import/Export service supports the following of storage accounts: - Standard General Purpose v2 storage accounts (recommended for most scenarios), - Blob Storage accounts, - General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments).
Azure Import/Export service supports the following storage types:
- Import supports Azure Blob storage and Azure File storage,
- Export supports Azure Blob storage.
So, Azure Files, Tables and Queues are not supported for export. <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements>
upvoted 2 times



  **VikasN** 2 years, 1 month ago

One can get hint from Question 1 of Topic 3
upvoted 1 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: B

Blobs are only type of storage which can be exported.
upvoted 2 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) "container1"

The following list of storage types is supported with Azure Import/Export service:
- Export: Azure Blob Storage -> Block blobs, Page blobs, and Append blobs supported.
* Azure Files not supported & Export from archive tier not supported

Reference: <https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>
upvoted 4 times

  **Mev4953** 2 years, 7 months ago

Import => Azure Blob Storage
Azure File Storage

Export=> Azure Blob Storage
upvoted 6 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

HOTSPOT -

You have an Azure Storage account named storage1.

You have an Azure App Service app named App1 and an app named App2 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App1 and App2 can read blobs from storage1. The solution must meet the following requirements:

- ⇒ Minimize the number of secrets used.
- ⇒ Ensure that App2 can only read from storage1 for the next 30 days.

What should you configure in storage1 for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

	▼
Access keys	
Advanced security	
Access control (IAM)	
Shared access signatures (SAS)	

App2:

	▼
Access keys	
Advanced security	
Access control (IAM)	
Shared access signatures (SAS)	

Answer Area

Correct Answer:

App1:

	▼
Access keys	
Advanced security	
Access control (IAM)	
Shared access signatures (SAS)	

App2:

	▼
Access keys	
Advanced security	
Access control (IAM)	
Shared access signatures (SAS)	

🗨️ **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

Box 1: Access Control (IAM)

Since the App1 uses Managed Identity, App1 can access the Storage Account via IAM. As per requirement, we need to minimize the number of secrets used, so Access keys is not ideal.

Box 2: Shared access signatures (SAS)

We need temp access for App2, so we need to use SAS.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-auth>
upvoted 499 times

🗨️ **Tayhull2023** 1 year, 6 months ago

I am starting to think mlantonis is a super computer =O
upvoted 20 times

🗨️ **Mentalfloss** 9 months, 1 week ago

If mlantonis was hired to research and post as he or she does, I approve of how my fees are used. :)
upvoted 5 times

🗨️ 👤 **sreekan** 3 years, 8 months ago
this is absolute!!!
upvoted 5 times

🗨️ 👤 **nahte** 2 years, 9 months ago
totally agree of using MI+IAM
upvoted 3 times

🗨️ 👤 **go4adil** 1 year, 3 months ago
Agreed.

Below link clearly maps the situation mentioned in the question.

<https://learn.microsoft.com/en-us/azure/app-service/scenario-secure-app-access-storage?tabs=azure-portal>
upvoted 2 times

🗨️ 👤 **Andersonalm** Highly Voted 👍 4 years, 5 months ago

I think App1 should access storage1 over IAM with managed identity. The requirement is minimize the number of secrets used...
upvoted 122 times

🗨️ 👤 **Abhi92** 4 years, 4 months ago
Yes Correct
upvoted 3 times

🗨️ 👤 **pieronegri** 4 years, 4 months ago
that was my thought as well.
upvoted 3 times

🗨️ 👤 **prashantjoge** 4 years, 4 months ago
That's what I thought too
upvoted 4 times

🗨️ 👤 **diligent176** 4 years, 4 months ago
Yes, and especially since they say "apps can read blobs from storage1"...
So, IAM is supported in that case and requires no secrets to keep.
App1 = IAM / RBAC and App2 = SAS
<https://docs.microsoft.com/en-us/azure/storage/common/storage-auth>
upvoted 20 times

🗨️ 👤 **Tranquillo1811** 3 years, 11 months ago
If you use IAM then for each access request a new token is requested by the service account. Hence for each access request a new token (a new secret) is used.
if you use the access keys though, it is always the very same secret is used.

Hence I'd say that "Access Keys" is the correct choice for App1...
upvoted 10 times

🗨️ 👤 **RamanAgarwal** 3 years, 11 months ago
You can use managed identity to access storage so this way you dont have to create a token anytime you want to access the storage account.
upvoted 6 times

🗨️ 👤 **Nepton** Most Recent 🕒 2 months ago

Box 1: Access Control (IAM)
Since the App1 uses Managed Identity, App1 can access the Storage Account via IAM. As per requirement, we need to minimize the number of secrets used, so Access keys is not ideal.

Box 2: Shared access signatures (SAS)
We need temp access for App2, so we need to use SAS.
A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data. You can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

Reference:
<https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
<https://docs.microsoft.com/en-us/azure/storage/common/storage-auth>
upvoted 1 times

🗨️ 👤 **Bravo_Dravel** 3 months, 1 week ago

Correct Answer:
BOX 1:Access Control(IAM)
pp1 has a managed identity, and you can assign a Storage Blob Data Reader role to the managed identity of App1 in the access control (IAM) settings for storage1. This approach eliminates the need for secrets and allows App1 to read blobs securely
Box 2: Shared access siganture(SAS)
Use a Shared access signature (SAS). This allows you to create a time-limited access token that grants read permissions to App2 for the next 30 days.
upvoted 2 times

🗨️ 👤 **[Removed]** 7 months, 3 weeks ago
WRONG

App1: Access control (IAM)
App2: Shared access signatures (SAS)
upvoted 3 times

🗨️ 👤 **[Removed]** 8 months ago
WRONG

App1: Access Control (IAM)
App2: Shared Access Signatures (SAS)
upvoted 1 times

🗨️ 👤 **ajay01avhad** 9 months, 1 week ago
App1: Access control (IAM)
App2: Shared access signatures (SAS)
upvoted 1 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago
- Access keys (IAM)
- shared access signatures (SAS)
upvoted 1 times

🗨️ 👤 **iamchoy** 1 year, 7 months ago
To ensure that App1 and App2 can read blobs from storage1 while meeting the given requirements, you would use the following:

1. ****App1****:
Since App1 uses a managed identity and there's no mention of time restrictions for its access, you should grant its managed identity the necessary permissions using Azure RBAC (Role-Based Access Control).

Thus, for App1, the answer would be:
- ****Access control (IAM)****: You should assign the managed identity of App1 the necessary role (e.g., "Storage Blob Data Reader") at the appropriate scope.

2. ****App2****:
For App2, it's specified that the access should only last for the next 30 days. Shared Access Signatures (SAS) are best for providing time-limited access to resources in Azure Storage.

Thus, for App2, the answer would be:
- ****Shared access signatures (SAS)****: Generate an SAS token with read permissions on the blob service and set its expiration to 30 days in the future.

Summary:
- App1: Access control (IAM)
- App2: Shared access signatures (SAS)
upvoted 5 times

🗨️ 👤 **az11q** 1 year, 8 months ago
It would be immensely appreciated if someone with "Contributor Access" could kindly share all the questions, answers, and associated discussions in a PDF format. Your invaluable support holds immense significance for me, and I earnestly seek your assistance in this journey. Any help extended is deeply appreciated.
upvoted 1 times

🗨️ 👤 **oopspruu** 1 year, 8 months ago
Since App1 uses managed identity, it means it can be given access through IAM. Doing it through Access Keys would make use of additional secret. Answer to first should be IAM.
upvoted 1 times

🗨️ 👤 **Mehedi007** 1 year, 9 months ago
IAM & SAS.
IAM because of managed identity. SAS because of time limited access.
upvoted 4 times

🗨️ 👤 **JWS80** 1 year, 9 months ago
For App1, you should configure Access control (IAM) in storage1. This will allow you to grant the managed identity used by App1 the necessary permissions to read blobs from storage1 using role-based access control (RBAC). This approach minimizes the number of secrets used, as it does not require the use of access keys or shared access signatures.

For App2, you should configure Shared access signatures (SAS) in storage1. This will allow you to create a shared access signature with an expiry time of 30 days, which will grant App2 temporary read access to blobs in storage1. After 30 days, the shared access signature will expire and App2 will no longer be able to read from storage1.
upvoted 1 times

🗨️ 👤 **Teroristo** 1 year, 9 months ago
Box 1: Access Control (IAM)
Since the App1 uses Managed Identity, App1 can access the Storage Account via IAM. As per requirement, we need to minimize the number of secrets used, so Access keys is not ideal.

Box 2: Shared access signatures (SAS)

We need temp access for App2, so we need to use SAS.



A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data. You can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>



<https://docs.microsoft.com/en-us/azure/storage/common/storage-auth>

upvoted 1 times

  **NYTK** 1 year, 9 months ago

Came in exams on 21/7/2023. I selected Access control and SAS


upvoted 7 times

  **itguyeu** 1 year, 10 months ago

I used free version access for this site and it helped me pass the exam. Some questions that I had on the exams, I took the exam more than once, are not available under the free tier access, but 80% of the questions came from here. I do recommend investing a bit of money and getting full access to this site. I didn't memorise answers but analysed them and studied as Microsoft does tweak them a bit.

This Q was on the exam.

upvoted 5 times

  **xRiot007** 1 year, 11 months ago

Box 1 : IAM - you want least amount of secrets used

Box 2 : SAS - you want this because you are able to set a duration

upvoted 2 times

HOTSPOT -

You need to create an Azure Storage account that meets the following requirements:

- ⇒ Minimizes costs
- ⇒ Supports hot, cool, and archive blob tiers
- ⇒ Provides fault tolerance if a disaster affects the Azure region where the account resides

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

```
az storage account create -g RG1 -n storageaccount1
```

--kind

	▼
FileStorage	
Storage	
StorageV2	

 --sku

	▼
Standard_GRS	
Standard_LRS	
Standard_RAGRS	
Premium_LRS	

Correct Answer:

Answer Area

```
az storage account create -g RG1 -n storageaccount1
```

--kind

	▼
FileStorage	
Storage	
StorageV2	

 --sku

	▼
Standard_GRS	
Standard_LRS	
Standard_RAGRS	
Premium_LRS	

Box 1: StorageV2 -

You may only tier your object storage data to hot, cool, or archive in Blob storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts do not support tiering.

General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices.

Box 2: Standard_GRS -

Geo-redundant storage (GRS): Cross-regional replication to protect against region-wide unavailability.

Incorrect Answers:

Locally-redundant storage (LRS): A simple, low-cost replication strategy. Data is replicated within a single storage scale unit.

Read-access geo-redundant storage (RA-GRS): Cross-regional replication with read access to the replica. RA-GRS provides read-only access to the data in the secondary location, in addition to geo-replication across two regions, but is more expensive compared to GRS.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs> <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

 **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

Box 1: StorageV2

Box 2: Standard_GRS

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs>

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

upvoted 244 times

  **memo454** 1 year, 8 months ago

Pass the exam on 11 August 2023 with 909, Below are some of the notes that may help for Blob and file storage:

A. Blob Storage:

- 1-Archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. Only storage accounts that are configured for LRS, GRS, or RA-GRS support moving blobs to the archive tier.
- 2-Import supports Azure Blob storage and Azure File storage
- 3 -Export supports Azure Blob storage
- 4-support Lifecycle management policies. Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.
- 5-Object Replication supports General Purpose V2 and Premium Blob accounts.
- 6-Support both Azure (AD) and SAS (Shared Access Signature) token.

upvoted 48 times

  **memo454** 1 year, 8 months ago

A. Blob Storage: Continue..

- 7-Support conditions when added to built-in or custom role assignments that have blob storage or queue storage data actions
- 8-Encryption scopes support a container or an individual blob
- 9-Not Support ZRS
- 10-az support
- 11-support stored access policies
- 12-Tieing is supporting only or block blobs
- 13-Flow logging for Blob Storage accounts has a retention period of 30 days. General Purpose v2 (GPv2) storage accounts instead, which support flow logging with a retention period of up to 365 days.

upvoted 23 times

  **memo454** 1 year, 8 months ago

B.File storage:

- 1-az support
- 2-Support persistent storage.
- 3-File share Supports Premium file shares (FileStorage), Premium LRS/ZRS for SMB Multichannel
- 4-File Storage: Only Shared Access Signature (SAS) token is supported.
- 5-Only Shared Access Signature (SAS)
- 6-Premium file shares
- 6-Import supports Azure Blob storage and Azure File storage
- 7-supports identity-based authentication over Server Message Block (SMB) through on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

upvoted 23 times

  **memo454** 1 year, 8 months ago

B.File storage:: Continue ..



- 8-Not support archive
- 9-Not support condition
- 10-No support Object Replication
- 11-No support Lifecycle management policies
- 12-no support encryption scope

upvoted 24 times

  **Hybrid410** 1 year, 5 months ago

Thank you so much

upvoted 2 times

  **jackill** 1 year, 8 months ago



I agree

Box 1: StorageV2

Box 2: Standard_GRS

Regarding a clear official statement of the missing support for access tiers by StorageV1 (named "Storage" in the --kind option), I've found this URL <https://azure.microsoft.com/en-us/pricing/details/storage/blobs/>, in the "Other" tab, you can read "Note: General-purpose v1 accounts don't have access to Hot, Cool, or Archive tiered storage. For access to tiered storage, upgrade to a general-purpose v2 account."

upvoted 3 times

  **Panapi** 2 years, 2 months ago

Answer Valid! This question was on the exam 22/02/2023. Scored 920. Thanks guys!

upvoted 26 times

  **obaali1990** 2 years, 1 month ago

Congratulations

upvoted 9 times

  **ihavespoken** Highly Voted  4 years, 5 months ago

Keep in mind the question is mentioning the minimize cost, even though Storage v2 and blob both can support the hot, cool, and archive but Storage V2 is lowest cost. so answer is correct.

upvoted 88 times

  **jelly_baby** 4 years, 4 months ago

agreed

upvoted 2 times

  **Aniruddha_dravyakar** 4 years, 2 months ago

agreed

upvoted 1 times

  **sidharthwader** 4 years ago

Yes GPv2 gives the storage in least price with latest features.

upvoted 2 times

  **JayBee65** 3 years, 11 months ago

This calculator shows the same price for Storage v2 as Blob Storage: <https://azure.microsoft.com/en-gb/pricing/calculator/?service=storage>

upvoted 3 times

  **xRiot007** 1 year, 11 months ago

Blob storage is not listed as an option. Maybe the question has been updated :) Today, Blob Storage and GPv2 have the same price (tested using the azure calculator)

upvoted 1 times

  **[Removed]** Most Recent 7 months, 3 weeks ago

CORRECT

upvoted 2 times

  **tashakori** 1 year, 1 month ago

Given answer is correct

upvoted 1 times

  **nmnm22** 1 year, 7 months ago

mlantonis i owe u my lyfe

upvoted 4 times



  **iamchoy** 1 year, 7 months ago

Considering the requirements, the `az` command would be:

az storage account create -g RG1 --n storageaccount1 --kind StorageV2 --sku Standard_GRS

Here, `--kind StorageV2` specifies a general-purpose v2 storage account, and `--sku Standard_GRS` specifies geo-redundant storage for disaster recovery.

upvoted 1 times

  **Kr1s** 1 year, 9 months ago

Q was in exam 29TH July 2023

upvoted 6 times

  **garmatey** 1 year, 10 months ago

RA-GRS provides read only access to the data in the secondary location. So does this mean GRS give you no access at all to the replica? Is there a way to have equally full access to the replica as the primary?

upvoted 2 times

  **habbey** 2 years ago

StorageV2 N Standard_GRS

upvoted 2 times

  **vbohr899** 2 years, 2 months ago

Cleared Exam today 26 Feb, This question was there in exam.

upvoted 5 times

  **[Removed]** 2 years, 5 months ago

on Exam 24.11.2022, passed with 780 !! Thanks to everyone!! Good Luck

upvoted 10 times

  **NaoVaz** 2 years, 7 months ago

- 1) StorageV2
- 2) Standard_GRS

GRS for redundancy, and V2 to support the various Access Tiers and keep costs as low as possible.



upvoted 2 times



  **EmnCours** 2 years, 8 months ago



Correct Answer:



Box 1: StorageV2

Box 2: Standard_GRS
upvoted 1 times

  **JacquesV** 2 years, 8 months ago
In exam on 10Aug2022
upvoted 3 times

  **vsharma041990** 2 years, 9 months ago
Keep in mind the question is mentioning the minimize cost, even though Storage v2 and blob both can support the hot, cool, and archive but Storage V2 is lowest cost. so answer is correct.
upvoted 2 times

  **Lazylinux** 2 years, 10 months ago
Answer is correct as per others comments
upvoted 1 times

  **manalshowaei** 2 years, 10 months ago
Box 1: StorageV2

Box 2: Standard_GRS
upvoted 1 times

You have an Azure subscription that contains the resources in the following table.

Name	Type
RG1	Resource group
store1	Azure Storage account
Sync1	Azure File Sync

Store1 contains a file share named data. Data contains 5,000 files.

You need to synchronize the files in the file share named data to an on-premises server named Server1.

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



NOTE: Each correct selection is worth one point.


- A. Create a container instance
- B. Register Server1
- C. Install the Azure File Sync agent on Server1
- D. Download an automation script
- E. Create a sync group

Correct Answer: BCE

Community vote distribution

BCE (100%)

-   **mlantonis**

Highly Voted 

 3 years, 11 months ago



Correct Answer: B, C and E



Step 1: Install the Azure File Sync agent on Server1. The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share.



Step 2: Register Server1. Register Windows Server with Storage Sync Service. Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server and the Storage Sync Service.


Step 3: Create a sync group and a cloud endpoint. A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

Reference:



<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>
upvoted 319 times
-   **SumanSaurabh** 2 years, 5 months ago


Awesome
upvoted 3 times
-   **harsh_cloud** 2 years, 2 months ago

Correct Answer. Thanks Mlantonis.
upvoted 5 times
-   **WYLC**

Highly Voted 



 4 years, 5 months ago



that's correct!
upvoted 29 times
-   **Red_lotus85**

Most Recent 

 2 months, 1 week ago

Selected Answer: BCE

Confermo
upvoted 1 times
-   **aaqibkhan123** 4 months, 2 weeks ago

C, B, E is the correct order.
Reference : <https://www.youtube.com/watch?v=CpqrEDzxdMc>
upvoted 2 times
-   **minura** 5 months ago


Selected Answer: BCE

Correct answers B, C and E
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: BCE

B C E are correct
upvoted 1 times

  **tashakori** 1 year, 1 month ago

B, C and E is right
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

B, C and E is correct
upvoted 1 times


  **iamchoy** 1 year, 7 months ago

To synchronize the files in the Azure file share named `data` to an on-premises server named Server1 using Azure File Sync, follow these steps:

1. ****Register Server1****: Before an on-premises server can join a sync group, it needs to be registered with the Storage Sync Service. This is an essential step for the Azure File Sync setup.
2. ****Install the Azure File Sync agent on Server1****: The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share. Installing this agent on Server1 will facilitate the synchronization of files between Azure and the on-premises server.
3. ****Create a sync group****: A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. In this scenario, one of the endpoints will be the Azure file share, and the other will be a path on Server1.

Given the options, the correct actions to perform are:

- B. Register Server1
 - C. Install the Azure File Sync agent on Server1.
 - E. Create a sync group.
- upvoted 3 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: BCE

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>
upvoted 1 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: BCE

Step 1: Install the Azure File Sync agent on Server1. The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share.

Step 2: Register Server1. Register Windows Server with Storage Sync Service. Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server and the Storage Sync Service.

Step 3: Create a sync group and a cloud endpoint. A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>
upvoted 4 times

  **ZakySama** 2 years, 5 months ago

Selected Answer: BCE

BCE are the correct answer
upvoted 2 times

  **NaoVaz** 2 years, 7 months ago

B) "Register Server1" & C) "Install the Azure File Sync Agent on Server1" & E) "Create a sync group"

Reference: <https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>
upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: BCE

Correct Answer: BCE
upvoted 1 times

  **Dannxx** 2 years, 8 months ago

Selected Answer: BCE

Correct Answer: B, C and E
upvoted 1 times

  **nkhan19** 2 years, 9 months ago

Selected Answer: BCE

Answer is correct
upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

Selected Answer: BCE

BCE is correct
<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>
upvoted 1 times

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group
VNET1	Virtual network	RG1
VNET2	Virtual network	RG2
VM1	Virtual machine	RG2

The status of VM1 is Running.

You assign an Azure policy as shown in the exhibit. (Click the Exhibit tab.)

Home > Policy - Assignments > Assign Policy

Assign Policy

SCOPE

* Scope (Learn more about setting the scope)

Azure Pass/RG2

Exclusions

Optionally select resources to exempt from the policy assignment

BASICS

* Policy definition

Not allowed resource types

* Assignment name ⓘ

Not allowed resource types

Description

Assigned by

First User

PARAMETERS

* Not allowed resource types ⓘ

3 selected

Assign

Cancel

You assign the policy by using the following parameters:

Microsoft.ClassicNetwork/virtualNetworks

Microsoft.Network/virtualNetworks

Microsoft.Compute/virtualMachines

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

	Statements	Yes	No
	An administrator can move VNET1 to RG2	<input type="radio"/>	<input type="radio"/>
	The state of VM1 changed to deallocated	<input type="radio"/>	<input type="radio"/>
	An administrator can modify the address space of VNET2	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

	Statements	Yes	No
	An administrator can move VNET1 to RG2	<input checked="" type="radio"/>	<input type="radio"/>
	The state of VM1 changed to deallocated	<input type="radio"/>	<input checked="" type="radio"/>
	An administrator can modify the address space of VNET2	<input type="radio"/>	<input checked="" type="radio"/>

- bogdan89

Highly Voted

4 years, 5 months ago

Y-N-N tested today in a LAB.
upvoted 217 times
- 58b2872

4 months ago

N- When you move a VM to a RG2, it is like creating a new VM, so the policy will prevent that for sure, no resource's modification or creation is allowed..... Y- VM1 is already created, so it won't get affected in the policy, new creation or modification will not be allowed, not deallocating the existed ones... N since I am modifying something in the resource newly, which is not allowed duo of the policy.... so the suggested answer by EXAMTOPICS is TRUE !!!
upvoted 1 times
- vrm1358

4 months ago

Tested IN lab Jan 2025
N,N,N
upvoted 6 times
- comin

3 years, 10 months ago

The answer is wrong.
Just did the test following the same structure as in the question and the answer they give is correct.

Answer: N Y N

Why wouldn't the VM state change to deallocated? You just can't make changes in the Settings section.
upvoted 9 times
- Mozbius_

3 years, 3 months ago

Policies don't make changes. They only mark already existing resources as non-compliant unless you setup a remediation which is not done by default. Policies affect new resources. I wasn't sure about changes done to already existing resources but it makes sense that policies also apply changes done after applying a policy.

That's a topic found even in AZ-900.
upvoted 10 times
- Mozbius_

3 years, 3 months ago



**that policies also apply to changes done after applying a policy
upvoted 3 times
- Sanaz90

9 months, 1 week ago

His answer is completely incorrect. It's NO NO NO. tested in lab.
upvoted 3 times
- MrJJ10

2 years, 4 months ago

VM1 never changed...its in RG2.....nothing says its connected to VNET1 (VNET1 is RG1)....the policy is set for RG2
upvoted 1 times

  **S3ktar** 3 years, 4 months ago

The answers have been reversed but this is 100% correct.

No - You cannot move a resource into a RG if the resource is restricted in the destination RG

No - The VM will not become deallocated, it will instead be marked as non-compliant

Yes - You can change the VNet address space, even with the virtualnetwork restriction, instead you will be prevented from making ANOTHER VNet and the existing VNet will be marked as Non-Compliant.


Source: Tested it in my Azure Lab

upvoted 139 times

  **aaqibkhan123** 4 months, 2 weeks ago



You cannot change the VNet address space when the 'VM is in running state'.

upvoted 1 times

  **sca88** 5 months, 2 weeks ago

Totally agree with you. NNY

upvoted 1 times

  **2d153f5** 5 months, 2 weeks ago

That's it. And it is clearly explained.

upvoted 1 times

  **idlir** Highly Voted  4 years, 5 months ago

N-N-N

Policy will identify the VM as not compliant but will not put VM in deallocate

upvoted 160 times

  **ostych** 3 years ago

Agreed, tested in a lab.

upvoted 3 times

  **Anon6969** 4 years, 5 months ago

This makes the most sense. Only one I am not sure on is how the policy would modify the change to the address space?

upvoted 4 times

  **prashantjoge** 4 years, 4 months ago

I agree. Existing non-compliant resources can be remediated with a remediation task. But no action is taken against them other than to mark them as non-compliant

upvoted 5 times

  **Baconrind** 3 years, 1 month ago

Agree with N-N-N, trying to move VNET1 to RG2 gives 'disallowed by policy' error after validation checking. Modifying address space fails with 'Failed to save address space changes to virtual network 'VNET2'. Error: Resource 'VNET2' was disallowed by policy. '

upvoted 8 times



  **MrMoris** Most Recent  2 months, 2 weeks ago

N-N-N

Tested in my lab.

lots if comments said that you are able to change the address space even with the policy, but it's not possible. The policy prevents you from doing that!

upvoted 1 times

  **witalis** 5 months, 1 week ago

N- restricted by policy

N - no changes

N - yes, you can make changes on ressources that restricted by policy

upvoted 4 times

  **sca88** 5 months, 2 weeks ago

Answer should be NNY.

The policy don't allow the creation of new resources in RG2 like VM and VNET, but it doesn't affect the already created resources. So 1 and 2 is NO.

The number 3 is YES, because the policy doesn't affect the administrator to edit the resources. Nobody can be create a new VNET, but admin can modify existing one.

upvoted 2 times

  **christovski** 6 months ago


Answer given is correct. N-Y-N

1. I am given the error Resource 'VNET1' was disallowed by policy

2. Virtual Machine deallocated without an issue

3. Error message: Failed to save address space changes to virtual network 'VNET2'. Error: Resource 'VNET2' was disallowed by policy

upvoted 4 times

  **TodRose** 6 months, 1 week ago

The correct answers are:

1. No

2. No

3. No

When you apply a policy that restricts certain resource types (e.g., Microsoft.Network/virtualNetworks and Microsoft.Compute/virtualMachines), it only prevents the creation of new resources of those types after the policy is enforced. Here's how it affects your existing resources:

1. State of VM1 (existing virtual machine):

The existing VM1 will remain unaffected. Azure Policy works as an allow/deny mechanism during the creation or modification of resources. It does not retroactively delete or modify existing resources that were created before the policy was applied. So, VM1 will continue to run normally after the policy is applied.

2. Changing the address space of the VNet:

Since the policy prevents actions on Microsoft.Network/virtualNetworks, you would not be able to modify the address space of the existing VNet. The policy will block updates or changes to the VNet because it restricts actions on resources of that type.

upvoted 2 times

  **kejo2** 7 months ago

Justed tested this in my LAB. The answer is N,N,N
Failed to save virtual network changes
Failed to save address space changes to virtual network 'VNET2'. Error: Resource 'VNET2' was disallowed by policy. Policy identifiers: [{"policyAssignment":{"name":"Not allowed resource types","id":"/subscriptions/4b52c793-3612-4942-a61f-2caf2d665ccf/resourceGroups/RG2/providers/Microsoft.Authorization/policyAssignments/0fa54e46d93e48dd9c72f3a1"}}, {"policyDefinition":{"name":"Not allowed resource

upvoted 3 times

  **Mshaty** 7 months ago

the answer is N_N_Y since the policy restricts creation of new resources and does not affect the resources that already in the resource group

upvoted 3 times

  **[Removed]** 8 months ago

WRONG

No

No

No

upvoted 2 times

  **radouani** 9 months ago


If you are confused about all those comments, The answer is NO, NO, NO, I have just tested on my azure account. When you create the policy, you should give it 10mn at least to show non compliant resources.

1. Resource move policy validation failed. Please see details. Diagnostic information:
Policy identifiers: [{"policyAssignment":{"name":"Not allowed resource types","id":"/subscriptions/.....

2. The VM still running, I thought that it has restarted but no, it is still running

3. Failed to save address space changes to virtual network 'VNET2'. Error: Resource 'VNET2' was disallowed by policy. Policy identifiers: [{"policyAssignment":{"name":"Not allowed resource types".....

upvoted 5 times

  **Surs** 9 months ago

Tried this out.

Answer > NYN

An Administrator can move VNet1 to RG2 > NO
[Error > Resource move policy validation failed. Resource 'VNet1' was disallowed by policy. Policy identifiers: [{"policyAssignment":{"name":"Not allowed resource types"]

The state of VM1 changed to deallocated > YES
[Was able to stop the VM. Was also able to start the VM]

An administrator can modify the address space of VNet2 > NO
[Error > Failed to save address space changes to virtual network 'VNet2'. Error: Resource 'VNet2' was disallowed by policy. Policy identifiers: [{"policyAssignment":{"name":"Not allowed resource types"]

upvoted 3 times

  **Y2** 9 months, 2 weeks ago



N-N-N Tested in lab,
A - Cannot add a V-Net to the RG
B- the VM's status will not be changed to deallocated
C- Cannot modify Address space of V-Net in the RG



upvoted 1 times



  **Jedi_sg2000** 9 months, 3 weeks ago

NYN is the answer

upvoted 1 times

  **23169fd** 11 months, 1 week ago
Correct Answer: N N N
upvoted 2 times

  **varinder82** 11 months, 2 weeks ago
Final Answer : NNY
upvoted 1 times

  **Amir1909** 1 year, 1 month ago
Yes
No
Yes
upvoted 1 times

DRAG DROP -

You have an Azure subscription that contains a storage account.

You have an on-premises server named Server1 that runs Windows Server 2016. Server1 has 2 TB of data.

You need to transfer the data to the storage account by using the Azure Import/Export service.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:

Actions	Answer Area
From the Azure portal, update the import job	
From the Azure portal, create an import job	
Attach an external disk to Server1 and then run waimportexport.exe	⬆
Detach the external disks from Server1 and ship the disks to an Azure data center	⬆

Correct Answer:

Actions	Answer Area
From the Azure portal, update the import job	Attach an external disk to Server1 and then run waimportexport.exe
From the Azure portal, create an import job	From the Azure portal, create an import job
Attach an external disk to Server1 and then run waimportexport.exe	Detach the external disks from Server1 and ship the disks to an Azure data center
Detach the external disks from Server1 and ship the disks to an Azure data center	From the Azure portal, update the import job

At a high level, an import job involves the following steps:

Step 1: Attach an external disk to Server1 and then run waimportexport.exe

Determine data to be imported, number of drives you need, destination blob location for your data in Azure storage.

Use the WAImportExport tool to copy data to disk drives. Encrypt the disk drives with BitLocker.

Step 2: From the Azure portal, create an import job.

Create an import job in your target storage account in Azure portal. Upload the drive journal files.

Step 3: Detach the external disks from Server1 and ship the disks to an Azure data center.

Provide the return address and carrier account number for shipping the drives back to you.

Ship the disk drives to the shipping address provided during job creation.

Step 4: From the Azure portal, update the import job

Update the delivery tracking number in the import job details and submit the import job.

The drives are received and processed at the Azure data center.

The drives are shipped using your carrier account to the return address provided in the import job.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

mlantonis Highly Voted 3 years, 11 months ago

Correct Answer:

Step 1: Prepare the drives (Attach an external disk to Server1 and then run waimportexport.exe)

Step 2: Create an import job (From the Azure portal, create an import job)



Step 3: Ship the drives to the Azure datacenter (Detach the external disks from Server1 and ship the disks to an Azure data center)



Step 4: Update the job with tracking information (From the Azure portal, update the import job)



Reference:



<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-data-to-files?tabs=azure-portal>



<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>
upvoted 583 times



  **Billy2023** 2 years, 3 months ago
Upvote this to get passed the comment for people just looking for a cert.
upvoted 17 times



  **chikorita** 2 years, 2 months ago
upvote this for 10 years of goodluck
upvoted 46 times



  **klasbeatz** 2 years, 7 months ago
Mlantonis for President! Thanks for your reliable answers as always man!
upvoted 36 times



  **Indy429** 1 year, 4 months ago
mlantonis - the mvp of az-104
upvoted 6 times



  **mg** Highly Voted 4 years, 1 month ago
Answer is correct
Step 1: Attach an external disk to Server1 and then run waimportexport.exe
Determine data to be imported, number of drives you need, destination blob location for your data in Azure storage.
Use the WAImportExport tool to copy data to disk drives. Encrypt the disk drives with BitLocker.
Step 2: From the Azure portal, create an import job.
Create an import job in your target storage account in Azure portal. Upload the drive journal files.
Step 3: Detach the external disks from Server1 and ship the disks to an Azure data center.
Provide the return address and carrier account number for shipping the drives back to you.
Ship the disk drives to the shipping address provided during job creation.
Step 4: From the Azure portal, update the import job
Update the delivery tracking number in the import job details and submit the import job.
upvoted 19 times

  **[Removed]** Most Recent 8 months ago
CORRECT
upvoted 2 times



  **MikeMat** 9 months, 1 week ago
Does Create, attach, detach, and then update also work and is correct?
upvoted 1 times



  **jacobc3939** 8 months, 3 weeks ago
I thought the same thing. Chatgpt4 says the same answer as the top comment so im going with that
upvoted 1 times



  **joemiller19762023** 1 year, 2 months ago
mlantonis is good at this for sure.
upvoted 1 times


  **Mehedi007** 1 year, 9 months ago
Attach an external disk to Server1 and then run waimportexport.exe (Prepare the drives),
From the Azure portal, create an import job,
Detach the external disks from Server1 and ship the disks to an Azure data center,
From the Azure portal, update the import job.

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-data-to-files?tabs=azure-portal-preview>
upvoted 2 times

  **Mehedi007** 1 year, 9 months ago
Passed the exam on 26 July 2023. Scored 870. Similar question came.
upvoted 3 times

  **garmatey** 1 year, 11 months ago
So let me get this straight. All this advanced cloud computing stuff and the way they do this is by having people physically mail physical disks to an Azure data center?
upvoted 3 times

  **xRiot007** 1 year, 11 months ago
Yup. Some servers are NEVER allowed to access any external sources, so the only way to create backups is manual. There is also the issue of data sovereignty. Their original motivation was that some data is just too large to transfer over network in a given amount of time, but considering today's speeds, I'd say that unless you have thousands of terabytes of data to transfer, you can probably send it over the network in batches with no problem.
upvoted 2 times

  **SlavaRuski** 1 year, 11 months ago
F this...

upvoted 5 times

  **garmatey** 1 year, 11 months ago

hey thats exactly what i wrote on my notes for this question

upvoted 1 times

  **bassmonster** 1 year, 11 months ago



My exam is tomorrow. i just know i'm gonna fail. The way MS ask the questions irritate me to no ends.

upvoted 4 times

  **eliisiita1** 1 year, 11 months ago

did you pass?

upvoted 1 times

  **Yodao** 1 year, 11 months ago

same question lol, I have exam in 5 hours, lets see lol

upvoted 1 times

  **ArronGC** 2 years ago

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service>

Answer is correct.

upvoted 1 times

  **marcusw526** 2 years ago

How can you update the job before it was created? Were going to update things that don't exist yet now? I want someone to explain to me how this is possibly marked as the "other correct answer"

upvoted 1 times

  **cankayahmet** 2 years ago

On exam today

upvoted 1 times

  **NJTH** 2 years ago

Exactly same question was on todays exam.

(7th April 2023)

upvoted 5 times

  **Gaskonader** 2 years, 1 month ago

On Exam 30/03/2023


upvoted 3 times

  **AzZnLuVaBol** 2 years, 1 month ago

On the Exam 3/29/23.



upvoted 3 times

  **djgodzilla** 2 years, 1 month ago

as described here in detail. 

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service#inside-an-import-job>

upvoted 1 times

  **djgodzilla** 2 years, 1 month ago

 Azure Import job (On-prem to AZ /blob & File)

- Prepare disks (using WAImportexport) On-Prem (only supported on windows devices)
- Create the Job (Provide carrier information + Journal file) + (Dest Region/Storage Account/drop-Off location)
- Ship drives to Microsoft
- Check Job status
- Receive disks back from On-Prem
- Check data in Azure Storage

upvoted 1 times

HOTSPOT -

You have Azure subscription that includes following Azure file shares:

Name	In storage account	Location
share1	storage1	West US
share2	storage1	West US

You have the following on-premises servers:

Name	Folders
Server1	D:\Folder1, E:\Folder2
Server2	D:\Data

You create a Storage Sync Service named Sync1 and an Azure File Sync group named Group1. Group1 uses share1 as a cloud endpoint.

You register Server1 and Server2 in Sync1. You add D:\Folder1 on Server1 as a server endpoint of Group1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
share2 can be added as a cloud endpoint for Group1	<input type="radio"/>	<input type="radio"/>
E:\Folder2 on Server1 can be added as a server endpoint for Group1	<input type="radio"/>	<input type="radio"/>
D:\Data on Server2 can be added as a server endpoint for Group1	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	share2 can be added as a cloud endpoint for Group1	<input type="radio"/>	<input checked="" type="radio"/>
	E:\Folder2 on Server1 can be added as a server endpoint for Group1	<input type="radio"/>	<input checked="" type="radio"/>
	D:\Data on Server2 can be added as a server endpoint for Group1	<input checked="" type="radio"/>	<input type="radio"/>

mlantonis Highly Voted 3 years, 11 months ago

Correct Answer:

Box 1: No
A sync group contains one cloud endpoint, or Azure file share, and at least one server endpoint.

Box 2: No

Azure File Sync does not support more than one server endpoint from the same server in the same Sync Group.

Box 3: Yes
Multiple server endpoints can exist on the same volume if their namespaces are not overlapping (for example, F:\sync1 and F:\sync2) and each endpoint is syncing to a unique sync group.

Reference:

<https://docs.microsoft.com/en-us/answers/questions/110822/azure-file-sync-multiple-sync-directories-for-same.html>
<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>
upvoted 435 times

CheMetto 9 months, 1 week ago
This is correct (NNY). for those one who says the last one is N this is the explanation why it's yes:

You can use file sync also as a hub for different server. Imagine you have 2 server, 1 in japan (A) and 1 in the us (B). On server A, you have a D:

with some data, on Server B, you have D: with some other data. You can sync those different with azure file sync, so all those 2 different data will be synced across those 2 server. You don't need to create a second sync group.

upvoted 1 times

  **Moezey** 3 years, 2 months ago



Both servers are in the same sync group though, so box 3 should be NO yeah ?

upvoted 3 times

  **MarcoEscanor** 2 years, 8 months ago



both service are in the same sync service not in same sync group?

upvoted 1 times

  **z** 2 years, 4 months ago

It has just one sync service and group, so however you say it, there is just one. It means that Box 2 N is against Box 3 Y. The correct answer is NNN.

upvoted 1 times

  **wpestan** 2 years, 3 months ago



end point only 1 - server endpoint of Group1 (end point is AZ side)

upvoted 1 times

  **wpestan** 2 years, 3 months ago

end poing only 1 - server endpoint of Group1 (end point is AZ side)

upvoted 2 times

  **op22233** 1 year ago

I will just want to point out that you can actually have more than one server end point pointing to a single Sync group when we have more than one share drive on a single server, Like in this case , The answer is N,Y,Y. Note E:\folder2 & D:\folder1 are on the same server.

upvoted 1 times

  **alexander_kuruvilla** 2 years, 10 months ago

In case of Box 2 it can be Yes if both the server endpoints are on the same volume. (e.g; F:/folder 1 and F:/ folder 2). Since here it is one two different volumes it is No

upvoted 6 times

  **wpestan** 2 years, 3 months ago

end point only 1 - server endpoint of Group1 (end point is AZ side)

upvoted 1 times

  **moris5121** 2 years, 3 months ago



yup, tested in my lab.

upvoted 5 times

  **boink** Highly Voted  4 years, 5 months ago

NO NO YES



upvoted 144 times

  **Ikrom** 4 years, 4 months ago

That's correct (NO NO YES), because to add another server endpoint from the same server you need to have another sync group...



"Multiple server endpoints can exist on the same volume if their namespaces are not overlapping (for example, F:\sync1 and F:\sync2) and each endpoint is syncing to a unique sync group."

upvoted 27 times

  **shnz03** 3 years, 10 months ago

I agree because I had tested it and sync group does not allow me to add the same registered server again in the endpoint.

upvoted 3 times

  **gitsyn** 4 years, 4 months ago

Answer is correct: NO YES YES



The documentation specifies the samve volume, not server. You can't have two server endpoints on the same volume in one sync group, but in this question, the volumes are D: and E:, so then you can have two server endpoints.

upvoted 6 times

  **JayBee65** 3 years, 11 months ago

"A registered server can support multiple server endpoints, however a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers." - <https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>. This is very specifically about servers not volumes, so No, No, Yes

upvoted 22 times



  **aaa112** 4 years, 4 months ago

But you cannot extend the existing endpoint, so you need to recreate it. Question is about adding Server 2 as an endpoint, but it is already an endpoint. "Once you add a server as an endpoint, you can't add it again."

upvoted 5 times

  **wpestan** 2 years, 3 months ago

end point only 1 - server endpoint of Group1 (end point is AZ side)
upvoted 1 times

  **certW1z** 4 years, 4 months ago

Lab tested ... NO NO YES is correct
confirmation of second que: <https://docs.microsoft.com/en-us/answers/questions/110822/azure-file-sync-multiple-sync-directories-for-same.html>
"Azure File Sync does not support more than one server endpoint from the same server in the same sync group."
upvoted 40 times

  **Jay_D_Lincoln** Most Recent 2 months, 4 weeks ago

A registered server can support multiple server endpoints. However, a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers.

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>
upvoted 1 times

  **[Removed]** 7 months, 4 weeks ago

WRONG

No
No
Yes

upvoted 2 times

  **[Removed]** 8 months ago

WRONG

No
No
No

upvoted 1 times

  **[Removed]** 7 months, 3 weeks ago

please ignore this, i've missread it, it's N N Y
upvoted 1 times

  **23169fd** 11 months, 1 week ago



share2 can be added as a cloud endpoint for Group1:
No: Since Group1 is already using share1 as its cloud endpoint, you cannot add another cloud endpoint (share2) to the same sync group. A sync group can have only one cloud endpoint.
E:\Folder2 on Server1 can be added as a server endpoint for Group1:

Yes: You can add multiple server endpoints from the same server or different servers to the same sync group. Therefore, E:\Folder2 on Server1 can be added as an additional server endpoint for Group1.
D:\Data on Server2 can be added as a server endpoint for Group1:

Yes: You can add server endpoints from different servers to the same sync group. Therefore, D:\Data on Server2 can be added as a server endpoint for Group1
upvoted 2 times

  **23169fd** 11 months, 1 week ago

Correct Answer : N,Y,Y
upvoted 1 times

  **Prashanthk5814** 1 year, 1 month ago

Answer: N N Y

A registered server can support multiple server endpoints, however a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

- No
- No
- Yes

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

Question is explained in <https://www.youtube.com/watch?v=HhhqHeqrcm0>
upvoted 1 times

  **rodrigo2186** 1 year, 8 months ago

N-N-Y
<https://www.youtube.com/watch?v=HhhqHeqrcm0>

upvoted 1 times

🗲️ 👤 **RonZhong** 1 year, 8 months ago

No

No

A registered server can support multiple server endpoints, however a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers.

Yes

upvoted 1 times

🗲️ 👤 **sebadito** 1 year, 8 months ago

This question is quite confusing... it appears in any recent exam?

upvoted 1 times

🗲️ 👤 **ABHISH_** 1 year, 8 months ago

Unlikely. Microsoft removed File Sync from the topics in 2022.

upvoted 1 times

🗲️ 👤 **Mehedi007** 1 year, 9 months ago

NNY

"A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints."

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-sync-group-and-a-cloud-endpoint>

"A registered server can support multiple server endpoints, however a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers."

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-server-endpoint>

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 10 months ago

Not agreed with the following Yes:

E:\Folder2 on Server1 can be added as a server endpoint for group1

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>

A registered server can support multiple server endpoints, however a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers

correct answer:

Box1: No

Box2: No

Box3: Yes

upvoted 2 times

🗲️ 👤 **picho707** 1 year, 10 months ago

Question 2 appears to be => YES. See below:

Server endpoint

A server endpoint represents a specific location on a registered server, such as a folder on a server volume. Multiple server endpoints can exist on the same volume if their namespaces are unique (for example, F:\sync1 and F:\sync2).

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/6-identify-components>

upvoted 3 times

🗲️ 👤 **31c21da** 1 year, 3 months ago

But D:\Folder1 and E:\Foler2 are not on the same volume, so even literally accoding to the sentence it should be N

upvoted 1 times

🗲️ 👤 **nightfxll** 1 year, 11 months ago

1. NO - "A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints."

Source: <https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-sync-group-and-a-cloud-endpoint>

2. NO - "A registered server can support multiple server endpoints, however, a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers."

Source: <https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-server-endpoint-create?tabs=azure-portal>

3. YES - Same source as number 2.

upvoted 2 times

DRAG DROP -

You have an Azure subscription named Subscription1.

You create an Azure Storage account named contosostorage, and then you create a file share named data.

Which UNC path should you include in a script that references files from the data file share? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Values

blob	blob.core.windows.net
contosostorage	data
file	file.core.windows.net
portal.azure.com	subscription1

Answer Area

\\ . \

Correct Answer:

Values

blob	blob.core.windows.net
contosostorage	data
file	file.core.windows.net
portal.azure.com	subscription1

Answer Area

\\ . \

Box 1: contosostorage -

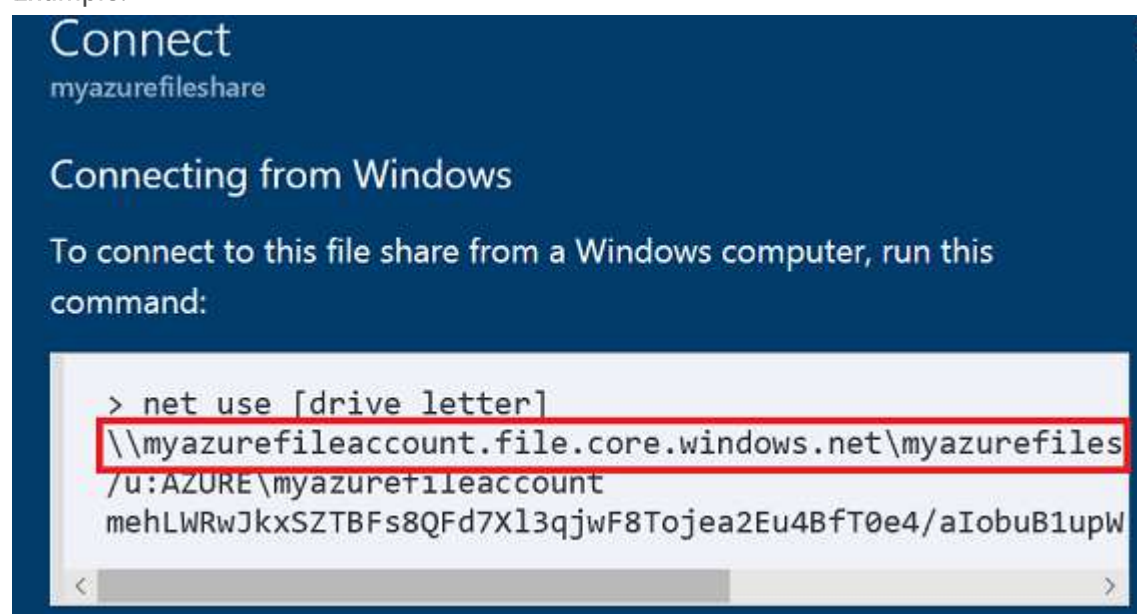
The name of account -

Box 2: file.core.windows.net -

Box 3: data -

The name of the file share is data.

Example:



Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

mlantonis Highly Voted 3 years, 11 months ago



Correct Answer:

[storageaccountname].file.core.windows.net/[FileShareName]

contosostorage.file.core.windows.net\data



Reference:



<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>
upvoted 279 times

  **RougePotatoe** 2 years, 3 months ago
Just in case you wanted to know exactly where to look.
"\\<storageAccountName>.file.core.windows.net\<fileShareName>"



Mount the Azure file share with File Explorer > Step 3



<https://learn.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows#mount-the-azure-file-share-with-file-explorer>
upvoted 7 times



  **Hibs2016** Highly Voted 4 years, 4 months ago
Correct Answer - contosostorage.file.core.windows.net\data.
upvoted 45 times



  **[Removed]** Most Recent 7 months, 4 weeks ago
CORRECT



\\ (Storage Account Name) . (file.core.windows.net) \ (FileShareName)
upvoted 2 times



  **varinder82** 11 months, 3 weeks ago
Final Answer:
[storageaccountname].file.core.windows.net/[FileShareName]
contosostorage.file.core.windows.net\data
upvoted 1 times



  **Amir1909** 1 year, 2 months ago
- contosostorage
- file.core.windows.net
- data
upvoted 1 times



  **AVATAR_AANG7** 1 year, 7 months ago
This was on my exam 7/15/23
upvoted 4 times

  **Pakawat** 1 year, 10 months ago
Found this Q in the exam, 3/7/23
upvoted 5 times

  **MHguy** 1 year, 9 months ago
confirmed.it's there
upvoted 2 times



  **Mpalana** 1 year, 11 months ago
This question was on exam 8June 2023
upvoted 4 times



  **habbey** 2 years ago
Answer is contosostorage.file.core.windows.net\data
upvoted 4 times

  **AK4U_111** 2 years, 2 months ago
Given answer is incorrect

correct answer:
\\contosostorage.file.core.windows.net\data

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>
upvoted 1 times

  **Ashfaque_9x** 2 years, 3 months ago
Passed today on 29Jan23 with a score of 970. This question was in the exam.
Correct Answer: contosostorage.file.core.windows.net\data
upvoted 5 times

  **[Removed]** 2 years, 3 months ago
this was on the test
upvoted 3 times

🗒️ 👤 **kapurg** 2 years, 6 months ago
1. contosostorage 2. file.core.windows.net 3. data
upvoted 2 times

🗒️ 👤 **NaoVaz** 2 years, 7 months ago
1) contosostorage
2) file.core.windows.net
3) data

Reference: <https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows#mount-the-azure-file-share-with-file-explorer>
upvoted 4 times

🗒️ 👤 **EmnCours** 2 years, 8 months ago
1. contosostorage
2. file.core.windows.net
3. data
upvoted 2 times

🗒️ 👤 **manalshowaei** 2 years, 10 months ago
\\contosostorage.file.core.windows.net\data
upvoted 1 times

🗒️ 👤 **benvdw** 3 years, 1 month ago
on exam 13/3/2022
upvoted 11 times

HOTSPOT -

You have an Azure subscription that contains an Azure Storage account.
You plan to copy an on-premises virtual machine image to a container named vmimages.
You need to create the container for the planned image.
Which command should you run? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

azcopy

▼

make

sync

copy

'https://mystorageaccount.'

▼

blob

dfs

queue

table

images

file

.core.windows.net/vmimages'

Answer Area

azcopy

▼

make

sync

copy

'https://mystorageaccount.'

▼

blob

dfs

queue


table

images

file

.core.windows.net/vmimages'

Correct Answer:


 **mlantonis** Highly Voted 3 years, 11 months ago
Correct Answer:

azcopy make 'https://mystorageaccount.blob.core.windows.net/vmimages'

Similar to OS Images, a VM Image is a collection of metadata and pointers to a set of VHDs (one VHD per disk) stored as page blobs in Azure Storage.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-make>
upvoted 288 times

 **Juwizee** 1 year, 6 months ago
Say No More... The man himself got it again.
upvoted 9 times

 **RougePotatoe** 2 years, 3 months ago

In case yall wanted to know where they got the quote from. You could've just googled it.

"Similar to OS Images, a VM Image is a collection of metadata and pointers to a set of VHDs (one VHD per disk) stored as page blobs in Azure Storage."



<https://azure.microsoft.com/en-us/blog/vm-image-blog-post/>
upvoted 9 times

  **garmatey** 1 year, 12 months ago

"You could've just googled it."

Um are you getting indignant over some imaginary person asking where some quote is from?

upvoted 9 times

  **tigerz** 1 year, 8 months ago

It must be nice being on such a high horse over us peasants.

upvoted 2 times

  **Tom900** Highly Voted 4 years, 4 months ago

Correct Answer. Similar to OS Images, a VM Image is a collection of metadata and pointers to a set of VHDs (one VHD per disk) stored as page blobs in Azure Storage

upvoted 41 times

  **Hibs2016** 4 years, 4 months ago

Agree correct answer - make, blob

upvoted 18 times

  **[Removed]** Most Recent 8 months ago

CORRECT

upvoted 2 times

  **tashakori** 1 year, 1 month ago

Given answer is correct

upvoted 1 times

  **Amir1909** 1 year, 2 months ago



Correct

upvoted 1 times

  **Kverma7** 1 year, 8 months ago



This was in Exam 23-08-23

upvoted 6 times

  **MHguy** 1 year, 9 months ago

Found this in the exam (july 2023)

upvoted 4 times

  **Pakawat** 1 year, 10 months ago



Found this Q in the exam, 3/7/23

upvoted 4 times

  **Brockssn** 2 years, 1 month ago

This one annoys me. Why would you upload a vm image to a blog and not file? You can mount virtual machine images from File storage during creation, you can't do that with Blobs. Why would we chose something specific to VHDs and put it somewhere you can't use it... when the place that we can use is available as an option?

upvoted 4 times

  **rodrod** 6 months, 1 week ago

it's an exam question, nothing to overthink, the question is about container, so file is not an option

upvoted 1 times

  **gauravit43** 2 years, 2 months ago

I passed my exam on 4th March,2023 and this question appeared in the exam. Correct Answer is copy and blob

upvoted 9 times

  **AK4U_111** 2 years, 2 months ago

Correct. Tested in lab

upvoted 3 times

  **keszi** 2 years, 2 months ago

Question was on the exam March 2023

upvoted 4 times

  **vbohr899** 2 years, 2 months ago

Cleared Exam today 26 Feb, This question was there in exam.

upvoted 2 times

🗒️ 👤 **myarali** 2 years, 2 months ago
azcopy make [resourceURL] [flags]

azcopy make "https://[account-name].[blob,file,dfs].core.windows.net/[top-level-resource-name]"

So Correct Answer:

azcopy make 'https://mystorageaccount.blob.core.windows.net/vmimages'

Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-make?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json>
upvoted 4 times

🗒️ 👤 **Ashfaque_9x** 2 years, 3 months ago

Passed today on 29Jan23 with a score of 970. This question was in the exam.

Correct Answer:

azcopy make 'https://mystorageaccount.blob.core.windows.net/vmimages'

upvoted 8 times

🗒️ 👤 **MothePro** 2 years, 1 month ago

how helpful was examtopics in the exam? what percentage of Q's came from it?

upvoted 1 times

🗒️ 👤 **typales2005** 2 years, 3 months ago

was on test 09/01/2023. "make"/ "blob"

upvoted 4 times

🗒️ 👤 **NaoVaz** 2 years, 7 months ago

1) make

2) blob

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-make>

upvoted 5 times

HOTSPOT -

You have an Azure File sync group that has the endpoints shown in the following table.

Name	Type
Endpoint1	Cloud endpoint
Endpoint2	Server endpoint
Endpoint3	Server endpoint

Cloud tiering is enabled for Endpoint3.

You add a file named File1 to Endpoint1 and a file named File2 to Endpoint2.

On which endpoints will File1 and File2 be available within 24 hours of adding the files? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

File1:

▼

Endpoint1 only

Endpoint3 only

Endpoint2 and Endpoint3 only

Endpoint1, Endpoint2, and Endpoint3

File2:

▼

Endpoint2 only

Endpoint3 only

Endpoint2 and Endpoint3 only

Endpoint1, Endpoint2, and Endpoint3

Answer Area

Correct Answer:

File1:

▼

Endpoint1 only

Endpoint3 only

Endpoint2 and Endpoint3 only

Endpoint1, Endpoint2, and Endpoint3

File2:

▼

Endpoint2 only

Endpoint3 only

Endpoint2 and Endpoint3 only

Endpoint1, Endpoint2, and Endpoint3

 **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

File1: Endpoint1 only

It is a cloud endpoint, and it is scanned by the detection job every 24 hours.

File2: Endpoint1, Endpoint2 and Endpoint3

With the on-premises servers the file is scanned and synced automatically after it's being added.

Note: They changed the question in Exam from "within 24 hours" to "after 24 hours".

So, the answer is:

File1: Endpoint1, Endpoint2 and Endpoint3

File2: Endpoint1, Endpoint2 and Endpoint3



Reference:



<https://docs.microsoft.com/en-us/learn/modules/extend-share-capacity-with-azure-file-sync/2-what-azure-file-sync>
upvoted 757 times



 **codeScalable** 2 years, 6 months ago



God bless you @mlantonis. You are a real gem




upvoted 18 times



  **suriyaswamy** 3 years, 8 months ago
Good Info
upvoted 3 times



  **Harshul** 3 years, 10 months ago
Excellent Explanation!
upvoted 4 times



  **juniorccs** 3 years, 9 months ago
Thanks a lot!
upvoted 2 times



  **AubinBakana** 3 years, 8 months ago
Thank you so much. That's something I thought was a little confusing as it would make their revealed answer wrong.
upvoted 3 times



  **Skankhunt** Highly Voted  4 years, 4 months ago
Should be File 1: Endpoint 1 only File 2: Endpoint 1, Endpoint 2 and Endpoint 3
upvoted 57 times




  **prashantjoge** 4 years, 4 months ago
This is correct. Confirmed it in labs
upvoted 3 times

  **xMilkyMan123** 3 years, 10 months ago
Tell me what exactly you did in your Lab
upvoted 2 times

  **janshal** 4 years, 4 months ago
you waited 24 hour for the job to be sync?
I think the answer is all endpoints because the syc job run every 24 hour so even if your created the file a second after the sync jobs started it will be sync within 24 hours
upvoted 16 times



  **vince60370** 4 years, 3 months ago
Not agree. Please read MLM0607's answer below.
upvoted 2 times



  **JayBee65** 3 years, 11 months ago
LM0607's answer are File 1: Endpoint 1 only File 2: Endpoint 1, Endpoint 2 and Endpoint 3!
upvoted 7 times



  **[Removed]** Most Recent  8 months ago
WRONG



Keyword (within 24 h)
File1: Endpoint1 only
File2: Endpoint1, Endpoint2 and Endpoint3









Keyword (after 24 h)
File1: Endpoint1, Endpoint2 and Endpoint3
File2: Endpoint1, Endpoint2 and Endpoint3
upvoted 6 times

  **varinder82** 11 months, 2 weeks ago
Final Answer: (key- within 24 hrs)
File1: Endpoint1 only
File2: Endpoint1, Endpoint2 and Endpoint3
upvoted 1 times

  **tashakori** 1 year, 1 month ago
File1: Endpoint1, Endpoint2 and Endpoint3
File2: Endpoint1, Endpoint2 and Endpoint3
upvoted 2 times

  **Amir1909** 1 year, 2 months ago
- Endpoint1, Endpoint2 and Endpoint3
- Endpoint1, Endpoint2 and Endpoint3
upvoted 1 times

  **nandakku** 1 year, 7 months ago
This Question appeared in Exam attended in September 15th.
Corredt answer is File 1 -----> Endpoint 1 only - Becuase question mentioned "within 24 hours".
File 2 -----> Endpoint 1,2 and 3
upvoted 4 times









-   **Mitazure7** 1 year, 7 months ago
What's going on within 24 hours?
upvoted 1 times
-   **rodrigo2186** 1 year, 8 months ago
https://www.youtube.com/watch?v=_Dv5HrAqsn4
upvoted 7 times
-   **Josete1106** 1 year, 9 months ago
File1: Endpoint1 only
File2: Endpoint1, Endpoint2 and Endpoint3
upvoted 1 times
-   **Madbo** 2 years ago
File1:
Answer: a. Endpoint1 only

Explanation:



File1 is added to Endpoint1 which is a cloud endpoint.
Cloud tiering is enabled for Endpoint3 but it is not guaranteed that the file will be tiered within 24 hours.
Therefore, File1 will only be available on Endpoint1 within 24 hours.

File2:
Answer: d. Endpoint1, Endpoint2, and Endpoint3



Explanation:

File2 is added to Endpoint2 which is a server endpoint.
Azure File Sync syncs files between all endpoints in the sync group.
Therefore, File2 will be available on Endpoint1, Endpoint2, and Endpoint3 within 24 hours.
upvoted 4 times
-   **Exilic** 2 years ago
If the question was changed to after 24 hours, Why has Examtopics not changed the question also?
upvoted 2 times
-   **orionduo** 2 years, 3 months ago
File1: Endpoint1 only
It is a cloud endpoint, and it is scanned by the detection job every 24 hours.
Note: They changed the question in Exam from "within 24 hours" to "after 24 hours".
So, the answer is:
File1: Endpoint1, Endpoint2 and Endpoint3
upvoted 2 times
-   **KeerthiVasanG** 2 years, 6 months ago
Azure Files doesn't have change notification or journaling yet, so Azure File Sync has a scheduled job called a change detection job. This job is initiated every 24 hours. That means that if you change a file in the Azure file share, you might not see the change on the on-premises file share for up to 24 hours.
upvoted 6 times
-   **NaoVaz** 2 years, 7 months ago
1) "Endpoint1 only"
2) "Endpoint1, Endpoint2, and Endpoint3"

Files added to the Cloud Endpoint are scanned every 24 hours.
With the rest of the server endpoints files are synced automatically.

Reference: <https://docs.microsoft.com/en-us/training/modules/extend-share-capacity-with-azure-file-sync/2-what-azure-file-sync>
upvoted 5 times
-   **EmnCours** 2 years, 8 months ago
File1: Endpoint1 only
It is a cloud endpoint, and it is scanned by the detection job every 24 hours.

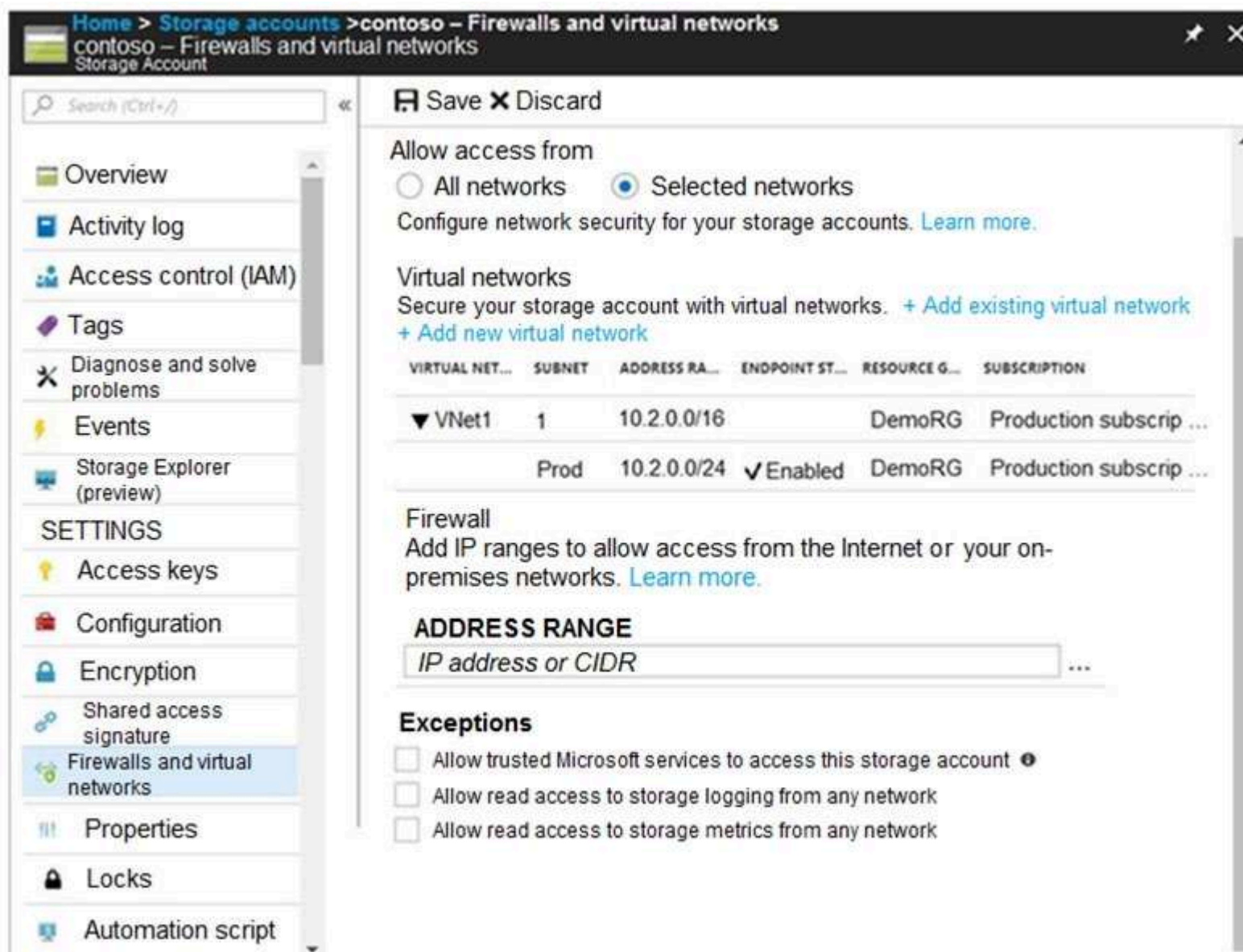
File2: Endpoint1, Endpoint2 and Endpoint3
With the on-premises servers the file is scanned and synced automatically after it's being added.

Note: They changed the question in Exam from "within 24 hours" to "after 24 hours".
So, the answer is:
File1: Endpoint1, Endpoint2 and Endpoint3
File2: Endpoint1, Endpoint2 and Endpoint3
upvoted 9 times
-   **pari205** 2 years, 9 months ago
Why correct answers are not updated in the main pages? isn't misleading
upvoted 9 times

HOTSPOT -

You have several Azure virtual machines on a virtual network named VNet1.

You configure an Azure Storage account as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account **[answer choice]**.

	▼
always	
during a backup	
never	

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account **[answer choice]**.

	▼
always	
during a backup	
never	

Correct Answer:

Answer Area

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account [answer choice].

always

during a backup

never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account [answer choice].

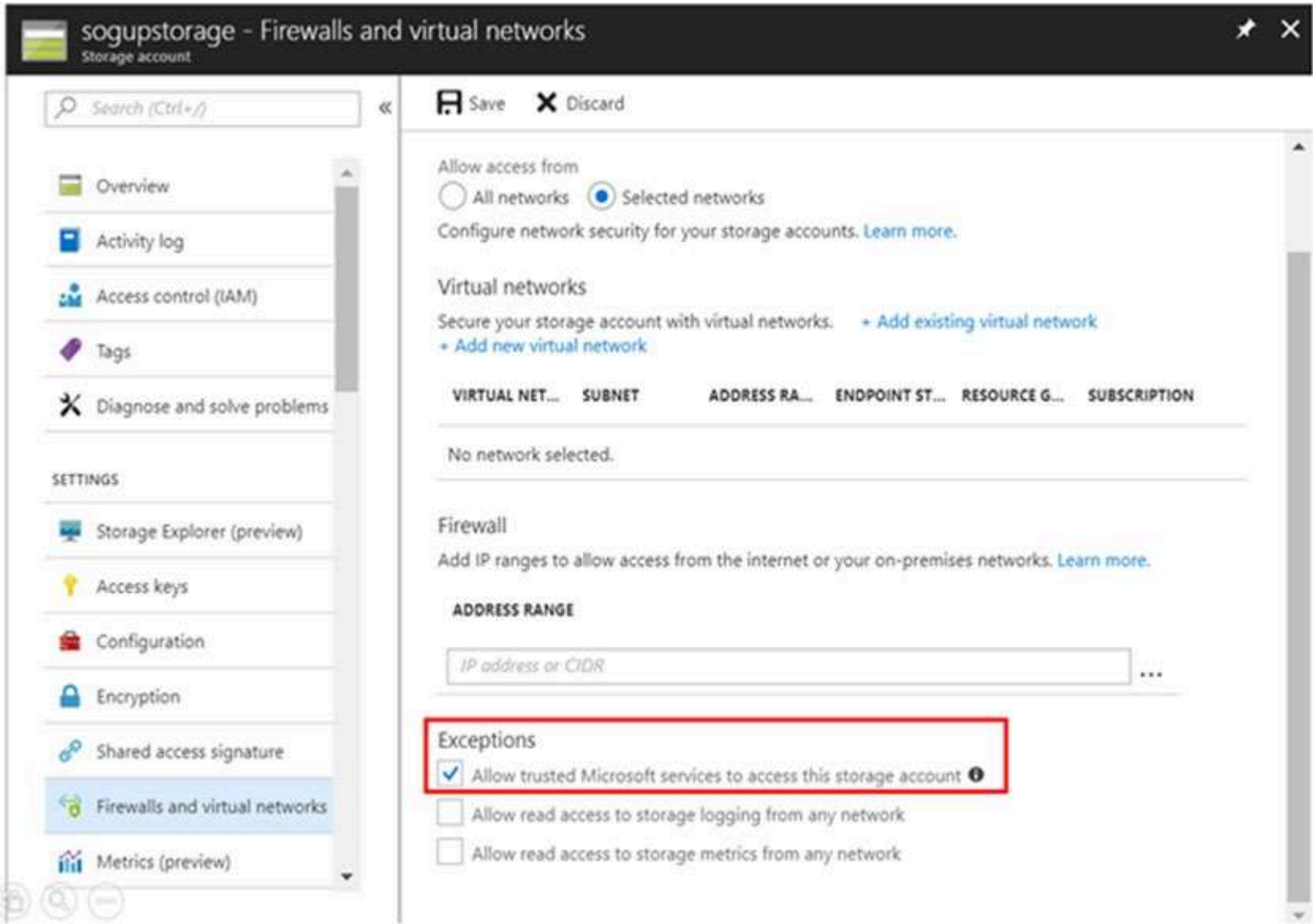
always

during a backup

never

Box 1: never -
The 10.2.9.0/24 subnet is not whitelisted.

Box 2: never -
After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.



Reference:
<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows> <https://azure.microsoft.com/en-us/blog/azure-backup-now-supports-storage-accounts-secured-with-azure-storage-firewalls-and-virtual-networks/>

mlantonis Highly Voted 3 years, 11 months ago
Correct Answer:

VNet1's address space is 10.2.0.0/16.
The VNet1 has only 1 Subnet associated: 10.2.0.0/24. The address space of a VNet is irrelevant if there isn't a corresponding Subnet from, which VMs can be assigned IP addresses.

Box1: Never
VMs from 10.2.9.0/24 (10.2.9.0 - 10.2.9.255) are out of Subnet.
Subnet IP range 10.2.0.0 - 10.2.0. 255.

Box2: Never
Since the checkbox to allow trusted Microsoft services is not checked. After you configure firewall and virtual network settings for your storage

account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.

upvoted 421 times

  **RougePotatoe** 2 years, 3 months ago

Their quote "After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account."

Section: "Getting started"

<https://azure.microsoft.com/en-us/blog/azure-backup-now-supports-storage-accounts-secured-with-azure-storage-firewalls-and-virtual-networks/>

upvoted 5 times

  **Leandroalonso** Highly Voted 4 years, 5 months ago

VMs from the 10.2.9.0/24 should NEVER access the storage!!!!

Since with the selection of the network is segmented by subnets, and not by virtual networks.

upvoted 76 times

  **Miles19** 4 years, 1 month ago

Yes, that's true. The virtual machine attached to the following virtual network 10.2.9.0/24 will never have access to the storage account, because of the firewall rules, so the correct answer is:

-Never


-Never

upvoted 19 times

  **besha** 4 years ago



Technically 10.2.9.0/24 subnet is part of 10.2.0.0/16 subnet which is in the allowed subnet. but should still be Never because it's Endpoint status is not enabled

upvoted 40 times

  **RamanAgarwal** 3 years, 11 months ago


Allowed access is at the subnet level which is 10.2.0.0/24 which includes Ip range 10.2.0.0-10.2.0.255, this means the VM on 10.2.9.0/24 will not have access to storage account.

upvoted 20 times

  **shnz03** 3 years, 10 months ago

I disagree. Your subnet mask understanding for network id and host id is wrong.

upvoted 4 times

  **shnz03** 3 years, 10 months ago


@RamanAgarwal. I apologize. I misread. Your statement is correct.

upvoted 12 times

  **[Removed]** Most Recent 8 months ago

CORRECT

upvoted 2 times

  **76d5e04** 11 months ago

The question tricks with IP address. The Vnet1 address space 10.2.0.0/16 and the VM address space 10.2.9.0/24 are different. So the VM will never be able to connect

upvoted 1 times

  **ihar_akhremchyk** 1 year ago

Incorrect case at all. How did they create subnet "1" with CIDR 10.2.0.0/16 and subnet "Prod" with CIDR 10.2.0.0/24 in one Vnet1? It's impossible to do because of overlapping of the subnets.

If you decide to repeat the test case you will receive an error - "Address prefix 10.2.0.0/24 overlaps with the address prefix 10.2.0.0/16 in subnet default. Subnets in the same virtual network cannot overlap."

upvoted 2 times

  **bobothewiseman** 1 year, 1 month ago

Never Never

10.2.9.0/24 subnet is part of 10.2.0.0/16 subnet which is in the allowed subnet. The reasons it's now allowed is because the Endpoint status is not enabled

upvoted 1 times

  **bobothewiseman** 1 year, 1 month ago

correction - *not allowed

upvoted 1 times

  **1828b9d** 1 year, 2 months ago

This question was in exam 01/03/2024

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

Always

Never

upvoted 1 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago

Correct Never Never

upvoted 1 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago

- always

- always

upvoted 1 times

🗨️ 👤 **SkyZeroZx** 1 year, 3 months ago

VNet1's address space is 10.2.0.0/16.

The VNet1 has only 1 Subnet associated: 10.2.0.0/24. The address space of a VNet is irrelevant if there isn't a corresponding Subnet from, which VMs can be assigned IP addresses.

Box1: Never

VMs from 10.2.9.0/24 (10.2.9.0 - 10.2.9.255) are out of Subnet.

Subnet IP range 10.2.0.0 - 10.2.0. 255.

Box2: Never

Since the checkbox to allow trusted Microsoft services is not checked. After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.

upvoted 1 times

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

This question appeared in Exam conducted on September 15th - 2023. Answer is,

Box 1 -----> Never (Check the CIDR range mentioned. Question contains wrong IP address)

Box 2 -----> Checkbox to allow trusted Microsoft services is not checked.

upvoted 3 times

🗨️ 👤 **Chris1120** 1 year, 8 months ago

Never! Never!

upvoted 1 times

🗨️ 👤 **Madbo** 2 years ago

It seems that the virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account as the subnet "Prod" is enabled with endpoints to access the storage account. Therefore, the answer to the first question should be "always".

As for the second question, if the Azure Backup service is configured to access the storage account as an exception, it should be able to back up the unmanaged hard disks of the virtual machines in the storage account. However, if the exception is not configured, the answer should be "never".

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 3 months ago

on the test

upvoted 2 times

🗨️ 👤 **UK7** 2 years, 4 months ago

On exam 21st Dec 2022 - answer is correct

upvoted 7 times

🗨️ 👤 **NaoVaz** 2 years, 7 months ago

1) The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account "never".

2) Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account "never".

Explanation:

The range 10.2.9.0/24 is not inside the allowed Virtual networks range "10.2.0.0/24".

The option "Allow trusted Microsoft services to access this storage account" is not enabled, so Azure Backup wont be able to back up the disks.

upvoted 2 times

HOTSPOT -

You have a sync group named Sync1 that has a cloud endpoint. The cloud endpoint includes a file named File1.txt. Your on-premises network contains servers that run Windows Server 2016. The servers are configured as shown in the following table.

Name	Share	Share contents
Server1	Share1	File1.txt, File2.txt
Server2	Share2	File2.txt, File3.txt

You add Share1 as an endpoint for Sync1. One hour later, you add Share2 as an endpoint for Sync1. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.	<input type="radio"/>	<input type="radio"/>
On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.	<input type="radio"/>	<input type="radio"/>
File1.txt from Share1 replicates to Share2.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.	<input type="radio"/>	<input checked="" type="radio"/>
	On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.	<input type="radio"/>	<input checked="" type="radio"/>
	File1.txt from Share1 replicates to Share2.	<input checked="" type="radio"/>	<input type="radio"/>

- boink** Highly Voted

4 years, 5 months ago

NO NO YES

upvoted 238 times
- Constantinos**

4 years, 4 months ago

tested on LAB and agree

upvoted 13 times
- prashantjoge**

4 years, 4 months ago

Agreed... tested it myself

upvoted 10 times
- allray15**

4 years, 1 month ago

came in exam today 3/24/21, passed 850+ score always check discussion for correct answers. answered n,n,y

upvoted 71 times
- jjj554**

4 years, 1 month ago

Did most of the questions come from this list?

upvoted 4 times
- cdc_jr3150**

3 years, 11 months ago

what else did you use to study? having a hard time passing.

upvoted 6 times
- Tinez**

2 years, 3 months ago

I hope you have finally passed now.

upvoted 5 times

🗨️ 👤 **Roy010** 1 year, 10 months ago
And I hope you have finally passed now
upvoted 2 times

🗨️ 👤 **alverdiyev91** 1 year, 4 months ago
and I hope you passed now too
upvoted 1 times

🗨️ 👤 **JannisJannisJannis** 1 year, 8 months ago
I hope you have finally passed now too
upvoted 1 times

🗨️ 👤 **sprons77** Highly Voted 👍 4 years, 4 months ago
Agree, files are never overwritten. If the file exists, it will get a new name on the endpoint (file1(1).txt)
upvoted 136 times

🗨️ 👤 **hateit** 3 years, 1 month ago
thanks
upvoted 1 times

🗨️ 👤 **memo454** 1 year, 8 months ago
2.File storage:

- az support
- Support ZRS
- Support persistent storage.
- supports identity-based authentication over Server Message Block (SMB) through on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).
- Not support archive
- Not support condition
- No support Object Replication
- No support Lifecycle management policies
- no support encryption scope
- File share Supports Premium file shares (FileStorage), Premium LRS/ZRS for SMB Multichannel
- Only Shared Access Signature (SAS)
- Import supports Azure Blob storage and Azure File storage
- Premium file shares
- File Storage: Only Shared Access Signature (SAS) token is supported.
- The SAS token is not supported in mounting Azure File share currently, it just supports the Azure storage account key.
- "net use" where it uses SMB. The SMB (Server Message Broker) protocol does not support SAS File storage

upvoted 5 times

🗨️ 👤 **memo454** 1 year, 8 months ago
Pass the exam on 11 August 2023 with 909, Below are some of the notes that may help for Blob and file storage:
A. Blob Storage:
1-Archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. Only storage accounts that are configured for LRS, GRS, or RA-GRS support moving blobs to the archive tier.
2-Import supports Azure Blob storage and Azure File storage
3 -Export supports Azure Blob storage
4-support Lifecycle management policies. Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.
5-Object Replication supports General Purpose V2 and Premium Blob accounts.
6-Support both Azure (AD) and SAS (Shared Access Signature) token.
upvoted 13 times



🗨️ 👤 **memo454** 1 year, 8 months ago
A. Blob Storage: Continue
7-Support conditions when added to built-in or custom role assignments that have blob storage or queue storage data actions
8-Encryption scopes support a container or an individual blob
9-Not Support ZRS
10-az support
11-support stored access policies
12-Tieing is supporting only or block blobs
13-Flow logging for Blob Storage accounts has a retention period of 30 days. General Purpose v2 (GPv2) storage accounts instead, which support flow logging with a retention period of up to 365 days.
upvoted 9 times

🗨️ 👤 **imartinez** 3 years, 9 months ago
ok then, if your statement is correct, the 3rd is ambiguous, since you will have file1.txt and file1(1).txt on the cloud endpoint and after 24 hours, you will have both on Share2, true, but the one named file1.txt it's the original one we had on the cloud endpoint
upvoted 2 times

🗨️ 👤 **Traian** 2 years, 7 months ago
The third one is Yes as the question asks if the file replicates nothing about the name of the file post-replication. And you are right about the naming:
"If the same file is changed on two servers at approximately the same time, what happens?
Azure File Sync uses a simple conflict-resolution strategy: we keep both changes to files that are changed in two endpoints at the same time. The most recently written change keeps the original file name. The older file (determined by LastWriteTime) has the endpoint name and the

conflict number appended to the filename. For server endpoints, the endpoint name is the name of the server. For cloud endpoints, the endpoint name is Cloud. The name follows this taxonomy:"

upvoted 11 times

  **itgg11** 3 years, 4 months ago

I just tested in the lab and files are not overwritten. File that is older will get name of the hosting server added. for example: srv01 creates a new version of "file1" so older version (hosted on srv02) gets renamed to "file1-srv02"

upvoted 17 times

  **JustinYoo** Most Recent 4 months, 2 weeks ago

Why is "file1.txt from share1 replicates to share2" Yes?



upvoted 3 times

  **[Removed]** 8 months ago

WRONG



No
No
Yes

upvoted 2 times

  **varinder82** 11 months, 3 weeks ago



Final Answer:
- No
- No
- Yes

upvoted 2 times

  **Amir1909** 1 year, 2 months ago



- No
- No
- Yes

upvoted 1 times

  **SkyZeroZx** 1 year, 3 months ago



NO NO YES
Agree, files are never overwritten. If the file exists, it will get a new name on the endpoint (file1(1).txt)

upvoted 3 times

  **nandakku** 1 year, 7 months ago


This question appeared on exam 15/09/2023
Correct answer is -----> N - N - Y

upvoted 3 times

  **Prasis** 1 year, 7 months ago

N, N, Y

upvoted 1 times

  **Prasis** 1 year, 7 months ago



N, N, Y
https://www.youtube.com/watch?v=mVPXuVLSS9w&list=PLIKA5U_Yqgof3H0YWhzvarFixW9QLTr4S&index=63

upvoted 3 times

  **rodrigo2186** 1 year, 8 months ago

N-N-Y <https://www.youtube.com/watch?v=mVPXuVLSS9w>

upvoted 1 times

  **Teroristo** 1 year, 9 months ago


Answer is NO, NO, YES:

Azure File Sync uses a simple conflict-resolution strategy: we keep both changes to files that are changed in two endpoints at the same time. The most recently written change keeps the original file name. The older file (determined by LastWriteTime) has the endpoint name and the conflict number appended to the filename. For server endpoints, the endpoint name is the name of the server. For cloud endpoints, the endpoint name is Cloud. The name follows this taxonomy:

(FileNameWithoutExtension)-(endpointName)[-#].

Reference:
<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning>

upvoted 8 times

  **go4adil** 1 year, 3 months ago

Agreed.

Answer is NO, NO, YES:

Azure File Sync uses a simple conflict-resolution strategy: we keep both changes to files that are changed in two endpoints at the same time. The most recently written change keeps the original file name. The older file (determined by LastWriteTime) has the endpoint name and the

conflict number appended to the filename. For server endpoints, the endpoint name is the name of the server. For cloud endpoints, the endpoint name is Cloud. The name follows this taxonomy:

(FileNameWithoutExtension)-(endpointName)[-#].

Below reference more accurately reflects the situation:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-faq>

upvoted 2 times

  **Josete1106** 1 year, 9 months ago

NO NO YES



upvoted 1 times

  **ExamKiller020** 1 year, 10 months ago

All Sync Server related questions were removed after October 2022

ref: <https://intunedin.net/2022/10/11/exam-az-104-microsoft-azure-administrator-resource-guide-october-2022-update/>

upvoted 9 times

  **JWS80** 1 year, 9 months ago

These questions need to be updated when things are removed

upvoted 1 times

  **etrop** 8 months, 4 weeks ago

Ah! thanks man! I will never use this product as a Devops engineer so I'm glad I don't have to spend more time on this.

upvoted 1 times

  **d008454** 1 year, 10 months ago

YES YES YES

upvoted 1 times

  **ppolychron** 1 year, 11 months ago

NNY

Source: <https://learn.microsoft.com/en-us/azure/storage/files/storage-files-faq#azure-file-sync>

Azure File Sync uses a simple conflict-resolution strategy: keep both changes to files that are changed in two endpoints at the same time. The most recently written change keeps the original file name. The older file (determined by LastWriteTime) has the endpoint name and the conflict number appended to the file name. For server endpoints, the endpoint name is the name of the server. For cloud endpoints, the endpoint name is Cloud. The name follows this taxonomy:

<FileNameWithoutExtension>-<endpointName>[-#].<ext>

upvoted 4 times

  **Madbo** 2 years ago

On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.

YES

On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.

NO

File1.txt from Share1 replicates to Share2

NO

When Share1 is added as an endpoint for Sync1, File1.txt from Share1 will overwrite the existing File1.txt on the cloud endpoint because it has the same name. Therefore, the answer to the first statement is YES.

However, when Share2 is added as an endpoint for Sync1, File1.txt from Share1 will not replicate to Share2 because it has not been modified or added since the last sync session. Therefore, the answer to the third statement is NO.

Since the file on the cloud endpoint is being overwritten by the one in Share1, the answer to the second statement is NO, as it indicates that the file in Server1 is being overwritten by the one on the cloud endpoint.

upvoted 1 times

  **xRiot007** 1 year, 11 months ago

Syncing does not everride, it will copy the second file and suffix it with (1). For the 3rd box, the answer is Yes.

upvoted 2 times

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Kind	Performance	Replication	Access tier
storage1	Storage (general purpose v1)	Premium	Geo-redundant storage (GRS)	None
storage2	StorageV2 (general purpose v2)	Standard	Locally-redundant storage (LRS)	Cool
storage3	StorageV2 (general purpose v2)	Premium	Read-access geo-redundant storage (RA-GRS)	Hot
storage4	BlobStorage	Standard	Locally-redundant storage (LRS)	Hot

You need to identify which storage account can be converted to zone-redundant storage (ZRS) replication by requesting a live migration from Azure support.



What should you identify?


- A. storage1
- B. storage2
- C. storage3
- D. storage4

Correct Answer: B



Community vote distribution



B (100%)

-   **diligent176**



Highly Voted 

 4 years, 4 months ago



This is one of those ridiculous questions that would imply we should memorize the 50 different combinations of storage type, replication type, versus live migration support. Useless info to keep in your head, why would they test for this. The support rules around live migration support are horrendous. Bleh.
upvoted 315 times
-   **balflearchen** 4 years, 3 months ago



Complain here is useless. And from your point of view, all certificate exams should be ridiculous.
Back to the question, answer B is correct.
"Live migration is supported only for storage accounts that use LRS or GRS replication. If your account uses RA-GRS, then you need to first change your account's replication type to either LRS or GRS before proceeding. This intermediary step removes the secondary read-only endpoint provided by RA-GRS before migration."
"ZRS supports general-purpose v2 accounts only"
upvoted 65 times
-   **rawrkadia** 3 years, 10 months ago



Most certificate exams **are** ridiculous. Hardly an extreme take.
upvoted 20 times



  **etrop** 8 months, 4 weeks ago

K8s exams are not rediculous, hands on and prove real skills
upvoted 4 times

  **rodrod** 6 months, 1 week ago

I agree!! CKAD exam really makes sense!
upvoted 1 times
-   **juniorccs** 3 years, 9 months ago

100% agree
upvoted 7 times
-   **moota** 3 years, 10 months ago

I agree. Most Azure certification exams are ridiculous.
upvoted 24 times
-   **itz4web** 3 years, 1 month ago

Is it even possible to create "Storage3" Premium as GRS ?
upvoted 1 times

🗄️ 👤 **fedztetz** Highly Voted 👍 4 years, 4 months ago

Answer is correct. It is storage2.
The key to the answer in this question is "Live migration"
- You can do Live migration to ZRS from LRS or GRS only.
- Also this only applies on General Purpose v2 storage.
upvoted 145 times

🗄️ 👤 **kilowd** 2 years, 11 months ago

Live migration is supported only for storage accounts that use LRS or GRS replication. If your account uses RA-GRS, then you need to first change your account's replication type to either LRS or GRS before proceeding. This intermediary step removes the secondary read-only endpoint provided by RA-GRS before migration. ZRS supports general-purpose v2 accounts only.

You can request live migration through the Azure Support portal.
upvoted 4 times

🗄️ 👤 **[Removed]** 3 years, 1 month ago

you can use ZRS with Premium block and premium file shares too: <https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>
upvoted 4 times

🗄️ 👤 **Bravo_Dravel** Most Recent 🕒 3 months, 1 week ago

Selected Answer: B

Tip
BlobStorage do not support Zone-Redundant Storage (ZRS) as a replication option.
upvoted 1 times

🗄️ 👤 **[Removed]** 8 months ago

Selected Answer: B

B is correct

Live Migration = Storage V2 + LRS or GRS
upvoted 2 times

🗄️ 👤 **Limobakry** 11 months, 3 weeks ago

To identify which storage account can be converted to Zone-redundant storage (ZRS) replication by requesting a live migration from Azure support, you should identify the following:

The storage account that you want to convert to ZRS replication, in this case, Storage2.
Provide justification or reasons for the conversion, such as the need for higher resilience and redundancy across availability zones within an Azure region.
Confirm that the storage account meets the prerequisites for ZRS replication, such as being a StorageV2 account and currently configured with Locally-redundant storage (LRS) replication.
By providing this information and justification to Azure support, you can request a live migration of Storage2 to Zone-redundant storage (ZRS) replication. Azure support will assess the request based on the provided details and perform the necessary actions to convert the storage account to ZRS replication.
upvoted 1 times

🗄️ 👤 **Amir1909** 1 year, 2 months ago

B is correct
upvoted 1 times

🗄️ 👤 **SkyZeroZx** 1 year, 3 months ago

Horrible question , currently how solutions architect professional in AWS , Azure is too horrible in question of certification the question only need memorized a lot of combinations exactly steps , why ? no have idea
upvoted 1 times

🗄️ 👤 **nandakku** 1 year, 7 months ago

This question appeared in latest exam in September 2023. The correct answer is ,
Live migration can be done to ZRS from LRS if the type is General purpose V2.
upvoted 5 times

🗄️ 👤 **Prasis** 1 year, 7 months ago

Storage 2
https://www.youtube.com/watch?v=-0LvU_g4Ksk&list=PLIKA5U_Yqgof3H0YWhzvarFixW9QLTr4S&index=64
upvoted 4 times

🗄️ 👤 **jackill** 1 year, 8 months ago

Selected Answer: B

storage1 -> NO, because the "(Standard) general purpose v1" does not support ZRS ... I've put "Standard" in parenthesis because the documentation I've found do not mention about *premium* general purpose v1, but since it is not specified I suppose the same limitations apply to it.
storage2 -> YES : the migration from LRS to ZRS is supported, and excluding the other options only this one remains.
storage3 -> NO : the conversion from "...from GRS/RA-GRS" requires "Switch to LRS first".
storage4 -> NO: the "BlobStorage" kind, is a "Legacy blob storage" that does not support ZRS.
References: tables from <https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal#storage-account-type>,

<https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal#replication-change-table>,
<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal#storage-account-type-parameters>
upvoted 3 times

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

Agree with B

Answer looks correct;

<https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal>
upvoted 1 times

🗨️ 👤 **Lapwing** 2 years ago

Selected Answer: B

Since ZRS is only supported by StorageV2 only B and C would apply. Live migration is not possible for RA-GRS (option C). Option B remains.
upvoted 2 times

🗨️ 👤 **NJTH** 2 years ago

Exactly same question was on todays exam.
(7th April 2023)
upvoted 3 times

🗨️ 👤 **shadad** 2 years, 2 months ago

Selected Answer: B

I took Exam of Azure- 104 at 27/2/2023
I score 920 points out of 1000 points. This was on it and my answer was: B
upvoted 9 times

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

Selected Answer: B

B- storage2

- ZRS Supports the following Storage Account Types:

Standard GPv2 Accounts

Premium File Share Accounts

Premium Block Blob Accounts

- Conversion is just supported for GPv2 and Premium File Share storage accounts (Not for Blob Accounts).

- Conversion from GRS/RA-GRS to ZRS, Switch to LRS first (Directly from RA-GRS is not possible).

According to these info;

- Storage1 is GPv1 so NO

- Storage3 is RA-GRS so NO

- Storage4 is BlobStorage so NO

Source: <https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal>
upvoted 6 times

🗨️ 👤 **[Removed]** 2 years, 3 months ago

On my 2nd test
upvoted 2 times

🗨️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) "storage2"

ZRS Supports the following Storage Account Types:

- Standard General-purpose v2 Accounts

- Premium File Share Accounts

- Premium Block Blob Accounts

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#zone-redundant-storage>
upvoted 8 times

You have an Azure subscription that contains a storage account named account1.

You plan to upload the disk files of a virtual machine to account1 from your on-premises network. The on-premises network uses a public IP address space of 131.107.1.0/24.

You plan to use the disk files to provision an Azure virtual machine named VM1. VM1 will be attached to a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24.

You need to configure account1 to meet the following requirements:

- ☞ Ensure that you can upload the disk files to account1.
- ☞ Ensure that you can attach the disks to VM1.
- ☞ Prevent all other access to account1.

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 Networking blade of account1, select Selected networks.
- B. From the Networking blade of account1, select Allow trusted Microsoft services to access this storage account.
- C. From the Networking blade of account1, add the 131.107.1.0/24 IP address range.
- D. From the Networking blade of account1, add VNet1.
- E. From the Service endpoints blade of VNet1, add a service endpoint.



Correct Answer: AC


Community vote distribution

AC (65%)

CD (24%)



5%

-   **chinnu_07**



Highly Voted 

 3 years, 4 months ago



A,C IS THE CORRECT ANSWER

upvoted 53 times
-   **awssecuritynewbie** 3 years, 2 months ago



Option C will allow for the public Address to be added but we just want VM1 to gain access to the VM that can be done via the private IP.

upvoted 5 times
-   **awssecuritynewbie** 3 years, 2 months ago



sorry mistake it states from on-perm therefore you need it to allow public OP of the VM to be allowed to access.

upvoted 3 times
-   **kmaneith** 2 years, 6 months ago



correct , attach disk to VM1 has nth to do with firewall

upvoted 2 times
-   **holytoni** 2 years, 1 month ago



I can confirm that. I tested it myself on the portal. I tried to attach a vhd with my public IP. Only when I am whitelisting my ip i can attach a dsik. I believe the main point here is "Ensure that you can attach the disks to VM1.": In this case "you", means our public IP must be allowed, ergo the onprem net.


upvoted 6 times
-   **ggogel** 1 year, 5 months ago

I agree. For clarification: D is not required because the VM does not mount the disk through the REST endpoint. So, network rules do not matter in this case.

upvoted 1 times
-   **sca88** 5 months, 2 weeks ago

D is required, because it ask for "Prevent all other access to disk"

upvoted 1 times
-   **klexams**

Highly Voted 

 3 years, 1 month ago

Too many mixed answers here. Decided to spend hours reading MS Docs! K, let's settle this one once and for all. Technically all answers are correct, however you can only choose 2. So here we go:
B, C, D depends on A. And B is selected by default btw (once you do A).
E has to be done for the disk to be used by VM1.
So the correct answer is A and E. A which will cover B C D. And E as explained above.
Hope this helps!

upvoted 40 times

  **epomatti** 3 years ago

From someone who did a "lot of research" you clearly have no idea what you're talking about.

B is not selected by default with A. You clearly don't understand what "Allow trusted Microsoft services to access this storage account", as this has nothing to do with the question.

The question CLEARLY says that you plan do upload from the on-premises network with PUBLIC ip address 131.107.1.0/24.

A, C are the only possible combination to answer this question.

For other options:

- B, theres no need to involve Microsoft trusted services here.
- D, that only works if there is a site-to-site VPN, and that is NOT stated in the problem.
- E, theres nothing to do with the problem.

upvoted 48 times

  **klexams** 2 years, 7 months ago

sure you seem to understand everything eh.. NOT! lol. How are you going to attach the disks to the VM1 sweetie???

upvoted 5 times

  **AzureG0d** 2 years, 6 months ago

Imfao!!

upvoted 3 times

  **gardenbooz** 2 years, 7 months ago

"Allow trusted Microsoft services to access this storage account" IS selected by default, once you switch to "selected networks" (A). However, trusted Microsoft services don't specifically include Microsoft Compute (VMs), so this answer is not relevant here (see <https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#trusted-access-for-resources-registered-in-your-subscription>)

upvoted 4 times

  **Jay_D_Lincoln** Most Recent 2 months, 3 weeks ago

Selected Answer: AC

A and C are correct. But D is not incorrect. Its the third step. I believe either combination will be correct since the question did not ask for a sequence

upvoted 1 times

  **Bravo_Dravel** 3 months, 1 week ago

Correct: AC

A. From the Networking blade of account1, select Selected networks.



This action restricts access to the storage account to only the specified networks or IP ranges, meeting the requirement to prevent all other access.
B. From the Networking blade of account1, select Allow trusted Microsoft services to access this storage account.

While this enables trusted Microsoft services to access the account, it is not required for this scenario, as VM1 is in the same subscription.
C. From the Networking blade of account1, add the 131.107.1.0/24 IP address range.

This allows the on-premises network to upload the disk files.
D. From the Networking blade of account1, add VNet1.

This is unnecessary if a service endpoint is used for VNet1 to access the storage account.
E. From the Service endpoints blade of VNet1, add a service endpoint.

This is not required because the requirement can be met by other configurations.
upvoted 1 times

  **sca88** 5 months, 2 weeks ago

Selected Answer: CD

select Selected networks, it's just the first step to implement the C and D.
Option C: From the Networking blade of account1, add the 131.107.1.0/24 IP address range: This action allows your on-premises network to upload the disk files to the storage account by specifying the IP address range of your on-premises network.

Option D: From the Networking blade of account1, add VNet1: This ensures that the virtual network (VNet1) can access the storage account, which is necessary for attaching the disks to VM1.
upvoted 2 times

  **RVivek** 5 months, 3 weeks ago

Selected Answer: CD

C will allow access from on-prem
D will allow access from VM1

A- is only hals of the solutuion. After slecting selcted network you have to complte C and D.
E will allow asscess to all storage accounts from Vnet1 unless limited by a service end point policy
upvoted 2 times

🗨️ 👤 **d7fb451** 7 months, 1 week ago

oh, and if the VHD is converted to a managed disk (as it should be), it would not be accessible from the internet.

upvoted 1 times

🗨️ 👤 **d7fb451** 7 months, 1 week ago

if you assume it is using SMB to connect to a file share to "provision" the VM. It could be A,C or A,E. But even then it is missing steps...

A,C - need to add the subnet

A,E - need to add end point policy

upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago

Selected Answer: AC

WRONG

A & C are correct

upvoted 2 times

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

What if for this type of question i check all answers? Did someone try this?

upvoted 1 times

🗨️ 👤 **Rediwed** 8 months, 3 weeks ago

You get an error.

upvoted 1 times

🗨️ 👤 **SDiwan** 1 year, 3 months ago

Selected Answer: AC

A: bcoz we need to prevent access from all n/w . Enabling this setting by default enables the setting to allow trusted azure services (option B).

C: will create firewall rule to allow on-prem n/w to access the storage account and upload disk.

Specifically, option D is not needed bcoz attaching the disk to vm is done by azure resource manager via backbone n/w. So allow trusted services option which is enabled as part of option A is sufficient to attach the disk.

upvoted 5 times

🗨️ 👤 **bacana** 1 year, 3 months ago

A and C

Allow Azure services on the trusted services list to access this storage account is select by default when you change from "Enabled from all networks" to "Enabled from selected virtual networks and IP addresses"

upvoted 2 times

🗨️ 👤 **MatAlves** 1 year, 3 months ago

Configuring access from on-premises networks

Go to the storage account that you want to secure.

Select Networking.

Check that you've chosen to allow access from Selected networks.

To grant access to an internet IP range, enter the IP address or address range (in CIDR format) under Firewall > Address Range.

To remove an IP network rule, select the delete icon () next to the address range.

Select Save to apply your changes.

upvoted 1 times

🗨️ 👤 **MatAlves** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>

upvoted 1 times

🗨️ 👤 **nchebbi** 1 year, 5 months ago

IMHO it should be C&D, before you need do C&D you need for sure to do option A, but here they are asking to actions to meet the requirements, AC or AD alone won't acheive the requirements.

Explanations:

C is mandatory to have access from on-premises, it should be set in the firewall section

D is required to have access to VNet1 to attached the disk to your VM, if you try to add that VNET1 to the Virtual Networks section (if there isn't any service endpoints already created) it will create it. Here's a message I get when I try to add VNET "The following networks don't have service endpoints enabled for 'Microsoft.Storage.Global'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait." So option E is required as well but it will be created automatically when you add the VNet1


upvoted 3 times

🗨️ 👤 **Ahkhan** 1 year, 5 months ago

I tested it on 11/12/2023 - A & C are correct.

This question could also come in a lab simulation where they will tell you to allow the access to storage account from a specific CIDR.

upvoted 3 times

  **CzechChris** 1 year, 6 months ago

I think I decided on every combination at some point, but I agree its AC now.
A few people below mentioned that the question is badly written. It would help if C mentioned Add an IP range in the Firewall section, which is what you need to do. As the text underneath Firewall says "Add IP ranges to allow access from the internet or your on-premises networks", which is what you want to achieve. Allow access from the public range so that you can copy up the VM image.
<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>



upvoted 1 times

  **damirbek369** 1 year, 6 months ago

I go for A,C.

D does not make sense. Why would you add a Service Endpoint after enabling Selected Virtual Networks option from Networking of Storage Account if you are not going to add IP Address.

upvoted 1 times

  **damirbek369** 1 year, 6 months ago
Sorry, I meant E does not make sense.

upvoted 1 times

DRAG DROP -

You have an on-premises file server named Server1 that runs Windows Server 2016.

You have an Azure subscription that contains an Azure file share.

You deploy an Azure File Sync Storage Sync Service, and you create a sync group.

You need to synchronize files from Server1 to Azure.

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

Install the Azure File Sync agent on Server1

Create an Azure on-premises data gateway

Create a Recovery Services vault

Register Server1

Add a server endpoint

Install the DFS Replication server role on Server1

Answer Area

Correct Answer:

Actions

Install the Azure File Sync agent on Server1

Create an Azure on-premises data gateway

Create a Recovery Services vault

Register Server1

Add a server endpoint

Install the DFS Replication server role on Server1

Answer Area

Install the Azure File Sync agent on Server1

Register Server1

Add a server endpoint

Step 1: Install the Azure File Sync agent on Server1

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share

Step 2: Register Server1.

Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

Step 3: Add a server endpoint -

Create a sync group and a cloud endpoint.

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

  **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

Step 1: Install the Azure File Sync agent on Server1

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share

Step 2: Register Server1

Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

Step 3: Add a server endpoint

Create a sync group and a cloud endpoint.

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

upvoted 286 times

  **fedztetz** Highly Voted 4 years, 4 months ago

Answer is correct

upvoted 36 times

  **[Removed]** Most Recent 8 months ago

CORRECT

upvoted 2 times

  **Amir1909** 1 year, 2 months ago

Step 1: Install the Azure File Sync agent on

Step 2: Register Server1

Step 3: Add a server endpoint

upvoted 1 times

  **TheLadyAce** 1 year, 7 months ago

The answers are correct, the video below explains more about how it worked. <https://youtu.be/Du623njpcHk>

upvoted 1 times

  **iamchoy** 1 year, 7 months ago

To synchronize files from the on-premises file server `Server1` to the Azure file share using Azure File Sync, you should follow these steps in sequence:

1. **A. Install the Azure File Sync agent on Server1.**

- The Azure File Sync agent enables data sync and cloud tiering. This agent must be installed on each server you want to sync with Azure.

2. **D. Register Server1.**

- After the agent is installed, you need to register your server with the Storage Sync Service. This step creates a trust relationship between your server and the Azure File Sync service.

3. **E. Add a server endpoint.**

- Once your server is registered, you add it to the sync group by creating a server endpoint. The server endpoint represents a specific location on the registered server, such as a folder, and keeps it in sync with the Azure file share.

To summarize, the sequence is:

1. Install the Azure File Sync agent on Server1.

2. Register Server1.

3. Add a server endpoint.

upvoted 2 times

  **Mehedi007** 1 year, 9 months ago

Install the Azure File Sync agent on Server1,

Register Server1,

Add a server endpoint

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>

upvoted 1 times

  **marioZuo** 1 year, 9 months ago


Install sync agent -> Register server -> Create a sync group

upvoted 1 times


  **orionduo** 2 years, 3 months ago

Correct Answer


upvoted 1 times


-  **NaoVaz** 2 years, 7 months ago


1) "Install the Azure File Sync agent on Server1"
2) "Register Server1"
3) "Add a server endpoint"


Reference: <https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>
upvoted 7 times
-  **EmnCours** 2 years, 8 months ago


Step 1: Install the Azure File Sync agent on Server1
The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share
Step 2: Register Server1.
Register Windows Server with Storage Sync Service
Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.


Step 3: Add a server endpoint -
Create a sync group and a cloud endpoint.
upvoted 1 times
-  **Lazylinux** 2 years, 10 months ago

Given answer is correct
upvoted 2 times
-  **manalshowaei** 2 years, 10 months ago

Install the Azure File Sync agent on Server1
Register Server1
Add a server endpoint
upvoted 1 times
-  **babzbabz** 2 years, 11 months ago

Came on exam today (24/05-2022)
upvoted 6 times
-  **benvdw** 3 years, 1 month ago

on exam 13/3/2022
upvoted 5 times
-  **stokazz** 3 years, 1 month ago

On the exam 07/03/2022. Read Mlantonis answer
upvoted 5 times
-  **InvisibleShadow** 3 years, 1 month ago

This question came in the exam today 8/Mar/2022.
I passed the exam, 95% questions came from here.
upvoted 7 times

HOTSPOT -

You plan to create an Azure Storage account in the Azure region of East US 2.

You need to create a storage account that meets the following requirements:

- ☞ Replicates synchronously.
- ☞ Remains available if a single data center in the region fails.

How should you configure the storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Replication:

	▼
Geo-redundant storage (GRS)	
Locally-redundant storage (LRS)	
Read-access geo-redundant storage (RA GRS)	
Zone-redundant storage (ZRS)	

Account type:

	▼
Blob storage	
Storage (general purpose v1)	
StorageV2 (general purpose v2)	

Answer Area

Correct Answer:

Replication:

	▼
Geo-redundant storage (GRS)	
Locally-redundant storage (LRS)	
Read-access geo-redundant storage (RA GRS)	
Zone-redundant storage (ZRS)	

Account type:

	▼
Blob storage	
Storage (general purpose v1)	
StorageV2 (general purpose v2)	

Box 1: Zone-redundant storage (ZRS)

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region.

LRS would not remain available if a data center in the region fails

GRS and RA GRS use asynchronous replication.

Box 2: StorageV2 (general purpose V2)

ZRS only support GPv2.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy> <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs>

 **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

Box 1: Zone-redundant storage (ZRS)

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single Region.

GRS protects against Zone failure, while ZRS protects against data center failure.

LRS would not remain available if a data center in the region fails.

GRS and RA GRS use asynchronous replication.

Box 2: StorageV2 (general purpose V2)

ZRS only support GPv2.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs>
upvoted 233 times

  **Snownoodles** 3 years, 5 months ago

>ZRS only support GPv2.

ZRS also support Premium Block Blobs an Premium file shares

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>
upvoted 10 times

  **Holydud** 2 years, 8 months ago

Was on exam 19 Aug 2022. Scored 870. Answered:

Box1: Zone-redundant storage (ZRS)

Box 2: StorageV2 (general purpose V2)

upvoted 19 times

  **MicroJ**  4 years, 5 months ago

Answer describes ZRS being correct but marks GRS. From reading the description is seems like ZRS is the correct answer.
upvoted 38 times

  **JohnAvlakitotis** 4 years, 5 months ago

True. ZRS is correct.

upvoted 12 times

  **Sandroal29** 4 years, 1 month ago

The thing is that ZRG is not Geo-redundant. it merely works within a single region.

upvoted 4 times

  **JayBee65** 3 years, 11 months ago

...and what is your point about this?



upvoted 2 times

  **Omar_Aladdin** 3 years, 7 months ago

ZRS means Zone Redundant, the only think to Introduce a G here, is if was asked about "Region Failover"

Whenever you hear a "Datacenter"; It is Z over there

upvoted 3 times

  **Shailen** 3 years, 10 months ago

Seems rectified now. It is showing ZRS selected as well in answer description below.

upvoted 3 times

  **[Removed]**  8 months ago

CORRECT

upvoted 2 times

  **tashakori** 1 year, 1 month ago


Given answer is correct

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

Correct

upvoted 1 times

  **31c21da** 1 year, 3 months ago

Is that only me cannot understand whether below from Microsoft Doc means ZRS is supported or not supported by BLOB:

"ZRS is supported for all Azure Storage services through standard general-purpose v2 storage accounts, including: Azure Blob storage (hot and cool block blobs and append blobs, non-disk page blobs), Azure Files (all standard tiers: transaction optimized, hot, and cool), Azure Table storage, Azure Queue storage"

upvoted 1 times

  **memo454** 1 year, 8 months ago

Pass the exam on 11 August 2023 with 909, Below are some of the notes that may help for Blob and file storage:

A. Blob Storage:

1-Archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. Only storage accounts that are configured for LRS, GRS, or RA-GRS support moving blobs to the archive tier.

2-Import supports Azure Blob storage and Azure File storage



3 -Export supports Azure Blob storage

4-support Lifecycle management policies. Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.

5-Object Replication supports General Purpose V2 and Premium Blob accounts.

6-Support both Azure (AD) and SAS (Shared Access Signature) token.

upvoted 1 times

  **Untilted** 1 year, 8 months ago

Is the free version of this site enough or do you need Contributor access?

upvoted 1 times

🗨️ 👤 **memo454** 1 year, 8 months ago

7-Support conditions when added to built-in or custom role assignments that have blob storage or queue storage data actions
8-Encryption scopes support a container or an individual blob
9-Not Support ZRS
10-az support
11-support stored access policies
12-Tieing is supporting only or block blobs
13-Flow logging for Blob Storage accounts has a retention period of 30 days. General Purpose v2 (GPv2) storage accounts instead, which support flow logging with a retention period of up to 365 days.

upvoted 1 times

🗨️ 👤 **memo454** 1 year, 8 months ago

B.File storage:
1-az support
2-Support persistent storage.
3-File share Supports Premium file shares (FileStorage), Premium LRS/ZRS for SMB Multichannel
4-File Storage: Only Shared Access Signature (SAS) token is supported.
5-Only Shared Access Signature (SAS)
6-Premium file shares
6-Import supports Azure Blob storage and Azure File storage
7-supports identity-based authentication over Server Message Block (SMB) through on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

upvoted 1 times

🗨️ 👤 **memo454** 1 year, 8 months ago

B.File storage: Continue..
8-Not support archive
9-Not support condition
10-No support Object Replication
11-No support Lifecycle management policies
12-no support encryption scope

upvoted 1 times

🗨️ 👤 **Mehedi007** 1 year, 9 months ago

Zone-redundant storage (ZRS),
StorageV2 (general purpose V2)

"Zone-redundant storage (ZRS) replicates your storage account synchronously across three Azure availability zones in the primary region."

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#zone-redundant-storage>

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-storage-account-types>

upvoted 1 times

🗨️ 👤 **vinsom** 2 years ago

Yes, very likely you would - Passed the exam today, 1/May/23 - scored 930. I am still digesting the fact that 95% of the questions are from here, though it is tough to believe before you take the exam. Big thanks to our super-hero mlantonis!

upvoted 6 times

🗨️ 👤 **zellck** 2 years, 2 months ago

1. ZRS
2. StorageV2 (general purpose V2)

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#zone-redundant-storage>

Zone-redundant storage (ZRS) replicates your storage account synchronously across three Azure availability zones in the primary region. Each availability zone is a separate physical location with independent power, cooling, and networking. ZRS offers durability for storage resources of at least 99.999999999% (12 9's) over a given year.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#standard-storage-accounts>

ZRS is supported for all Azure Storage services through standard general-purpose v2 storage accounts.

upvoted 1 times

🗨️ 👤 **GBAU** 2 years, 2 months ago

For reference, when people say the likes of "ZRS only support GPv2", this is not true (or perhaps no longer true).

ZRS does support Premium Blob and Premium File Share 'in some regions', but these are not an option in the question.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview>

upvoted 1 times

🗨️ 👤 **bacana** 2 years, 6 months ago

ZRS currently supports standard general-purpose v2, FileStorage and BlockBlobStorage storage account types

upvoted 1 times

🗨️ 👤 **NaoVaz** 2 years, 7 months ago

1) Replication: "Zone-redundant storage (ZRS)"
2) Account type. "StorageV2 (general purpose v2)"

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs>

upvoted 2 times

  **EmnCours** 2 years, 8 months ago

Given answer is correct

upvoted 1 times

  **Lazylinux** 2 years, 10 months ago

Given answer is correct


upvoted 2 times

  **manalshowaei** 2 years, 10 months ago

Zone-redundant storage (ZRS)'

StorageV2 (general purpose V2)

upvoted 1 times

  **babzbabz** 2 years, 11 months ago

Came on exam today (24/05-2022)

upvoted 6 times

You plan to use the Azure Import/Export service to copy files to a storage account.
Which two files should you create before you prepare the drives for the import job? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. an XML manifest file
- B. a dataset CSV file
- C. a JSON configuration file
- D. a PowerShell PS1 file
- E. a driveset CSV file

Correct Answer: *BE*

Community vote distribution

BE (97%)

mlantonis

Highly Voted

3 years, 11 months ago

Correct Answer: B and E

Modify the dataset.csv file in the root folder where the tool resides. Depending on whether you want to import a file or folder or both, add entries in the dataset.csv file

Modify the driveset.csv file in the root folder where the tool is.

Reference:

<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-to-files>

upvoted 255 times

suriyaswamy

3 years, 8 months ago

Good Info

upvoted 3 times

PPSHREE_123

3 years, 10 months ago

I find mlantonis's answers are correct and most reliable

upvoted 44 times

Panapi

2 years, 2 months ago

Answer valid! This question was on the exam 22/02/2023. Scored 920. Thanks guys!

upvoted 11 times

Lobe

Highly Voted

4 years, 5 months ago

It should be B and E. Explanation is right though

upvoted 56 times

[Removed]

Most Recent

8 months ago

Selected Answer: BE

B & E are correct

upvoted 1 times

op22233

1 year ago

thanks mlantonis

upvoted 1 times

iamchoy

1 year, 7 months ago

Selected Answer: BE


Before you prepare the drives for the import job with Azure Import/Export service, you should create the following two files:

B. a dataset CSV file

E. a driveset CSV file

These files are used by the `WAImportExport` tool to facilitate copying your data to the drive and encrypting the data on the drive with AES 256-bit BitLocker.


upvoted 2 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: BE

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-data-to-files?tabs=azure-portal-preview#step-1-prepare-the-drives>

upvoted 1 times

  **Athul07** 1 year, 11 months ago

A. An XML manifest file: The XML manifest file contains the details of the import job, such as the storage account information, destination container name, and other configuration settings.


E. A driveset CSV file: The driveset CSV file provides information about the physical drives you are using for the import job, including the drive serial number, drive letter or mount point, and the drive size.

Therefore, the correct files to create before preparing the drives for the import job are:

A. An XML manifest file.



E. A driveset CSV file.

upvoted 2 times

  **SivaPannier** 1 year, 8 months ago

I understand the xml manifest file is created during copy of Blob contents to Azure Storage Account and while using the WAImport tool. Here we are doing the copy of the files, so the answer should be B

upvoted 2 times

  **lordrjd** 1 year, 11 months ago

Selected Answer: BE

<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-to-files>

upvoted 1 times

  **zzreflexzz** 2 years ago

on exam 4/29/23

upvoted 1 times

  **djgodzilla** 2 years, 1 month ago

Selected Answer: BE

Additional files: Import will also take



1) dataset.csv: contains a list of directories and/or a list of files to be copied to target drives.

BasePath ,DstBlobPathOrPrefix, BlobType, Disposition, MetadataFile, PropertiesFile

"F:\50M_original\","containername/","BlockBlob,rename,"None",None

2) driveset.csv: contains the list of disks to which the drive letters are mapped so that the tool can correctly pick the list of disks to be prepared.

upvoted 4 times

  **mdwSysOps** 2 years, 2 months ago

Selected Answer: BE

. When using the Azure Import/Export service to copy files to a storage account, you should create the following two files before preparing the drives for the import job:

B. A dataset CSV file: This file contains the details of the files to be imported, such as the name of the files, the size of the files, and the path to the files on the drive.

E. A driveset CSV file: This file specifies the details of the drives to be used in the import job, such as the drive letter, the path to the drive, and the name of the drive.

Therefore, the correct answers are B. a dataset CSV file and E. a driveset CSV file.

A. An XML manifest file, C. a JSON configuration file, and D. a PowerShell PS1 file are not required when preparing drives for an Azure Import/Export job.

upvoted 4 times

  **bloodtech** 2 years, 2 months ago

On exam 24/02/2023

upvoted 4 times

  **zellck** 2 years, 2 months ago

Got this in Feb 2023 exam.

upvoted 3 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: BE

See <https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-data-to-files?tabs=azure-portal-preview>

upvoted 1 times

  **typales2005** 2 years, 3 months ago

Was on the 09/01/2023 exam.

upvoted 5 times

  **shejinbacker** 2 years, 3 months ago

did you pass ? is ET enough for prep ?



upvoted 1 times

  **[Removed]** 2 years, 5 months ago

Selected Answer: BE

on Exam 24.11.2022, passed with 780 !! Thanks to everyone!! Good Luck

upvoted 6 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: BE

B) "a dataset CSV file" & E) "a driveset CSV file"

(...) "Modify the dataset.csv file in the root folder where the tool is." (...) "Modify the driveset.csv file in the root folder where the tool is." (...)

Reference: <https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-data-to-files?tabs=azure-portal-preview#step-1-prepare-the-drives>

upvoted 1 times

You have a Recovery Service vault that you use to test backups. The test backups contain two protected virtual machines. You need to delete the Recovery Services vault. What should you do first?

- A. From the Recovery Service vault, delete the backup data.
- B. Modify the disaster recovery properties of each virtual machine.
- C. Modify the locks of each virtual machine.
- D. From the Recovery Service vault, stop the backup of each backup item.

Correct Answer: D

Community vote distribution

D (100%)

- mlantonis**

Highly Voted

3 years, 11 months ago

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault#delete-protected-items-in-the-cloud>

upvoted 134 times
- Holydud**

2 years, 8 months ago

Was on exam 22 Aug 2022. Scored 870. Answered D

upvoted 8 times
- Holydud**

2 years, 8 months ago

Sry, 19 Aug 2022

upvoted 6 times
- confetti**

2 years, 7 months ago

was this enough to get passed? can you please share dumps you referred to?

upvoted 1 times
- tuta**

Highly Voted

4 years, 5 months ago

correct

upvoted 25 times
- diazed**

Most Recent

6 months, 2 weeks ago

In another question they mention that just deleting the data from the vault is enough. And that is the correct answer to that question. Here they mention that you should stop the backup, which makes more sense to me. But now I am doubting the answer to the other question.

upvoted 5 times
- ethansyh**

5 months, 3 weeks ago

It appears to be we need to stop the backup first, then delete the backup data, and the deletion of recovery service will be possible.

The another question you mentioned maybe not having a on-going backup service at the time, so delete the backup data will be suffient.

upvoted 5 times
- [Removed]**

8 months ago

Selected Answer: D

D is correct

upvoted 1 times
- tashakori**

1 year, 1 month ago

D is correct

upvoted 1 times
- iamchoy**

1 year, 7 months ago

Selected Answer: D

Before you can delete the Recovery Services vault, you should first:

D. From the Recovery Service vault, stop the backup of each backup item.

After stopping the backup, you need to delete the backup data. Please note that you can't delete a Recovery Services vault that contains protected data sources (for example, IaaS VMs, SQL databases, Azure file shares) or that contains backup data. Once backup data is deleted, it will go into the

soft deleted state. You also can't delete a vault that has registered storage accounts. If you try to delete the vault without removing these dependencies, you'll encounter error messages.

upvoted 7 times

  **ChetanPrk** 1 year, 8 months ago

Selected Answer: D

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault#delete-protected-items-in-the-cloud>

upvoted 1 times

  **ChetanPrk** 1 year, 8 months ago

Selected Answer: D

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault#delete-protected-items-in-the-cloud>

upvoted 1 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: D

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-delete-vault?tabs=portal#delete-protected-items-in-the-cloud>



upvoted 1 times

  **kamalpur** 1 year, 9 months ago

This question is explained below video with practical

<https://youtu.be/urc93glDu30>

upvoted 1 times

  **xitzee** 1 year, 11 months ago



Funy is that in similar question eartlier in the subset it was to delete backups not to stop them

upvoted 11 times

  **eduardovzermeno** 6 months, 4 weeks ago


I think the key is in the question; "What should you do first?". Emphasis in "first".

upvoted 1 times

  **ajdann** 1 year, 8 months ago

I remember this too...

upvoted 1 times

  **Athul07** 1 year, 11 months ago

Before deleting the Recovery Services vault, you should first perform the following action:



A. From the Recovery Service vault, delete the backup data: This action involves deleting the backup data stored in the Recovery Services vault. By deleting the backup data, you ensure that the vault no longer contains any protected data and can be safely deleted.

Therefore, the correct first step is:

A. From the Recovery Service vault, delete the backup data.

The other options mentioned are not necessary as the primary concern is removing the backup data from the vault

upvoted 2 times

  **SivaPannier** 1 year, 8 months ago

refer to the link below and other sections in this.. it says we need to stop the backup and then go for the deletion of protected items. Hence the answer is D.

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault#delete-protected-items-in-the-cloud>

upvoted 2 times

  **Andreas_Czech** 1 year, 11 months ago

Selected Answer: D

Correct Answer id D,

because: when you delete the Job, it asks you / you can delete the Data too, but disable under Properties -> Security Settings the Soft delete first.

<https://learn.microsoft.com/en-gb/azure/backup/backup-azure-delete-vault>

upvoted 1 times

  **mdwSysOps** 2 years, 2 months ago



Selected Answer: D

Before you can delete a Recovery Service vault that contains protected virtual machines, you need to stop the backup of each backup item.

Therefore, the correct answer is D. From the Recovery Service vault, stop the backup of each backup item.

Once you have stopped the backup, you can proceed with deleting the Recovery Service vault. You can do this by selecting the vault in the Azure portal and then clicking on the "Delete" button. Please note that deleting a vault is a permanent action and cannot be undone, so you should ensure that you have a backup of your data before proceeding.

upvoted 9 times

  **zelck** 2 years, 2 months ago

Got this in Feb 2023 exam.

upvoted 5 times

  **ChakaZilly** 2 years, 3 months ago

I think correct answer is A. The question doesn' t state that there is an backup job active. Also Azure docs mention explicit that a vault can only be removed when there are no backup-files in it.

upvoted 3 times

  **Sivashankarrp** 2 years, 5 months ago

Correct Answer: D

upvoted 2 times

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	West US	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
Vault1	Recovery Services vault	Central US	RG1
Vault2	Recovery Services vault	West US	RG2
VM1	Virtual machine	Central US	RG2
storage1	Storage account	West US	RG1
SQL1	Azure SQL database	East US	RG2

In storage1, you create a blob container named blob1 and a file share named share1.

Which resources can be backed up to Vault1 and Vault2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Can use Vault1 for backups:

▼

VM1 only

VM1 and share1 only

VM1 and SQL1 only

VM1, storage1, and SQL1 only

VM1, blob1, share1, and SQL1

Can use Vault2 for backups:

▼

storage1 only

share1 only

VM1 and share1 only

blob1 and share1 only

storage1 and SQL1 only

Answer Area

Can use Vault1 for backups:

▼

VM1 only

VM1 and share1 only

VM1 and SQL1 only

VM1, storage1, and SQL1 only

VM1, blob1, share1, and SQL1

Can use Vault2 for backups:

▼

storage1 only

share1 only

VM1 and share1 only

blob1 and share1 only

storage1 and SQL1 only

Box 1: VM1 only -

VM1 is in the same region as Vault1.

File1 is not in the same region as Vault1.

SQL is not in the same region as Vault1.

Blobs cannot be backup up to service vaults.

Note: To create a vault to protect virtual machines, the vault must be in the same region as the virtual machines.

Box 2: Share1 only.

Storage1 is in the same region (West USA) as Vault2. Share1 is in Storage1.

Note: After you select Backup, the Backup pane opens and prompts you to select a storage account from a list of discovered supported storage accounts. They're either associated with this vault or present in the same region as the vault, but not yet associated to any Recovery Services

vault.

Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault> <https://docs.microsoft.com/en-us/azure/backup/backup-afs>

🗨️ 👤 **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

Box 1: VM1 only

VM1 is in the same region as Vault1. File1 is not in the same region as Vault1. SQL is not in the same region as Vault1. Blobs cannot be backup up to service vaults.

Note: To create a Vault to protect VMs, the Vault must be in the same Region as the VMs.

Box 2: Share1 only

Storage1 is in the same region as Vault2. Share1 is in Storage1.

Note: Only VM and Fileshare is allowed to Backup.

Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault>

<https://docs.microsoft.com/en-us/azure/backup/backup-afs>

<https://feedback.azure.com/forums/217298-storage/suggestions/37096837-possibility-to-backup-blob-data-in-the-recovery-se>
upvoted 298 times

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

I have seen the portal and I think you can't backup an Azure SQL Databases in PaaS, only SQL Server in Azure VM. Right?

upvoted 2 times

🗨️ 👤 **Omar_Aladdin** 3 years, 7 months ago

good talk

upvoted 7 times

🗨️ 👤 **habbey** 2 years ago

Wrong! You can backup Azure blobs to recovery service vaults !

<https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage?tabs=operational-backup>

upvoted 3 times

🗨️ 👤 **AdamHulek** 3 weeks, 1 day ago

Box 2: Share1 only Blob can be configured in Backup Vault:

<https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage?tabs=operational-backup>

"A Backup vault is a management entity that stores recovery points created over time and provides an interface to perform backup related operations."

<https://techcommunity.microsoft.com/discussions/compute/backup-vaults-vs-recovery-service-vault/4403249>

Recovery Services Vault:

-Azure Virtual Machines (Windows and Linux)

-SQL Server in Azure VMs

-SAP HANA in Azure VMs

-Azure Files (file shares)

-Azure Backup Server

- System Center DPM)

Backup Vault:

-Azure Blobs

-Azure Disks

-Azure Database for PostgreSQL servers

upvoted 1 times

🗨️ 👤 **SDiwan** 1 year, 3 months ago

I think the point is that there is no option to select a whole storage account while creating backup policies. You have either select file or blobs, but its not possible to select the entire storage account. So, "Share 1 only" is the correct answer here.

upvoted 3 times

🗨️ 👤 **sca88** 5 months, 2 weeks ago

So blob1 and share1 only should be the correct answer

upvoted 1 times

🗨️ 👤 **pstree** 5 months, 2 weeks ago

No!! Azure Recovery Service Vault and Azure Backup Vault are two different things.

The link from habbey is definitely the wrong link for this question. (Azure Backup Vault)

Blobs are only supported by Azure Backup Vault.



Check for supported datasources:

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq>


upvoted 2 times

  **JunetGoyal** 2 years ago

Yes , I am with Habbey, we can backup blob n file in vault 2
upvoted 3 times

  **May2** 2 years, 11 months ago



what is File1?
upvoted 2 times

  **JimmyYop** 2 years, 3 months ago

I think he meant share1 (File Share)
upvoted 5 times

  **Hibs2016** Highly Voted 4 years, 4 months ago

Answer looks correct it is only share1 within storage1 that can be backed up as you can't back up blobs
See: <https://feedback.azure.com/forums/217298-storage/suggestions/37096837-possibility-to-backup-blob-data-in-the-recovery-se>
upvoted 32 times

  **Borbz** 4 years, 4 months ago

Answer is correct. Storage1 is not valid because it contains a Blob inside, so only Share1 can be backup.
upvoted 13 times

  **FitObelix** 3 years, 10 months ago

it says nothing about blobs, it talks about a blob container
upvoted 1 times

  **Download100** Most Recent 3 months, 1 week ago

Box1: VM1 only -
VM1 is in the same region as Vault1.

Box2: share1 only
Vault1 and Vault2 are Recovery Services vaults, not Backup vaults.
The following lists the various datasources that each vault supports:
Recovery Services vault
Supported datasources:

- Azure Virtual Machine
- SQL in Azure VM
- Azure Files
- SAP HANA in Azure VM
- Azure Backup Server
- Azure Backup agent
- DPM

Backup vault
Supported datasources:

- Azure Disks
- Azure Blobs
- Azure Database for PostgreSQL server
- Kubernetes services (preview)

Reference: <https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq>
upvoted 4 times

  **sca88** 5 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage?tabs=operational-backup>
upvoted 1 times

  **sca88** 5 months, 2 weeks ago

Box1: VM1 only
Box 2: Storage1, or Share1 and Blob1.
The link I provided explain how to do blob backup in Azure Backup Vault. Recovery Service it's a super set of Azure Backup
upvoted 1 times

  **sca88** 5 months, 2 weeks ago

It's definitely blob1 and share1 only
upvoted 1 times

  **[Removed]** 8 months ago



CORRECT

You can backup only VM and Fileshare.

Vault1 and VM1 are in the same zone.
Vault2 and Share1 are in the same zone (because Share1 and Storage1 are in the same zone).
upvoted 2 times



  **tashakori** 1 year, 1 month ago

Given answer is correct
upvoted 1 times



  **SkyZeroZx** 1 year, 3 months ago
1) VM1 ONLY , because need the same region
2) Only share1 , because only support by type of backup and region position


Specifically stating BACKUP VAULT supports BLOB, while RECOVERY SERVICES VAULT supports FILE SHARE

you can "configure/create both vaults using BACKUP CENTER", that is the reason for confusion. hope it is clear now
upvoted 9 times

  **WeepingMaplte** 1 year, 5 months ago
- Recovery service vaults need to be the same region as the virtual machine.
- RSG can backup VM, File Share, SQL and SAP
- Backup Vault is used to protect/backup blob containers

Ans: Vault1 - VM 1 only, Vault2 - share 1 only
Reference: https://youtu.be/ciM5rtXYYYI?si=AQJI4wRz_61dDc4p
upvoted 2 times



  **93d821b** 1 year, 5 months ago
VM1 only, Share 1 only.
See this guy's AMAZING video.
<https://www.youtube.com/watch?v=ciM5rtXYYYI>
upvoted 1 times



  **Richardfu007** 1 year, 5 months ago
Box 2: Share1 only

Recovery Services vault and Backup vault are both supported in Azure Backup, and target the backup and restore of different datasources. You need to create the appropriate vault based on the datasource type that you want to protect.



The following table lists the various datasources that each vault supports:

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq#what-are-the-various-vaults-supported-for-backup-and-restore->
upvoted 2 times



  **DWILK** 1 year, 6 months ago
Is this still true that Vaults can't provide backups for Blobs? Because my lab at Pluralsight says no. There looks to be backups for blobs now provided
upvoted 3 times



  **nmshrwt** 1 year, 4 months ago
Specifically stating BACKUP VAULT supports BLOB, while RECOVERY SERVICES VAULT supports FILE SHARE



you can "configure/create both vaults using BACKUP CENTER", that is the reason for confusion. hope it is clear now
upvoted 1 times



  **Mehedi007** 1 year, 9 months ago
VM1 only,
Share1 only

"the vault must be in the same region as the data source." Also see the image on step 4 of 'Create a Recovery Services vault'
<https://learn.microsoft.com/en-us/azure/backup/backup-create-recovery-services-vault#create-a-recovery-services-vault>
upvoted 4 times

  **marioZuo** 1 year, 9 months ago
for Blob, you can use backup vault not recovery service vault to backup
upvoted 6 times

  **Andreas_Czech** 1 year, 11 months ago
tested in LAB
Option 1: VM1 only (same Region required)
Option 2: Share 1 only
upvoted 8 times

  **keszi** 2 years, 2 months ago
Question was on the exam March 2023
upvoted 10 times

  **vbohr899** 2 years, 2 months ago
Cleared Exam today 26 Feb, This question was there in exam.
upvoted 4 times

  **Ashfaque_9x** 2 years, 3 months ago

Passed today on 29Jan23 with a score of 970. This question was in the exam.

Correct Answer:

Box 1: VM1 only

Box 2: Share1 only

upvoted 6 times

You have an Azure subscription named Subscription1.
You have 5 TB of data that you need to transfer to Subscription1.
You plan to use an Azure Import/Export job.
What can you use as the destination of the imported data?

- A. a virtual machine
- B. an Azure Cosmos DB database
- C. Azure File Storage
- D. the Azure File Sync Storage Sync Service

Correct Answer: C

Community vote distribution

C (95%)5%

mlantonis

Highly Voted

3 years, 11 months ago

Correct Answer: C

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files. The maximum size of an Azure Files Resource of a file share is 5 TB.

Note: There are several versions of this question in the exam. The question has two correct answers:

1. Azure File Storage
- or
2. Azure Blob Storage

The question can have other incorrect answer options, including the following:

- Azure Data Lake Store
- Azure SQL Database
- Azure Data Factory

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

upvoted 205 times

Rodro13

Highly Voted

4 years, 4 months ago

Correct

upvoted 18 times

Nietje

Most Recent

6 months, 3 weeks ago

Is this outdated? It says here Azure Files not supported. Only blob.

upvoted 1 times

[Removed]

8 months ago

Selected Answer: C

C is corerct

upvoted 1 times

Amir1909

1 year, 2 months ago

C is correct

upvoted 1 times

iamchoy

1 year, 7 months ago

Selected Answer: A

Yes, assigning the "Logic App Contributor" role to the Developers group on the Dev resource group will provide the Developers group with the necessary permissions to create, edit, and manage Logic Apps in that specific resource group without granting permissions to other resources.

So, the answer is:

A. Yes

upvoted 1 times

OttomanITGuy

1 year, 3 months ago

What drugs are u on my guy?

upvoted 6 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: C

When you use the Azure Import/Export job, you can transfer data to the following Azure storage solutions:

- A. ****a virtual machine**** - Incorrect. Azure Import/Export does not directly import data to virtual machines. You'd typically use Azure Import/Export to move data to Azure Storage and then copy or access it from a virtual machine if needed.
- B. ****an Azure Cosmos DB database**** - Incorrect. Azure Import/Export does not support Azure Cosmos DB as a destination.
- C. ****Azure File Storage**** - Correct. Azure Import/Export supports both Azure Blob Storage and Azure File Storage as destinations.
- D. ****the Azure File Sync Storage Sync Service**** - Incorrect. While Azure File Sync interacts with Azure File Storage, you don't import directly into the Azure File Sync Storage Sync Service using Azure Import/Export. You'd import into Azure File Storage and then let Azure File Sync handle synchronization.

The correct answer is:

C. Azure File Storage.

upvoted 4 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: C

Azure File Storage


<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>

upvoted 1 times

  **JunetGoyal** 2 years ago

If in question it says Azure file n blob storage, then we will chose this over Azure file share!

upvoted 2 times

  **mdwSysOps** 2 years, 2 months ago

Selected Answer: C

Azure Import/Export service supports importing data to Azure Blob storage and Azure Files only. Therefore, the correct answer to the question is C - Azure File Storage.

To perform an Azure Import/Export job to transfer 5 TB of data to Subscription1

Other valid option would be Azure Blob.

upvoted 3 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: C

C. Azure File Storage

upvoted 2 times

  **John696** 2 years, 6 months ago

Selected Answer: C

Correct answer C

upvoted 1 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: C

C) "Azure File Storage"

Reference: <https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>

upvoted 2 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: C


Correct Answer: C

upvoted 1 times

  **anilagio** 2 years, 8 months ago

Appeared on the exam 26/08/2022.

upvoted 4 times

  **confetti** 2 years, 7 months ago

were these dumps enough to pass the exam?

upvoted 1 times

  **vinsom** 2 years ago

Yes, very likely you would - Passed the exam today, 1/May/23 - scored 930. I am still digesting the fact that 95% of the questions are from here, though it is tough to believe before you take the exam.

upvoted 6 times

  **Lazylinux** 2 years, 10 months ago

Selected Answer: C

C for sure...below more info once u know dont matter how MS will vary the questions

There are two versions of WAImportExport:

*Version 1 for import/export into Azure Blob Storage

*Version 2 for import into Azure Files

*It is WAImportExport.exe ONLY compatible with 64-bit Windows

*Modify the driveset.csv file in the root folder where the tool resides.

*Modify the dataset.csv file in the root folder where the tool resides. Depending on whether *you want to import a file or folder or both, add entries in the dataset.csv file

*The maximum size of an Azure Files Resource of a file share is 5 TB

upvoted 5 times

  **manalshowaei** 2 years, 10 months ago

Selected Answer: C

C. Azure File Storage

upvoted 1 times

HOTSPOT -

You have an Azure subscription.

You create the Azure Storage account shown in the following exhibit.

Microsoft Azure (Preview)

Search resources, services, and docs (G+/?)

Home > Subscriptions > Subscription1 - Resources > New > Create storage account

Create storage account

Validation passed

BasicsNetworkingAdvancedTagsReview + create

Basics

Subscription

Subscription1

Resource group

RG1

Location

{Europe} North Europe

Storage account name

storage16852

Deployment model

Resource manager

Account kind

StorageV2 (general purpose v2)

Replication

Locally-redundant storage (LRS)

Performance

Standard

Access tier (default)

Hot

Networking

Connectivity method

Private endpoint

Private Endpoint

{New} StorageEndpoint1 (blob) (privatelink.blob.core.windows.net)

Advanced

Secure transfer required

Enabled

Large file shares

Disabled

Blob soft delete

Disabled

Blob change feed

Disabled

Hierarchical namespace

Disabled

NFS v3

Disabled

Create< PreviousNext >

[Download a template for automation](#)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The minimum number of copies of the storage account will be [answer choice]

1

2

3

4

To reduce the cost of infrequently accessed data in the storage account, you must modify the [answer choice] setting

Access tier (default)

Performance

Account kind

Replication

Answer Area

The minimum number of copies of the storage account will be [answer choice]

Correct Answer:

To reduce the cost of infrequently accessed data in the storage account, you must modify the [answer choice] setting

1
2
3
4

Access tier (default)
Performance
Account kind
Replication

Box 1: 3 -
Locally Redundant Storage (LRS) provides highly durable and available storage within a single location (sub region). We maintain an equivalent of 3 copies (replicas) of your data within the primary location as described in our SOSP paper; this ensures that we can recover from common failures (disk, node, rack) without impacting your storage account's availability and durability.

Box 2: Access tier -
Change the access tier from Hot to Cool.
Note: Azure storage offers different access tiers, which allow you to store blob object data in the most cost-effective manner. The available access tiers include:
Hot - Optimized for storing data that is accessed frequently.
Cool - Optimized for storing data that is infrequently accessed and stored for at least 30 days.
Archive - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).
Reference:
<https://azure.microsoft.com/en-us/blog/data-series-introducing-locally-redundant-storage-for-windows-azure-storage/>
<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

- sk1803

Highly Voted

3 years, 7 months ago

Both of them are correct.

- LRS has 3 copies of data

- Access tier has the "cool" option to store infrequently accessed data.

upvoted 70 times
- Panapi

2 years, 2 months ago

Answer valid! This question was on the exam 22/02/2023. Scored 920. Thanks guys!

upvoted 18 times
- Omar_Aladdin

Highly Voted

3 years, 7 months ago

Answer is Correct:
in LRS: "Three" Copies in "Three" Racks in a "Single" Datacenter
in ZRS: "Three" Copies in "Three" Datacenters in a "Single" Region

Ref:
<https://docs.microsoft.com/en-us/learn/modules/configure-blob-storage/4-create-blob-access-tiers?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.az-104-manage-storage>

upvoted 41 times
- [Removed]

Most Recent

8 months ago

CORRECT

LRS makes 3 copies in the datacenter

upvoted 2 times
- Amir1909

1 year, 2 months ago



Correct



upvoted 1 times
- LemonVine



1 year, 8 months ago



I just took the exam..and i failed. I didn't have time to go thru topic 3 anyway.
This quesiton showed up in the exam Aug/2023, with modified qusetion, .. it asked, To reduce the cost of networking traffic, which field should you



modify ..
upvoted 4 times



  **Rimoonaa** 1 year, 8 months ago
What was your answer?
upvoted 2 times



  **chucklu** 9 months, 2 weeks ago
To reduce the cost of networking traffic, you should consider modifying the Connectivity method, using the default public endpoint or configuring a Virtual Network (VNet) service endpoint.
upvoted 1 times

  **zzreflexzz** 2 years ago
on exam 4/29/23
upvoted 3 times

  **orionduo** 2 years, 3 months ago
Answer is Correct
upvoted 2 times



  **typales2005** 2 years, 3 months ago
On exam 09/01/2023.
upvoted 7 times



  **[Removed]** 2 years, 5 months ago
on Exam 24.11.2022, passed with 780 !! Thanks to everyone!! Good Luck
- LRS has 3 copies of data
- Access tier has the "cool" option to store infrequently accessed data.
upvoted 7 times



  **NaoVaz** 2 years, 7 months ago
1) The minimum number of copies of the storage account will be "3".
2) To reduce the cost of infrequently accessed data in the storage account, you must modify the "Access tier (default)" setting.



"Locally redundant storage (LRS) replicates your storage account three times within a single data center in the primary region." - <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#locally-redundant-storage>

Pricing related information: <https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview#pricing-and-billing>
upvoted 3 times

  **EmnCours** 2 years, 8 months ago
- LRS has 3 copies of data
- Access tier has the "cool" option to store infrequently accessed data.
upvoted 1 times

  **Jigga14** 3 years ago
Question is stated poorly but answer is correct
upvoted 1 times

  **Dobby25** 3 years, 1 month ago
Received this on my exam today 19/03/2022
upvoted 6 times

  **sanbt** 3 years, 4 months ago
3 and Access tier
upvoted 3 times



You have an Azure Storage account named storage1.
You plan to use AzCopy to copy data to storage1.
You need to identify the storage services in storage1 to which you can copy the data.
Which storage services should you identify?


- A. blob, file, table, and queue
- B. blob and file only
- C. file and table only
- D. file only
- E. blob, table, and queue only

Correct Answer: B

Community vote distribution



B (100%)

-   **rrabeya**



Highly Voted 

 3 years, 7 months ago



Correct Answer B - blob and file only
Azure Import job supports: Azure Blob Storage, and Azure Files storage
Azure Export job supports: Azure Blob Storage


<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-requirements>
upvoted 31 times
-   **boom666** 3 years, 7 months ago

Why do you refer to Import/Export here? I would refer to documentation about azcopy copy command instead - <https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>

upvoted 14 times
-   **zr79** 3 years, 2 months ago



This is Azcopy and not Import/Export tool

upvoted 10 times
-   **riclamer**



Highly Voted 

 3 years, 6 months ago



**** The new version 7.3 version of AZCOPY, now copy Azure Table... So this question maybe was updated in exam Az-104 . Reference --> <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#download-azcopy>

upvoted 27 times
-   **tableton** 1 year, 1 month ago

AzCopy support for table storage has been dropped in the latest versions.

upvoted 3 times
-   **LHNING2** 3 years, 2 months ago



Version 7.3 is not new, it is old version...


upvoted 5 times
-   **epomatti** 3 years ago

Wrong. New version is v10.

Only Blobs and Files are supported.

Provided answer "B" is correct.



upvoted 28 times
-   **[Removed]**

Most Recent 



 8 months ago

Selected Answer: B

B is corerct

upvoted 1 times
-   **tashakori** 1 year, 1 month ago

B is correct

upvoted 1 times
-   **Amir1909** 1 year, 2 months ago

B is correct

upvoted 1 times

  **Babustest** 1 year, 7 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

upvoted 1 times

  **Babustest** 1 year, 7 months ago

Correct answer. Only Blobs and files.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

upvoted 1 times

  **CarlosMarin** 1 year, 8 months ago

This question was in my exam on 31/08/2023.

upvoted 3 times



  **Mehedi007** 1 year, 9 months ago

Selected Answer: B

"AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account."

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

upvoted 4 times

  **Siraf** 1 year, 11 months ago

Correct answer is B:

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

upvoted 3 times

  **shadad** 2 years, 2 months ago

I took Exam of Azure- 104 at 27/2/2023

I score 920 points out of 1000 points. This was on it and my answer was: B - blob and file only

upvoted 5 times

  **mdwSysOps** 2 years, 2 months ago



Selected Answer: B

The correct answer is B - blob and file only.

AzCopy is a command-line utility used to copy data to and from various Azure services, including Azure Blob storage and Azure File storage. Table storage and Queue storage are not supported by AzCopy for data transfer.

Therefore, when identifying the storage services to which you can copy the data using AzCopy, you should identify blob and file storage only. This means that you can copy data to blob storage or file storage in the storage account named storage1 using AzCopy.

upvoted 3 times

  **zellck** 2 years, 2 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#authorize-azcopy>

upvoted 2 times

  **wwwmmm** 2 years, 3 months ago



choose B,

now azcopy v10 only supports blob and file type, v7.3 which is old version also supports table, but none of them support queue

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

<https://stackoverflow.com/questions/32023572/azcopy-include-tables-and-queues>

upvoted 1 times

  **rj9102** 2 years, 5 months ago

A service shared access signature (SAS) delegates access to a resource in just one of the storage services: Azure Blob Storage, Azure Queue Storage, Azure Table Storage, or Azure Files.


<https://learn.microsoft.com/en-us/rest/api/storageservices/create-service-sas>

upvoted 1 times

  **Davindra** 2 years, 5 months ago

It was in exam on 11/23

upvoted 8 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B

B) "blob and file only"

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy#synopsis>

upvoted 5 times

HOTSPOT -

You have an Azure Storage account named storage1 that uses Azure Blob storage and Azure File storage.

You need to use AzCopy to copy data to the blob storage and file storage in storage1.

Which authentication method should you use for each type of storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Blob storage:

	▼
Azure Active Directory (Azure AD) only	
Shared access signatures (SAS) only	
Access keys and shared access signatures (SAS) only	
Azure Active Directory (Azure AD) and shared access signatures (SAS) only	
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)	

File storage:

	▼
Azure Active Directory (Azure AD) only	
Shared access signatures (SAS) only	
Access keys and shared access signatures (SAS) only	
Azure Active Directory (Azure AD) and shared access signatures (SAS) only	
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)	

Correct Answer:

Answer Area

Blob storage:

	▼
Azure Active Directory (Azure AD) only	
Shared access signatures (SAS) only	
Access keys and shared access signatures (SAS) only	
Azure Active Directory (Azure AD) and shared access signatures (SAS) only	
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)	

File storage:

	▼
Azure Active Directory (Azure AD) only	
Shared access signatures (SAS) only	
Access keys and shared access signatures (SAS) only	
Azure Active Directory (Azure AD) and shared access signatures (SAS) only	
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)	

You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.

Box 1:

Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage.

Box 2:

Only Shared Access Signature (SAS) token is supported for File storage.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

 **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.

Box 1: Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage.

Box 2: Only Shared Access Signature (SAS) token is supported for File storage.



Reference:



<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>



upvoted 240 times

 **KevinR97** 1 year, 2 months ago



Now both valid for Fileshare and Blobs
<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-files>
upvoted 20 times


  **cosmicT73** 3 months, 4 weeks ago
File shares can support AD credentials only if the operations are targeting directly files and directories, however if it target the storage account or the file share itself then SAS only is supported..so in that question it is AD &SAS for blob , and SAS only for file storage
upvoted 2 times



  **RishiRawal** 1 year, 11 months ago
why not access keys for blob?
upvoted 2 times



  **obaemf** 1 year, 11 months ago
Because AzCopy only supports Azure AD & SAS.

AzCopy >> Blob supports both Azure AD & SAS
AZCopy >> File supports SAS only
upvoted 9 times

  **riseme2476** 1 year, 2 months ago
I checked this source (<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#authorize-azcopy>) with wayback machine, and now I can say that they edited it after EntraID rebranding. Year ago, there was clear statement about using AD for only blob storage, but now it is not mentioned at all. So I thing now we can you AD for File Shares too. (sorry for bad England btw)
upvoted 8 times




  **tableton** 1 year, 1 month ago
I agree
Both Azure Active Directory (AD) and Shared Access Signature (SAS) token
<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>
upvoted 4 times

  **klexams** 2 years, 6 months ago
Emphasising this is in the context of AZcopy
upvoted 3 times

  **joergsi** 3 years, 4 months ago
Authorize AzCopy
You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.


Use this table as a guide:

AUTHORIZE AZCOPY
Storage type Currently supported method of authorization
Blob storage Azure AD & SAS
Blob storage (hierarchical namespace) Azure AD & SAS
File storage SAS only
upvoted 15 times

  **waterzhong** Highly Voted  4 years, 4 months ago
Authorize AzCopy
You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.



Use this table as a guide:

AUTHORIZE AZCOPY
Storage type Currently supported method of authorization
Blob storage Azure AD & SAS
Blob storage (hierarchical namespace) Azure AD & SAS
File storage SAS only
upvoted 39 times

  **bob_az7** Most Recent  2 months ago
Box 1: Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage

Box 2: Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>
upvoted 2 times

  **vrn1358** 5 months, 1 week ago
Today, 11 Nov 2024, Microsoft supports for File share, both Azure AD & SAS to authenticate

Box 1: Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage.

Box 2: Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage.
upvoted 4 times

- [Removed]** 8 months ago

CORRECT

upvoted 2 times
- a3432e2** 11 months, 3 weeks ago

Correct Answer:
Box 1: Azure AD & SAS(Blob storage)
Box 2: SAS (File storage)
There is no recent change to this, the links individuals are posting assuming that File Storage is supported via AD is incorrect.

upvoted 1 times
- tableton** 1 year, 1 month ago

I think this has been updated now, you can use EntraID to azcopy files too
"If you want to upload files to an Azure file share, then verify that the Storage File Data Privileged Reader has been assigned to your security principal."

upvoted 1 times
- tableton** 1 year, 1 month ago

File Storage:
"Azure Active Directory (AD) and Shared Access Signature (SAS) only "
<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

upvoted 3 times
- Amir1909** 1 year, 1 month ago

Given answer is rigt

upvoted 1 times
- tashakori** 1 year, 1 month ago

Given answer is correct

upvoted 1 times
- Arash123** 1 year, 1 month ago

Finally tested Fileshare vs AzCopy:
You cannot copy files to a share by AzCopy when you authenticated via AzureAD. The error is:
failed to parse user input due to error: azure files only supports the use of SAS token authentication

upvoted 2 times
- Amir1909** 1 year, 2 months ago

Correct

upvoted 1 times
- MSBITSM** 1 year, 2 months ago

For commands that target files and directories, you can now provide authorization credentials by using Microsoft Entra ID and omit the SAS token from those commands.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-files?source=recommendations#get-started>

upvoted 2 times
- rajlmok** 1 year, 3 months ago

Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for BOTH Blob and File storage.

upvoted 9 times
- tableton** 1 year, 1 month ago

Agree: <https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

upvoted 1 times
- CarlosMarin** 1 year, 8 months ago

This question was in my exam on 31/08/2023.

upvoted 4 times
- ment0s** 1 year, 8 months ago

This question is unclear. There is a difference between what one "should" use, and what all possible options are.

upvoted 2 times
- Mehedi007** 1 year, 9 months ago

AAD & SAS only for Blob storage.
SAS only for File storage.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#authorize-azcopy>

upvoted 1 times
- itismadu** 7 months ago

From the link provided



[Authorize AzCopy](#)
You can provide authorization credentials by using Microsoft Entra ID, or by using a Shared Access Signature (SAS) token.

upvoted 1 times

  **itismadu** 7 months ago

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-files>

upvoted 1 times

  **NYTK** 1 year, 9 months ago

Came in exams 21/7/2023.

upvoted 3 times

You have an Azure subscription that contains an Azure Storage account.

You plan to create an Azure container instance named container1 that will use a Docker image named Image1. Image1 contains a Microsoft SQL Server instance that requires persistent storage.

You need to configure a storage service for Container1.

What should you use?



- A. Azure Files
- B. Azure Blob storage
- C. Azure Queue storage
- D. Azure Table storage


Correct Answer: A

Community vote distribution

A (94%)



5%

-   **waterzhong**



Highly Voted 

 4 years, 5 months ago



Correct answer should be Azure Files

upvoted 150 times
-   **wooyourdaddy** 4 years, 5 months ago



Where did you validate this from ?

upvoted 1 times
-   **RoastChicken** 3 years, 9 months ago

Azure table is unstructured data. Answer should be Azure Files.



upvoted 8 times
-   **ngamabe** 3 years, 9 months ago

I agree



upvoted 1 times
-   **JimBobSquare101** 3 years, 9 months ago

I would also consider the answer to be A: Files



Reason being the word persistent in the question....

upvoted 12 times
-   **photon99** 1 year, 6 months ago

Reason is for the mounting of the File shares from within the linux container you need file shares.



upvoted 3 times
-   **abu3lia** 4 years, 5 months ago

Correct, here is the proof: <https://azure.microsoft.com/en-us/blog/persistent-docker-volumes-with-azure-file-storage/>

upvoted 35 times
-   **epomatti** 3 years ago



This plugin has been deprecated for 6 years now.... it migrated to native Docker:

<https://docs.docker.com/cloud/aci-integration/#using-azure-file-share-as-volumes-in-aci-containers>

upvoted 2 times
-   **Acai** 3 years, 9 months ago



I agree, Here's another link if you're still skeptical


<https://docs.microsoft.com/en-us/azure/aks/concepts-storage#persistent-volumes>

upvoted 9 times
-   **epomatti** 3 years ago

This link is for AKS, and AKS support blobs.

The question is about ACI.

upvoted 5 times
-   **fedztadz**

Highly Voted 

 4 years, 4 months ago

Answer is not Correct. It should be A "Azure Files"

Azure files are used as persistent disks for docker images. It doesn't matter the type of the image or its functionality.

upvoted 114 times

  **[Removed]** Most Recent 8 months ago

Selected Answer: A

A is corerct

upvoted 2 times

  **varinder82** 11 months, 3 weeks ago

Final Answer:

A "Azure Files"

Azure files are used as persistent disks for docker images. It doesn't matter the type of the image or its functionality.

upvoted 1 times

  **MCLC2021** 11 months, 3 weeks ago

Selected Answer: A

To configure persistent storage for your Azure Container Instance (ACI) named container1, you should use Azure Files. Azure Files provides fully managed file shares in the cloud that can be mounted as volumes in ACI containers. It allows you to store and share data across multiple containers and instances, making it suitable for your SQL Server instance's storage needs. <https://learn.microsoft.com/es-es/azure/container-instances/container-instances-volume-azure-files>

upvoted 1 times

  **tashakori** 1 year, 1 month ago

B is right answer

upvoted 1 times

  **Amir1909** 1 year, 2 months ago

B is correct

upvoted 1 times

  **Rams786** 1 year, 7 months ago

This question was on my exam on 22 Sep 2023. scored 900 i answered Azure Files

upvoted 7 times

  **nmnm22** 1 year, 7 months ago


did you study all these 500 questions of dumps?

upvoted 2 times

  **Vicky83574** 1 year, 7 months ago

Is it any practical questions like write a code or labs are came in exam?

upvoted 1 times

  **james2033** 1 year, 8 months ago

Selected Answer: A

Azure Files for Azure Docker container , see <https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files>

upvoted 3 times

  **Mehedi007** 1 year, 9 months ago



Selected Answer: A

Azure Files.

<https://azure.microsoft.com/en-us/blog/persistent-docker-volumes-with-azure-file-storage/>

Passed the exam on 26 July 2023. Scored 870. Exact question came.

upvoted 3 times

  **Teroristo** 1 year, 9 months ago

Answer is Azure Files

In Azure container instances, you can mount Azure File shares for persistent storage. Azure files are used as persistent disks for docker images. It doesn't matter the type of the image or its functionality.



Persistent shared storage for containers. Easily share data between containers using NFS or SMB file shares. Azure Files is tightly integrated with Azure Kubernetes Service (AKS) for easily storing and managing data.

Reference:

<https://azure.microsoft.com/en-us/blog/persistent-docker-volumes-with-azure-file-storage>

<https://azure.microsoft.com/en-us/services/storage/files/#features>

upvoted 3 times



  **NYTK** 1 year, 9 months ago



Came in exams 21/7/2023. Answered A



upvoted 2 times

  **JunetGoyal** 2 years ago

Container instance has a temporary storage, but it got deleted when container is deleted .
As Question mentioned persistent we can use Either Managed disk or Azure file share with standard or premium sku. Also Azure file share can share to multiple instances
Means: any of these storage will keep the data and remain for future use even we delete the Container instance.
upvoted 6 times



  **Gaskonader** 2 years, 1 month ago
On Exam 30/03/2023
upvoted 5 times



  **Phil_Spencer** 2 years, 1 month ago
Never run a DB in a container.
upvoted 6 times

  **shadad** 2 years, 2 months ago

Selected Answer: A

I took Exam of Azure- 104 at 27/2/2023
I score 920 points out of 1000 points. This was on it and my answer was: A
upvoted 8 times

  **amzash** 2 years, 2 months ago
Congrats! thats a really good score. do you know how many of the questions from this website?
upvoted 2 times

  **mdwSysOps** 2 years, 2 months ago

Selected Answer: A

A. Azure Files

Azure Files is the recommended storage service for use with Azure Container Instances when you need to share data between containers or persist data across container restarts. Since Image1 contains a Microsoft SQL Server instance that requires persistent storage, you should use Azure Files as the storage service for container1.

Azure Blob storage, Azure Queue storage, and Azure Table storage are not recommended for use with Azure Container Instances when you need to persist data across container restarts. These storage services are more appropriate for other types of data storage and retrieval scenarios.
upvoted 10 times

You have an app named App1 that runs on two Azure virtual machines named VM1 and VM2. You plan to implement an Azure Availability Set for App1. The solution must ensure that App1 is available during planned maintenance of the hardware hosting VM1 and VM2. What should you include in the Availability Set?



- A. one update domain
- B. two fault domains
- C. one fault domain
- D. two update domains


Correct Answer: D

Community vote distribution

D (85%)

B (15%)

-   **mlantonis**

Highly Voted 

 3 years, 11 months ago

Correct Answer: D



When you create an Availability Set, the hardware in a location is divided into multiple update domains and fault domains.



An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.



VMs in the same fault domain share common storage as well as a common power source and network switch.



During scheduled maintenance, only one update domain is updated at any given time. Update domains aren't necessarily updated sequentially. So, we need two update domains.



Reference:



<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets>
<https://docs.microsoft.com/en-us/azure/virtual-machines/manage-availability>
<https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-and-updates>
upvoted 192 times
-   **Omar_Aladdin** 3 years, 7 months ago


Planned Maintenance "FOR THE HARDWARE ((HOSTING))"
I'm SURE "two fault domains" is the correct answer
upvoted 10 times
-   **bbhagya12** 3 years, 3 months ago

If it is maintinance - Update domain
If it is hardware failed - Fault Domain
Correct Ans is D
upvoted 38 times
-   **Lazylinux** 2 years, 10 months ago



If it is hardware failed - Fault Domain ==> Incorrect Sir ==> hardware failure or maintenance are same and means you lost update domain
on other hand Rack failure or maintenance are FAULT DOMAINS!
upvoted 3 times
-   **SilverFox22** 3 years, 7 months ago

"Microsoft updates, which Microsoft refers to as planned maintenance events, sometimes require that VMs be rebooted to complete the update." Planned maintenance refers to update domains, not fault domains. We need two update domains, answer is D.
upvoted 8 times
-   **Renz123** 1 year, 6 months ago

its mlantonis
upvoted 5 times
-   **Parsec**



Highly Voted 



 4 years, 5 months ago



It's "planned maintenance of the HARDWARE" in the question, not OS or software update. Should be 2 fault domains imho.
upvoted 36 times
-   **janshal** 4 years, 4 months ago



Hi the answer is D:
the Q talk about the hardware hosting VM1 and VM2.



the hardware, meaning the Server containing the VMs (Called Update domain).
During a Planed maintenance the update domains are shutdown one at a time. so D is ther right answer
upvoted 37 times

  **HuseinHasan** 4 years, 4 months ago
what will happen if the fault domain crashes, thats why i would go with two fault domains
upvoted 1 times



  **Alir95** 4 years ago
The question is specific to "Planned Maint", not outages and redundancy ... D is right.
upvoted 7 times

  **sandipk91** 3 years, 8 months ago
your assumption is wrong as they are talkin about planned maintenance
upvoted 2 times

  **wgalan** 1 year, 10 months ago
Is a trick answer using the "hardware" to steer you towards the fault domain answer, but the keyword is "planned maintenance" that's why D is the correct answer
upvoted 2 times



  **1d07c8e** Most Recent 6 months, 1 week ago
Correct answer is still D. In case there is any confusion, update domains are for “planned”maintenance.



<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets> <https://docs.microsoft.com/en-us/azure/virtual-machines/manage-availability> <https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-and-updates>
upvoted 1 times

  **[Removed]** 8 months ago



Selected Answer: D



D is corerct
upvoted 1 times



  **pverma20** 12 months ago
when hardware failure, fault domain need to use. If update such as windows update that require system reboot, update domain is use. So it should be fault tolerance I blv.
upvoted 2 times



  **moadabdou** 1 year, 1 month ago
The correct answer is: B. Two fault domains.



Explanation: An availability set in Azure is a way to ensure high availability of applications by distributing them across multiple distinct physical servers called fault domains. Each fault domain shares a common underlying infrastructure, such as power and cooling, but is isolated from other fault domains. Thus, if an issue occurs in one of the fault domains, the other domains remain operational, ensuring the continuous availability of applications. In this case, by having two fault domains, the availability set will ensure that App1 remains available during planned maintenance of the hardware hosting VM1 and VM2.
upvoted 2 times

  **cosmicT73** 3 months, 4 weeks ago
fault domain is mainly to protect against the unplanned failures , while update domains are for the planned system maintenance which is the correct answer here (2 update domains) ..fault domain is not related to that case
upvoted 1 times

  **tashakori** 1 year, 1 month ago
D is right
upvoted 1 times

  **1828b9d** 1 year, 2 months ago
This question was in exam 01/03/2024
upvoted 1 times

  **WeepingMaplte** 1 year, 5 months ago
Fault Domains = Physical Rack sharing power and network. Unplanned maintenance. Max 3
Update Domains = Logical grouping of virtual machine. Allows restarts/planned maintenance. Max 20.
Ref: <https://youtu.be/BGcKAXMBmcs?si=1-aPQzYi1wQ-DRbG>
upvoted 1 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: D

keywords: planned maintenance.
"The order of update domains being rebooted may not proceed sequentially during planned maintenance, but only one update domain is rebooted at a time."
<https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview#how-do-availability-sets-work>
upvoted 1 times

  **Pakawat** 1 year, 10 months ago

Found this Q in the exam, 3/7/2023

upvoted 5 times

🗨️ 👤 **xRiot007** 1 year, 11 months ago

I think MS needs to merge these 2 because they create confusion. If a system is down, then it's down and can't serve your customers. The reason is irrelevant, be it maintenance or an unexpected failure of whatever nature. In concept, update and failure domains should coincide.

upvoted 2 times

🗨️ 👤 **margotfrpp** 2 years ago

Selected Answer: B

Fault domains represent separate racks in the data center and protect against single points of failure.

Update domains protect against planned maintenance and software updates.

It is best practice to place VMs across multiple fault domains and update domains for the highest level of availability.

Therefore, in this scenario, including two fault domains in the Availability Set will ensure that the application remains available during planned maintenance of the hardware hosting VM1 and VM2.

upvoted 5 times

🗨️ 👤 **vbohr899** 2 years, 2 months ago

Cleared Exam today 26 Feb, This question was there in exam.

upvoted 6 times

🗨️ 👤 **zellck** 2 years, 2 months ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview#how-do-availability-sets-work>

Update domains indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time. When more than five virtual machines are configured within a single availability set with five update domains, the sixth virtual machine is placed into the same update domain as the first virtual machine, the seventh in the same update domain as the second virtual machine, and so on. The order of update domains being rebooted may not proceed sequentially during planned maintenance, but only one update domain is rebooted at a time. A rebooted update domain is given 30 minutes to recover before maintenance is initiated on a different update domain.

upvoted 2 times

🗨️ 👤 **Ashfaque_9x** 2 years, 3 months ago

Selected Answer: D

Passed today on 29Jan23 with a score of 970. This question was in the exam.

Correct Answer:

D. two update domains

upvoted 9 times

🗨️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: D

D) "two update domains"

To assure that during planned maintenance at least 1 VM is still operational, 2 Update Domains need to be created.

Each VM will be in its respective Update Domain.

upvoted 4 times



You have an Azure subscription named Subscription1.
You have 5 TB of data that you need to transfer to Subscription1.
You plan to use an Azure Import/Export job.
What can you use as the destination of the imported data?


- A. an Azure Cosmos DB database
- B. Azure Blob storage
- C. Azure Data Lake Store
- D. the Azure File Sync Storage Sync Service

Correct Answer: B

Community vote distribution



B (100%)

-   **Phani1701**



Highly Voted 


 2 years, 11 months ago

Azure blob storage and Azure files are the one's for azure import/export service to securely transfer data to Azure by shipping the data from disk drives,

upvoted 16 times
-   **Holydud** 2 years, 8 months ago

Was on exam 19 Aug 2022. Scored 870. Answered B

upvoted 8 times
-   **Lazylinux**



Highly Voted 


 2 years, 10 months ago

Selected Answer: B

I Luv Honey because it is B here is summary

There are two versions of WAImportExport:
*Version 1 for import/export into Azure Blob Storage
*Version 2 for import into Azure Files
*It is WAImportExport.exe ONLY compatible with 64-bit Windows
*Modify the driveset.csv file in the root folder where the tool resides.
*Modify the dataset.csv file in the root folder where the tool resides. Depending on whether *you want to import a file or folder or both, add entries in the dataset.csv file
*The maximum size of an Azure Files Resource of a file share is 5 TB



upvoted 14 times
-   **[Removed]**

Most Recent 



 8 months ago

Selected Answer: B



B is corerct

upvoted 1 times
-   **[Removed]** 7 months, 3 weeks ago

only Blob Storage & File Storage can be exported



upvoted 1 times
-   **rajneeshverma2020** 1 year, 4 months ago

Repeated question



upvoted 1 times
-   **Mehedi007** 1 year, 9 months ago

Selected Answer: B

Azure blob storage
<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>

upvoted 1 times
-   **zellck** 2 years, 2 months ago

Same as Question 63.
<https://www.examttopics.com/discussions/microsoft/view/98317-exam-az-104-topic-3-question-63-discussion>

upvoted 2 times
-   **zellck** 2 years, 2 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service>
Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.


upvoted 3 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: B



It's Blob

upvoted 2 times

  **Davindra** 2 years, 5 months ago



It was in exam on 11/23

upvoted 6 times

  **majerly** 2 years, 7 months ago

today in exam ,is B

upvoted 1 times

  **NaoVaz** 2 years, 7 months ago

Selected Answer: B


B) " Azure Blob storage"

Reference: <https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>

upvoted 3 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Correct Answer: B 



Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

Note:

There are several versions of this question in the exam. The question has two correct answers:



1. Azure File Storage
2. Azure Blob Storage

upvoted 3 times

  **Exilic** 2 years, 7 months ago

So you can choose any of the 2 answers?

upvoted 1 times

  **Exilic** 2 years, 7 months ago

I mean, any of the 2 that is available on that certain question.

upvoted 1 times

  **manalshowaei** 2 years, 10 months ago

Selected Answer: B

B. Azure Blob storage



upvoted 1 times

  **Scoobysnaks86** 2 years, 11 months ago

Selected Answer: B

B. Only does blob and file storage

upvoted 1 times

  **Racinely** 2 years, 11 months ago

Selected Answer: B

Look documentation Only azure blob and azure file share are supported by import/export

upvoted 2 times

DRAG DROP -

You have an Azure subscription that contains an Azure file share.

You have an on-premises server named Server1 that runs Windows Server 2016.

You plan to set up Azure File Sync between Server1 and the Azure file share.

You need to prepare the subscription for the planned Azure File Sync.

Which two actions should you perform in the Azure subscription? To answer, drag the appropriate actions to the correct targets. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Actions

Create a Storage Sync Service

Install the Azure File Sync agent

Create a sync group

Run Server Registration

Answer Area

First action:

Action

Second action:

Action

Correct Answer:

Actions

Create a Storage Sync Service

Install the Azure File Sync agent

Create a sync group

Run Server Registration

Answer Area

First action:

Create a Storage Sync Service

Second action:

Create a sync group

  **gujjudesi420**  4 years ago

I think answer should be Create Storage Sync Service, Create a Sync Group as they are asking for "Which two actions should you perform in the Azure subscription?"

upvoted 420 times

  **swk1_az104** 3 months, 3 weeks ago

I think in the question of "<https://www.examtopics.com/exams/microsoft/az-104/view/171/>" you find the answer.

"You have an on-premises file server named Server1 that runs Windows Server 2016.

You have an Azure subscription that contains an Azure file share.

-> You deploy an Azure File Sync Storage Sync Service, and you create a sync group.

You need to synchronize files from Server1 to Azure.



Which three actions should you perform in sequence?"

upvoted 1 times

  **Praveen66** 3 years, 8 months ago

Agree with you, its actions on the subscription/azure portal and does not ask for actions on the server

upvoted 12 times

  **xupiter** 3 years, 10 months ago

Correct.

Link: <https://docs.microsoft.com/en-us/learn/modules/extend-share-capacity-with-azure-file-sync/5-set-up-azure-file-sync>

upvoted 4 times

  **mcc** 3 years, 6 months ago

correct:

Create Azure resources: You need a storage account to contain a file share, a Storage Sync Service, and a sync group. Create the resources in that order.

upvoted 8 times

  **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

First action: Create a Storage Sync Service

The deployment of Azure File Sync starts with placing a Storage Sync Service resource into a resource group of your selected subscription.

Second action: Install the Azure File Sync agent

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share.


1. Prepare Windows Server to use with Azure File Sync
2. Deploy the Storage Sync Service
3. Install the Azure File Sync agent
4. Register Windows Server with Storage Sync Service
5. Create a sync group and a cloud endpoint
6. Create a server endpoint
7. Configure firewall and virtual network settings

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

<https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#deploy-the-storage-sync-service>

upvoted 243 times

  **augustogcn** 3 years, 3 months ago

Install the Azure File Sync agent is not an action that you can perform in the Azure Subscription. The file Sync agent is installed on your on-premises server. This question is a tricky one.

upvoted 25 times

  **chaudha4** 3 years, 11 months ago

The question is about what you do in your Azure subscription. The second action that you suggest cannot be done on your subscription. It needs to be done on the on-prem server.

upvoted 9 times

  **suriyaswamy** 3 years, 8 months ago

Nice explanation

upvoted 2 times

  **Praveen66** 3 years, 8 months ago

But the question talks about actions on the subscription and not on the servers.

so it should be

First action: Create a Storage Sync Service

Second action: Create a sync group

upvoted 22 times

  **Jay_D_Lincoln** Most Recent 2 months, 4 weeks ago

First Action: Create a storage sync service

Second Action: Create a sync group

If you read the question again

- it did not ask for a sequence, like which two actions to take first. Keeping that in mind the second and the third action are both correct answer. That does not make sense

- It clearly asked "prepare the subscription" or "two (unique) actions that you need to perform in the subscription". It did not mention any action need to taken from the on-prem server side.

Check the below doc to see which two actions can be done on the Azure side. Do not focus on the sequence. Question did not ask about sequence.

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>

upvoted 1 times

  **sca88** 5 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>

The answer is correct:

"The deployment of Azure File Sync starts with placing a Storage Sync Service resource into a resource group of your selected subscription. We recommend provisioning as few of these as needed. You'll create a trust relationship between your servers and this resource. A server can only be registered to one Storage Sync Service. As a result, we recommend deploying as many storage sync services as you need to separate groups of servers. Keep in mind that servers from different storage sync services can't sync with each other."

upvoted 1 times

  **117b84e** 7 months, 1 week ago

chatgpt

Actions to place:

Create a storage sync service: This sets up the service in Azure to manage the sync process.
Create a sync group: This links the storage sync service with your endpoints (Azure file share and Server1).
upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago
WRONG

1. Create Storage Sync Service
2. Create a Sync Group

since the question states the performing in the Azure subscription.
upvoted 4 times

🗨️ 👤 **Aiyooo** 1 year, 6 months ago
This is one of the stupidest questions
upvoted 10 times

🗨️ 👤 **clg003** 1 year, 6 months ago
All of these are steps of Azure File Sync but only two of them are actually performed within the subscription (in Azure). Deploy a Storage Sync Service and Create a sync group are the answer.
upvoted 3 times

🗨️ 👤 **iamchoy** 1 year, 7 months ago
For Azure File Sync setup, you first create necessary services in Azure before setting up the on-premises server. Here are the initial steps in the Azure subscription:

****Create a Storage Sync Service****: This service is the top-level resource for Azure File Sync. It is used to create and manage sync groups and registered servers.

****Create a sync group****: After setting up the Storage Sync Service, you create a sync group which defines the sync topology for a set of files. The endpoints within a sync group are kept in sync with each other.

Steps involving the Azure File Sync agent and server registration are done on the on-premises server, not directly in the Azure subscription.

So, the first two actions in the Azure subscription are:

1. Create a Storage Sync Service
2. Create a sync group.

upvoted 4 times

🗨️ 👤 **18c2076** 1 year, 1 month ago
Right.... But don't you need a server endpoint before you can create a sync group?
Which would imply you need to install the agent despite "preparing the subscription"
upvoted 1 times

🗨️ 👤 **raj_raj22** 1 year, 7 months ago
as per the step in MS azure file sync.. the posted answers are correct.
upvoted 1 times

🗨️ 👤 **ikidreamz** 1 year, 8 months ago
In my view, Can you proceed to next steps without the agent ? I think the answer is right becoz YOU cannot go to next step without the agent installed and also the selection choice is poorly worded it should match the steps <https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#register-windows-server-with-storage-sync-service>
upvoted 1 times

🗨️ 👤 **Mehedi007** 1 year, 9 months ago
Create a Storage Sync Service,
Install the Azure File Sync agent

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>
upvoted 1 times

🗨️ 👤 **KiwE** 1 year, 9 months ago
For those of you who are struggling with all the filesynch questions there's a reason - it was removed from the AZ-104 exam Oct 2022
<https://intunedin.net/2022/10/11/exam-az-104-microsoft-azure-administrator-resource-guide-october-2022-update/>
upvoted 6 times

🗨️ 👤 **rajneeshverma2020** 1 year, 4 months ago
Still there <https://intunedin.net/2023/12/01/az-104-microsoft-azure-administrator-exam-resource-guide-october-2023-update/>
upvoted 1 times

🗨️ 👤 **Teroristo** 1 year, 9 months ago
Second action: Create a sync group.
A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on a registered server. A server can have server endpoints in multiple sync groups. You can create as many sync groups as you need to appropriately describe your desired sync topology.
upvoted 1 times

🗨️ 👤 **Josete1106** 1 year, 9 months ago

Correct: Create Storage Sync Service & Create a Sync Group
upvoted 2 times

🗨️ 👤 **ExamKiller020** 1 year, 10 months ago

In your exam you wont get questions anymore about Azure Sync Service, they removed it sometimes last year. Please like this post sp everybody will see
upvoted 39 times

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

1. Deploy a Storage Sync Service.
 2. Create a sync group.
 3. Install Azure File Sync agent on the server with the full data set.
 4. Register that server and create a server endpoint on the share.
- upvoted 3 times

HOTSPOT -

You have an Azure subscription that contains the file shares shown in the following table.

Name	Location
share1	West US
share2	West US
share3	East US

You have the on-premises file shares shown in the following table.

Name	Server	Path
data1	Server1	D:\Folder1
data2	Server2	E:\Folder2
data3	Server3	E:\Folder2

You create an Azure file sync group named Sync1 and perform the following actions:

- ☞ Add share1 as the cloud endpoint for Sync1.
- ☞ Add data1 as a server endpoint for Sync1.
- ☞ Register Server1 and Server2 to Sync1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can add share3 as an additional cloud endpoint for Sync1.	<input type="radio"/>	<input type="radio"/>
You can add data2 as an additional server endpoint for Sync1.	<input type="radio"/>	<input type="radio"/>
You can add data3 as an additional server endpoint for Sync1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
You can add share3 as an additional cloud endpoint for Sync1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add data2 as an additional server endpoint for Sync1.	<input checked="" type="radio"/>	<input type="radio"/>
You can add data3 as an additional server endpoint for Sync1.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints.



Box 2: Yes -



Data2 is located on Server2 which is registered to Sync1.



Box 3: No -



Data3 is located on Server3 which is not registered to Sync1.



Reference:
<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-sync-group-and-a-cloud-endpoint>



  **cyna58** Highly Voted 4 years ago
NO - only one cloud endpoint can be added to sync1
YES - Server2 has been registered to Sync1 but data2 is not added to server endpoint. So we can add data2 as additional server endpoint for Sync1
NO - We have to register Server3 first
upvoted 198 times



  **23169fd** 11 months, 1 week ago
That's totally correct.
upvoted 1 times



  **op22233** 1 year ago
correct
upvoted 1 times

  **ABhi101** 3 years, 3 months ago
Correct
upvoted 2 times

  **josevirtual** 3 years, 1 month ago
I'm confused. If this is correct, why we could add data1 as a server endpoint before to register Server 1?
upvoted 2 times

  **itguy2** 3 years, 1 month ago
because the question mentioned that Server1 and Server2 are registered
upvoted 6 times

  **josevirtual** 3 years, 1 month ago
They are registered after data1 is added. It may not be relevant, but it makes me wonder if there is something tricky here...
upvoted 2 times

  **Testyboy15** 2 years, 10 months ago
I think the steps done aren't necessarily listed in order they were done. It is merely saying that is what has been.
upvoted 2 times



  **mlantonis** Highly Voted 3 years, 11 months ago
Correct Answer:



Box 1: No
A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints.



Box 2: Yes
Data2 is located on Server2 which is registered to Sync1.

Box 3: No
Data3 is located on Server3 which is not registered to Sync1.

Reference:
<https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-sync-group-and-a-%20cloud-endpoint>
upvoted 177 times

  **suriyaswamy** 3 years, 8 months ago
Accurate Info, Thanks
upvoted 3 times

  **awssecuritynewbie** 2 years, 6 months ago
but i thought you cannot add a new drive to the Sync group ? and the cloud server endpoint is mapped against drive "E". So how is it possible?
upvoted 2 times



  **cris_exam** Most Recent 2 months, 3 weeks ago
N - you can only have 1 Cloud Endpoint per Sync Group
Y - because you can have up to 99 registered servers to Sync1 and Server 2 is also registered
N - Server 3 is not registered to be able to find and add

Hope this info helps you guys understand the limits.

Cloud Endpoints
Maximum Number of Cloud Endpoints per Sync Group: 1 cloud endpoint1.
Maximum Number of Sync Groups per Storage Sync Service: 1001.
Maximum Number of Storage Sync Services per Subscription: 2001.

Server Endpoints
Maximum Number of Server Endpoints per Sync Group: 991.
Maximum Number of Registered Servers per Storage Sync Service: 991.
Maximum Number of Sync Groups per Server: 301.

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-scale-targets#azure-file-sync-scale-targets>
upvoted 1 times

  **cris_exam** 2 months, 3 weeks ago
correcting the numbers there a bit, sorry, it was copy/paste formatting issue

Cloud Endpoints
Maximum Number of Cloud Endpoints per Sync Group: 1 cloud endpoint.
Maximum Number of Sync Groups per Storage Sync Service: 100
Maximum Number of Storage Sync Services per Subscription: 200



Server Endpoints
Maximum Number of Server Endpoints per Sync Group: 99
Maximum Number of Registered Servers per Storage Sync Service: 99
Maximum Number of Sync Groups per Server: 30
upvoted 1 times

  **[Removed]** 8 months ago
CORRECT

No, a sync group must contain only one Cloud Endpoint and one or more Server Endpoints.



Yes, Data2 is on Server2 which is registered to Sync1.



No, Data3 is on Server3 which is not registered to Sync1.
upvoted 2 times



  **varinder82** 11 months, 3 weeks ago
Final Answer:
Box 1: No
A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints.

Box 2: Yes
Data2 is located on Server2 which is registered to Sync1.

Box 3: No
Data3 is located on Server3 which is not registered to Sync1.
upvoted 1 times



  **tashakori** 1 year, 1 month ago
Given answer is right
upvoted 1 times

  **Amir1909** 1 year, 2 months ago
Correct
upvoted 1 times

  **Mehedi007** 1 year, 9 months ago
N: "A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints."
<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-sync-group-and-a-cloud-endpoint>

Y: "A registered server can support multiple server endpoints, however a sync group can only have one server endpoint per registered server at any given time. Other server endpoints within the sync group must be on different registered servers."
<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-server-endpoint>

N: Data3 is located on Server3 which is not registered to Sync1.
upvoted 1 times



  **NaoVaz** 2 years, 7 months ago
1) You can add share3 as an additional cloud endpoint for Sync1: "No"
2) You can add data2 as an additional server endpoint for Sync1: "Yes"
3) You can add data3 as an additional server endpoint for Sync1: "No"



Explanation:



1) Only a single Cloud Endpoint can exist in a Sync group;
2) data2 is in a different server using a folder with a different name, and Server2 is already registered to Sync1.
3) Server3 is not yet registered.
upvoted 7 times



  **EmnCours** 2 years, 8 months ago



NO - only one cloud endpoint can be added to sync1
YES - Server2 has been registered to Sync1 but data2 is not added to server endpoint. So we can add data2 as additional server endpoint for Sync1
NO - We have to register Server3 first
upvoted 1 times



  **atilla** 2 years, 8 months ago
if server3 was registered was it possible to add as endpoint? since it has the same drive/folder
upvoted 2 times



  **anurag1122** 2 years, 5 months ago
I have the same question
upvoted 2 times



  **ericZX** 2 years ago
if server3 was registered, I guess yes.
on question 2, it's trying to add data2 only
on question 3, it's trying to add data3 only, not add data2 and data3 at the same time
upvoted 1 times



  **Socca** 2 years, 9 months ago
You can add one cloud endpoint to a sync so the first question is no .You can add only registred servers to the share that means only data2 can be added
upvoted 1 times

  **justjeroen** 2 years, 10 months ago
Box 3 is debate able. Yes you can add data 3, but you have to register first. Just need two steps to accomplish it.
upvoted 1 times

  **Lazylinux** 2 years, 10 months ago
NO-YES-NO and as per other comments
upvoted 1 times

  **manalshowaei** 2 years, 10 months ago
No Yes No
upvoted 1 times

  **Scoobysnaks86** 2 years, 11 months ago
I hate how these are a test of the English language and not actual knowledge.
upvoted 5 times

  **ajayasa** 3 years, 1 month ago
this question was there on 16/03/2022 with same question and passed with 900 percent
upvoted 2 times

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table:

Name	Type	Location	Resource group
RG1	Resource group	East US	Not applicable
RG2	Resource group	West US	Not applicable
Vault1	Recovery Services vault	West Europe	RG1
storage1	Storage account	East US	RG2
storage2	Storage account	West US	RG1
storage3	Storage account	West Europe	RG2
Analytics1	Log Analytics workspace	East US	RG1
Analytics2	Log Analytics workspace	West US	RG2
Analytics3	Log Analytics workspace	West Europe	RG1

You plan to configure Azure Backup reports for Vault1.

You are configuring the Diagnostics settings for the AzureBackupReports log.

Which storage accounts and which Log Analytics workspaces can you use for the Azure Backup reports of Vault1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Storage accounts:

▼

storage1 only

storage2 only

storage3 only

storage1, storage2, and storage3

Log Analytics workspaces:

▼

Analytics1 only

Analytics2 only

Analytics3 only

Analytics1, Analytics2, and Analytics3

Answer Area

Storage accounts:

▼

storage1 only

storage2 only

storage3 only

storage1, storage2, and storage3

Correct Answer:

Log Analytics workspaces:

▼

Analytics1 only

Analytics2 only

Analytics3 only

Analytics1, Analytics2, and Analytics3

Box 1: storage1, storage2, and storage3

The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your vaults exist.

Box 2: Analytics3 -

Vault1 and Analytics3 are both in West Europe.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-configure-reports>

- RithuNethra

Highly Voted

4 years, 5 months ago

storage 3
analytics 1,2 & 3
this is correct as analytics are independent of locations!
upvoted 443 times
- Bapan

3 years, 7 months ago

This is the correct one.
upvoted 3 times
- wooyourdaddy

4 years, 5 months ago

What did you use to verify this ?
upvoted 2 times
- Bogdan_85

2 years, 6 months ago

The answer is in here: "The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your vaults exist." Took from here: <https://learn.microsoft.com/en-us/azure/backup/configure-reports#1-create-a-log-analytics-workspace-or-use-an-existing-one>
upvoted 8 times
- af68218

1 year, 1 month ago

Tested that is still true just now. Created a bunch of new Log Analytics workspaces in various regions, and they all showed up as option for backing up in the vault after a few minutes. No storage accounts, however, showed, because I didn't have any in the same region as the vault.
upvoted 3 times
- Amju

4 years ago

its not recommended due to different government policies in US and Europe and thats why only workspace 3 is correct answer.
upvoted 9 times
- Jamie1337

3 years, 4 months ago

This is not correct, it asks what is possible not what is recommended. Others have confirmed 1,2,3 is the correct answer.
upvoted 7 times
- Veronika1989

4 years ago

I agree! Tested on my tenant.
upvoted 12 times
- mlantonis

Highly Voted

3 years, 11 months ago

Correct Answer:

Storage accounts: Storage 3 only
Storage Account must be in the same Region as the Recovery Services Vault.

Log Analytics workspaces: Analytics1, Analytics2, and Analytics3
Set up one or more Log Analytics workspaces to store your Backup reporting data. The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your Vaults exist.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/configure-reports#1-create-a-log-analytics-workspace-or-use-an-existing-one>
upvoted 429 times
- sca88

5 months, 2 weeks ago

Absolutelly agree with you. 1) Storage 3 only. 2) Analytics1, Analytics2, Analytics3
upvoted 2 times
- MandAsh

1 year, 1 month ago

You are the Batman! helping poor cloud'ers even after so many years.
upvoted 10 times
- Solution_2

1 year ago

Indeed , he is the chosen one.
upvoted 5 times
- aamalik7

3 years, 5 months ago

You are the superman!
upvoted 26 times
- happyaka

2 years, 10 months ago

I check your answer instead of the answer given by examtopics. You rock !!!
upvoted 7 times
- Abhisk127

Most Recent

3 months, 1 week ago

This question on exam dated:23 Jan 2025.
Box1:Storage 3
Box2:Analytics 1,2 & 3
this is correct as analytics are independent of locations!
upvoted 1 times

🗨️ 👤 **0378d43** 6 months, 3 weeks ago
Storage 3 due to location and Log Analytics Workspace is not location dependent its global resource
upvoted 1 times

🗨️ 👤 **[Removed]** 8 months ago
WRONG

Storage accounts: Storage 3 only
(Storage accounts must be in the same location of the Recovery Services vault).

Log Analytics workspaces: Analytics1, Analytics2, and Analytics3
(Log Analytics are independent of locations).
upvoted 2 times

🗨️ 👤 **tashakori** 1 year, 1 month ago
- storage 3 only
- analytics 1,2 & 3
upvoted 1 times

🗨️ 👤 **subinjarackal** 1 year, 1 month ago
Should the storage account, log analytics workspace be in the same resource group as valut1
upvoted 1 times

🗨️ 👤 **Wojer** 1 year, 3 months ago
Azure supports multiple types of storage accounts for different storage scenarios customers may have, but there are two main types of storage accounts for Azure Files. Which storage account type you need to create depends on whether you want to create a standard file share or a premium file share:

General purpose version 2 (GPv2) storage accounts: GPv2 storage accounts allow you to deploy Azure file shares on standard/hard disk-based (HDD-based) hardware. In addition to storing Azure file shares, GPv2 storage accounts can store other storage resources such as blob containers, queues, or tables. File shares can be deployed into the transaction optimized (default), hot, or cool tiers.

FileStorage storage accounts: FileStorage storage accounts allow you to deploy Azure file shares on premium/solid-state disk-based (SSD-based) hardware. FileStorage accounts can only be used to store Azure file shares; no other storage resources (blob containers, queues, tables, etc.) can be deployed in a FileStorage account.
upvoted 1 times

🗨️ 👤 **yukkki** 1 year, 3 months ago
storage: 3only
log: all
upvoted 2 times

🗨️ 👤 **Ahkhan** 1 year, 6 months ago
I tested. A log analytic workspace can be in different region than resources connected to it.
upvoted 1 times

🗨️ 👤 **kaizoogi** 1 year, 7 months ago
I think these answers need to be flipped:

Change From:
Box 1: storage1, storage2, and storage3
The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your vaults exist.

Box 2: Analytics3 -
Vault1 and Analytics3 are both in West Europe.


Change To:
Box 1: storage3
Vault1 and Analytics3 are both in West Europe.

Box 2: Analytics1, Analytics2, Analytics3 -
The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your vaults exist.
upvoted 5 times

🗨️ 👤 **CarlosMarin** 1 year, 8 months ago
This question was in my exam on 31/08/2023.
upvoted 5 times

🗨️ 👤 **msstanci_111** 1 year, 8 months ago
no way, storage accounts are not correct, sa must be in same region and same resource group.

upvoted 1 times

  **msstanci_111** 1 year, 8 months ago

Not at all storage account, and analytics 1,2,3 (only one of them). If I created sa and it was in different region or rg, I can't see sa. In my oppinion, those answers not cover right answer. (I tested it in lab)

upvoted 1 times

  **Mehedi007** 1 year, 9 months ago

Storage 3 only.

"the vault must be in the same region as the data source."

<https://learn.microsoft.com/en-us/azure/backup/backup-create-recovery-services-vault#create-a-recovery-services-vault>

Analytics1, Analytics2, and Analytics3.

"You can use a single workspace for all your data collection."

<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview>

upvoted 3 times

  **Josete1106** 1 year, 9 months ago

storage 3

analytics 1,2 & 3

Correct!

upvoted 1 times

  **[Removed]** 1 year, 10 months ago

Correct Answer:

Storage accounts:

Storage3 only, because Vault1 is West Europe and Storage3 is also in West Europe.

Log Analytics workspaces:

Analytics1, Analytics2 and Analytics3, becasue those analytics backup are not related to the location and subscription where your vaults exist..

<https://learn.microsoft.com/en-us/azure/backup/configure-reports?tabs=recovery-services-vaults>

Set up one or more Log Analytics workspaces to store your Backup reporting data. The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your vaults exist

upvoted 1 times

HOTSPOT -

You have an Azure subscription that contains the storage accounts shown in the following exhibit.

Storage accounts

Default Directory

+ Add

⚙ Manage view

🔄 Refresh

📄 Export to CSV

🏷 Assign tags

🗑 Delete

💡 Feedback

Filter by name...

Subscription == all

Resource group == all

Location == all

+ Add filter

Showing 1 to 4 of 4 records.

<input type="checkbox"/>	Name ↑	Type ↑	Kind ↑	Resource group ↑	Location ↑
<input type="checkbox"/>	contoso101	Storage account	StorageV2	RG1	East US
<input type="checkbox"/>	contoso102	Storage account	Storage	RG1	East US
<input type="checkbox"/>	contoso103	Storage account	BlobStorage	RG1	East US
<input type="checkbox"/>	contoso104	Storage account	FileStorage	RG1	East US

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can create a premium file share in

contoso101only

contoso104 only

contoso101 or contoso104 only

contoso101, contoso102, or contoso104 only

contoso101, contoso102, contoso103, or contoso104

You can use the Archive access tier in

contoso101only

contoso101 or contoso103 only

contoso101, contoso102, and contoso103 only

contoso101, contoso102, and contoso104 only

contoso101, contoso102, contoso103, and contoso104

Answer Area

You can create a premium file share in

contoso101only

contoso104 only

contoso101 or contoso104 only

contoso101, contoso102, or contoso104 only

contoso101, contoso102, contoso103, or contoso104

Correct Answer:

You can use the Archive access tier in

contoso101only

contoso101 or contoso103 only

contoso101, contoso102, and contoso103 only

contoso101, contoso102, and contoso104 only

contoso101, contoso102, contoso103, and contoso104

mlantonis

Highly Voted

 3 years, 11 months ago
Correct Answer:



Box 1: contoso104 only
Premium file shares are hosted in a special purpose storage account kind, called a FileStorage account.



Box 2: contoso101 and contoso103 only
Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering.
The archive tier supports only LRS, GRS, and RA-GRS.



Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>



<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-premium-fileshare?tabs=azure-portal>
<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>
upvoted 394 times

  **JayJay22215** 3 years, 2 months ago
Box 1: contoso104 only
Premium is available for blob as well, but it asked for "Premium File Shares"
Box 2: contoso101 and contos103 only
not available for normal storage. In addition to the ms docs list above, you can just check via the price calculator as well.
<https://azure.microsoft.com/de-de/pricing/calculator/>
upvoted 5 times



  **Katlegobogosi** 2 years ago
That "and or" seems to have confused alot of people.
I think you might have typed and instead of or.
But you are correct that is the answer
upvoted 2 times



  **Traian** 2 years, 7 months ago
Standard general-purpose v1 Blob Storage, Queue Storage, Table Storage, and Azure Files LRS/GRS/RA-GRS
Standard general-purpose v1 actually supports tiering check the redundancy options from the following link:
<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview>



The provided answer is correct 101,102,103
upvoted 3 times



  **Daan_peacock** 2 years, 7 months ago
Your link actually states the following: "Access tier refers to the data usage pattern you've specified for your general-purpose v2 or Blob Storage account."

So, 101 or 103 only
upvoted 6 times

  **atilla** 2 years, 8 months ago
contoso101 and contos103 only is not an option in the answers, it says contoso 101 or contoso 103 only
upvoted 5 times



  **Grande** 2 years, 8 months ago
contoso101 or contos103 only
upvoted 2 times



  **AzureJobsTillRetire** 2 years, 5 months ago
Hi ailla, I think in this context "contoso101 and contos103 only" and "contoso101 or contos103 only" have the same meaning
upvoted 3 times



  **Rajash** Highly Voted 4 years ago
Box1 - 104 only.
Box2 - 101 and 103 only (Storage V2 and BLOB storage)
<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

-Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering.
upvoted 85 times

  **Veronika1989** 3 years, 11 months ago
I agreed. Here is the article <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>
upvoted 4 times

  **Bravo_Dravel** Most Recent 3 months, 1 week ago
Box 1: Contoso104 only
Box 2: contoso101 and contos103 only.
General Purpose v1 (GPv1) accounts do not support tiering.
upvoted 2 times

  **Dankho** 7 months, 2 weeks ago
Box1: contoso104 only
Box3: contoso101 only
Why Box3 shouldn't include contoso103/BlobStorage - this is because BlobStorage implies that it's a Premium storage account. Premium storage account is in its own league and does not yet support hot, cool, archive data tiering, see - <https://learn.microsoft.com/en-us/azure/storage/blobs/storage-feature-support-in-storage-accounts>
upvoted 1 times

  **[Removed]** 8 months ago
WRONG

You can create a premium file share in: contoso104 only.
(Premium File share is supported only by FileStorage account)

You can use the Archive access tier in: contoso101 and contoso103 only.
(Archive access tier is supported in Blob Storage and General Purpose V2)
upvoted 2 times

🗨️ 👤 **Amir1909** 1 year, 2 months ago
Box 1: contoso104 only
Box 2: contoso101 and contoso103 only
upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 6 months ago
Blob storage is a legacy so 101 only for 2nd question
upvoted 1 times

🗨️ 👤 **Josete1106** 1 year, 9 months ago
Box 1: contoso104 only
Box 2: contoso101 and contoso103 only
upvoted 2 times

🗨️ 👤 **Mpalana** 1 year, 11 months ago
This question was in the exam 08June 2023
upvoted 6 times

🗨️ 👤 **wolf13** 1 year, 11 months ago
Box 2: You can use the Archive access tier in: contoso101 or contoso103 only
Contoso101 or Contoso103 only is correct as tiering in a Storage account is supported by only two types of storage accounts - BlobStorage and StorageV2.
You cannot configure any other type of storage accounts like Storage,FileStorage etc.
Note: The archive tier is not supported as the default access tier for a storage account.
Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts.
General Purpose v1 (GPv1) accounts don't support tiering.
The archive tier supports only LRS, GRS, and RA-GRS.
The archive tier isn't supported for ZRS, GZRS, or RA-GZRS accounts.
upvoted 1 times

🗨️ 👤 **ArronGC** 2 years ago
<https://images.squarespace-cdn.com/content/v1/5af21c03e17ba3f52f6d007b/1561741063599-OYAYQPVVN84F8TMRVKV/Table+comparing+Storage+Account+Types%2C+Services+and+Performance?format=1500w>

all you need for storage related capabilities
upvoted 4 times

🗨️ 👤 **sk4shi** 1 year, 10 months ago
Thanks for this ArronGC. This explains it all
upvoted 1 times

🗨️ 👤 **worldkalabe** 2 years ago
Box 1 is correct
Box 2 is just contoso101 and 103; here is why:
The general-purpose v1 storage account, which is the older version of the standard storage account, only supports two tiers: hot and cool. It doesn't support the archive tier.

However, if you have an existing general-purpose v1 storage account, you can use the Azure portal, Azure PowerShell, or Azure CLI to migrate it to the v2 kind, which then allows you to use the archive tier. Once you migrate a v1 storage account to v2, you can't revert it back to v1.
upvoted 2 times

🗨️ 👤 **keszi** 2 years, 2 months ago
Question was on the exam March 2023
upvoted 8 times



🗨️ 👤 **vbohr899** 2 years, 2 months ago
Cleared Exam today 26 Feb, This question was there in exam.
upvoted 6 times



🗨️ 👤 **zellck** 2 years, 3 months ago
1. contoso104 only
2. contoso 101 or contoso103 only

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-premium-fileshare>
FileStorage storage accounts: FileStorage storage accounts allow you to deploy Azure file shares on premium/solid-state disk-based (SSD-based) hardware. FileStorage accounts can only be used to store Azure file shares; no other storage resources (blob containers, queues, tables, etc.) can be deployed in a FileStorage account.
upvoted 2 times

🗨️ 👤 **Ashfaque_9x** 2 years, 3 months ago
Passed today on 29Jan23 with a score of 970. This question was in the exam.
Correct Answer:

Box 1: contoso104 only
Box 2: contoso101 and contoso103 only
upvoted 5 times

  **noorms** 2 years, 1 month ago
Hi, did the exam questions come from this dump?
upvoted 1 times

  **orionduo** 2 years, 3 months ago
contoso104 only
Premium file shares are hosted in a special purpose storage account kind, called a FileStorage account.

contoso101 and contoso103 only
Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering.
The archive tier supports only LRS, GRS, and RA-GRS.
upvoted 1 times

HOTSPOT -

You have an Azure subscription named Subscription1.

In Subscription1, you create an Azure file share named share1.

You create a shared access signature (SAS) named SAS1 as shown in the following exhibit:

Allowed services ⓘ

☐ Blob ☒ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ

☒ Read ☒ Write ☐ Delete ☒ List ☐ Add ☐ Create ☐ Update ☐ Process

Start and expiry date/time ⓘ

Start

2018-09-01 2:00:00 PM

End

2018-09-14 2:00:00 PM

(UTC+02:00) --- Current Timezone ---

Allowed IP addresses ⓘ

193.77.134.10-193.77.134.50

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Signing key ⓘ

key1

Generate SAS and connection string

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If on September 2, 2018, you run Microsoft Azure Storage Explorer on a computer that has an IP address of 193.77.134.1, and you use SAS1 to connect to the storage account, you **[answer choice]**.

	▼
will be prompted for credentials	
will have no access	
will have read, write, and list access	
will have read-only access	

If on September 10, 2018, you run the net use command on a computer that has an IP address of 193.77.134.50, and you use SAS1 as the password to connect to share1, you **[answer choice]**.

	▼
will be prompted for credentials	
will have no access	
will have read, write, and list access	
will have read-only access	

Answer Area

If on September 2, 2018, you run Microsoft Azure Storage Explorer on a computer that has an IP address of 193.77.134.1, and you use SAS1 to connect to the storage account, you [answer choice].

will be prompted for credentials

will have no access

will have read, write, and list access

will have read-only access

Correct Answer:

If on September 10, 2018, you run the net use command on a computer that has an IP address of 193.77.134.50, and you use SAS1 as the password to connect to share1, you [answer choice].

will be prompted for credentials



will have no access

will have read, write, and list access

will have read-only access

  **fedztedz** Highly Voted 4 years, 4 months ago



The Answer is not correct.
It should be no access for both cases.
- for first case, cause the IP is not matching the SAS requirements
- for second case, since it is using "net use" where it uses SMB. The SMB (Server Message Broker) protocol does not support SAS. it still asks for username/password. Accordingly, it will give error wrong username/pass and will not provide access.
upvoted 290 times

  **regex33** 4 months, 3 weeks ago



the answer is:
Correct Answer:



Box 1: will have no access
The IP 193.77.134.1 does not have access on the SAS, because it is not matching the SAS requirements. IP is out of range.



Box 2: will have no access
Refer to this resource for better understanding.
<https://learn.microsoft.com/en-us/answers/questions/40741/sas-key-for-unc-path>
upvoted 2 times



  **KiwE** 1 year, 9 months ago



It's amazing that wrong answers can be on the site for 2.5 years when this is a paid service.
upvoted 32 times



  **ProfessorJayy** 1 year ago
keeps them from getting shutdown.
upvoted 5 times



  **Exilic** 1 year, 9 months ago
Boggles the mind.
upvoted 5 times



  **researched_answer_boi** 3 years, 11 months ago
Authenticating against an Azure File Share using SAS is currently not supported. Only the Storage Account Keys would work.
<https://docs.microsoft.com/en-us/answers/questions/40741/sas-key-for-unc-path.html>
upvoted 6 times

  **sshiv** 4 years, 4 months ago
could provide refer doc links what you are saying
upvoted 1 times

  **berkejf** 4 years, 4 months ago
fedztedz is correct. both are no access.
upvoted 2 times

  **berkejf** 4 years, 4 months ago
prove: <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-faq#:~:text=Shared%20access%20signature%20keys%20are%20supported%20only%20via%20the%20REST%20API%20or%20in%20client%20libraries.%20You%20must%20mount%20the%20Azure%20file%20share%20over%20SMB%20by%20using%20the%20storage%20account%20keys>
upvoted 3 times

  **Allahham** 4 years, 3 months ago
so the answer will be prompted for credentials or have no access?
upvoted 2 times

  **Beitran** 4 years, 3 months ago
"System error 86 has occurred.
The specified network password is not correct."

upvoted 3 times

 **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer:

Box 1: will have no access

The IP 193.77.134.1 does not have access on the SAS, because it is not matching the SAS requirements. IP is out of range.

Box 2: will have no access

The SAS token is not supported in mounting Azure File share currently, it just supports the Azure storage account key.

Since it is using "net use" where it uses SMB, the SMB (Server Message Broker) protocol does not support SAS. it still asks for username/password. Accordingly, it will give error wrong username/pass and will not provide access.

Reference:


<https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1>

<https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows>

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

<https://docs.microsoft.com/en-us/answers/questions/40741/sas-key-for-unc-path.html>

upvoted 250 times

 **dhihi** 1 year, 2 months ago

Shared access signature (SAS) tokens aren't currently supported for mounting Azure file shares.

Proof/Demo: <https://github.com/MicrosoftDocs/azure-docs/blob/main/articles/storage/files/storage-how-to-use-files-windows.md>

upvoted 2 times

 **JPA210** Most Recent 6 months, 2 weeks ago

The response is correct .

no access for the first option

read, write, and list access for the case you use 'net use' command:

you can use a SAS (Shared Access Signature) with the net use command to map an Azure file share as a network drive. Here's how you can do it:

Generate the SAS URL for your Azure file share.

Open Command Prompt with administrative privileges.

Use the net use command with the SAS URL.


Here's an example command:

```
net use Z: https://<storage-account-name>.file.core.windows.net/<file-share-name> /user:Azure\<storage-account-name> "<SAS-token>"
```

Replace <storage-account-name>, <file-share-name>, and <SAS-token> with your actual storage account name, file share name, and SAS token.

This command maps the Azure file share to the Z: drive on your local machine. If the SAS token is valid, you should be able to access the file share as if it were a local drive.

upvoted 2 times

 **JPA210** 6 months, 2 weeks ago

On the other hand I have just found the following in here: <https://learn.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

" Shared access signature (SAS) tokens aren't currently supported for mounting Azure file shares."

upvoted 1 times


 **[Removed]** 8 months ago

WRONG

1. will have no access

2. will have no access

upvoted 2 times

 **MatAlves** 1 year, 2 months ago

Shared access signature (SAS) tokens aren't currently supported for mounting Azure file shares.

<https://learn.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>


upvoted 1 times

 **Amir1909** 1 year, 2 months ago

- will have no access

- will have no access

upvoted 2 times

 **Ishraj** 1 year, 3 months ago

Box1: have no access , due to IP restriction.

Box2: Will be able to access, since storage explorer can access the share using SAS. Now the SAS will need to be modified by appending the share name after the storage account file endpoint "https://<StorageAccount>.file.core.windows.net/<share1>/?<SAS>"

upvoted 2 times

🗨️ 👤 **SgtDumitru** 1 year, 5 months ago

Box 1: Will have no access. The IP 193.77.134.1 is not in IP range of SAS requirements;
Box 2: Will have all rights. Net use now supports SAS token when mounting Azure File share:

CMD:
net use Z: \\mystorageaccount.file.core.windows.net\myshare /u:Azure\mystorageaccount <SAS_Token>
upvoted 6 times

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

In my examp september 2023.
upvoted 3 times

🗨️ 👤 **JWS80** 1 year, 7 months ago

Found the question on another site I am studying, and it has the same answer which I don't think is correct. It takes forever to check some of these questions.
upvoted 4 times

🗨️ 👤 **Teroristo** 1 year, 9 months ago

Box 1: will have no access
The IP 193.77.134.1 does not have access on the SAS, because it is not matching the SAS requirements. IP is out of range.

Box 2: will have no access
The SAS token is not supported in mounting Azure File share currently, it just supports the Azure storage account key.
Since it is using "net use" where it uses SMB, the SMB (Server Message Broker) protocol does not support SAS. it still asks for username/password.
Accordingly, it will give error wrong username/pass and will not provide access.

Reference:
<https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1>
<https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows>
<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>
<https://docs.microsoft.com/en-us/answers/questions/40741/sas-key-for-unc-path.html>
upvoted 5 times

🗨️ 👤 **LGWJ12** 1 year, 9 months ago

I agree, very good explanation.
upvoted 2 times

🗨️ 👤 **Qjb8m9h** 1 year, 10 months ago

I had this in my exam today - Passed 800
upvoted 3 times

🗨️ 👤 **Sizzle** 1 year, 10 months ago

How are most these answers wrong? What a trash exam collection
upvoted 6 times

🗨️ 👤 **xRiot007** 1 year, 11 months ago

Some of these questions are just trash, I swear, like they WANT you to FAIL.
upvoted 6 times

🗨️ 👤 **JunetGoyal** 2 years ago

Exact same Q came in my exam on 30 April2023.
upvoted 5 times

🗨️ 👤 **jassa012** 2 years ago

Answer is
A: No Access
B: No Access
SAS can't be used as a password. It has to be passed as a Key
<https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview#how-a-shared-access-signature-works>
upvoted 2 times

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

The Answer is incorrect.
It should be no access for both cases.
upvoted 3 times


You have two Azure virtual machines named VM1 and VM2. You have two Recovery Services vaults named RSV1 and RSV2. VM2 is backed up to RSV1. You need to back up VM2 to RSV2. What should you do first?


- A. From the RSV1 blade, click Backup items and stop the VM2 backup
- B. From the RSV2 blade, click Backup. From the Backup blade, select the backup for the virtual machine, and then click Backup
- C. From the VM2 blade, click Disaster recovery, click Replication settings, and then select RSV2 as the Recovery Services vault
- D. From the RSV1 blade, click Backup Jobs and export the VM2 job

Correct Answer: A

Community vote distribution

A (97%)

-  **NikserPro**


Highly Voted 


 2 years, 11 months ago

This is wrong answer, first step should be stopping the backup

If you want to change the recovery service vault you need to disassociate the previous RSV and delete the backup data. To delete backup data, you need to stop the backup first.
So:

 1. Stop the backup in RSV1 (D)
 2. Remove the backup data.
 3. Disassociate the VM in RSV1.
 4. Associate the VM in RSV2.

upvoted 112 times
-  **Erazed**

Highly Voted 


 2 years, 11 months ago


Selected Answer: A

The correct answer is:
A. From the RSV1 blade, click Backup items and stop the VM2 backup

upvoted 47 times
-  **DeinosK** 2 years, 8 months ago


Agree, when you try to add a VM in RSV you are warned that the VM shown are only those "[Discovering] virtual machines that can be backed up, are in the same region as vault and not protected by another vault."

upvoted 2 times
-  **Bravo_Dravel**

Most Recent 

 3 months, 1 week ago



Answer A:
Once the backup is stopped, you can then configure the backup for VM2 in RSV2.

upvoted 1 times
-  **[Removed]** 8 months ago

Selected Answer: A

it's A


the first backup must be stopped, then deleted

upvoted 1 times
-  **Limobakry** 11 months, 3 weeks ago

From the RSV1 blade, click Backup items and stop the VM2 backup.

Explanation:

By stopping the backup of VM2 to RSV1, you ensure that the resources are freed up in RSV1 and can be allocated to RSV2. Once the backup in RSV1 is stopped, you can then initiate the backup process for VM2 to RSV2. After stopping the backup in RSV1, you would then perform the necessary backup configuration in RSV2 using the Azure portal or Azure Backup PowerShell cmdlets.

upvoted 2 times
-  **tashakori** 1 year, 1 month ago

A is right

upvoted 1 times
-  **WeepingMaplte** 1 year, 5 months ago

Ans: A
Ref: https://youtu.be/u1Y4EptZqgc?si=taoA0NEL_WakXSbQ
upvoted 2 times

🗳️ 👤 **Richardfu007** 1 year, 5 months ago

If you want to move an Azure virtual machine that has backup enabled, then you have two choices. They depend on your business requirements:

Don't need to preserve previous backed-up data
Must preserve previous backed-up data

<https://learn.microsoft.com/en-us/azure/backup/backup-azure-move-recovery-services-vault#move-an-azure-virtual-machine-to-a-different-recovery-service-vault>
upvoted 2 times

🗳️ 👤 **iamchoy** 1 year, 7 months ago

Selected Answer: A

The first step to back up VM2 to RSV2 is to stop the backup of VM2 in RSV1. So, the correct answer is:

A. From the RSV1 blade, click Backup items and stop the VM2 backup³

Source:

- (1) How to move my VMs from an existing RSVault to a new RSVault without <https://learn.microsoft.com/en-us/answers/questions/75965/how-to-move-my-vms-from-an-existing-rsvault-to-a-n>.
- (2) Back up Azure VMs in a Recovery Services vault - Azure Backup. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-vms-prepare>.
- (3) Backup VM to a recovery service vault in a different subscription. <https://learn.microsoft.com/en-us/answers/questions/94866/backup-vm-to-a-recovery-service-vault-in-a-differe>.
- (4) undefined. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq>.
- (5) undefined. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms>.

upvoted 2 times

🗳️ 👤 **oopspruu** 1 year, 8 months ago

Jesus christ, this site has a lot of wrong answers. Its just ridiculous at this point. But then again, without these questions, a lot of us will probably fail the exam anyways lol.

upvoted 13 times

🗳️ 👤 **GoldenDisciple2** 1 year, 8 months ago

My thoughts exactly. What's holding this site up is the dialogue in the discussions.

upvoted 8 times

🗳️ 👤 **maxsteele** 1 year, 7 months ago

I cant believe yall dont realize its on purpose lol. Just think about why theyd do it this way.

upvoted 4 times

🗳️ 👤 **basanta123** 1 year, 8 months ago

Selected Answer: A

When you back up a virtual machine to a Recovery Services vault, the backup is stored in that vault. You cannot have the same virtual machine backed up to two different vaults. In order to back up VM2 to RSV2, you first need to stop the backup of VM2 from RSV1. Once the backup is stopped, you can then create a new backup job for VM2 in RSV2.

Here are the steps on how to back up VM2 to RSV2:

- ① In the Azure portal, go to the Recovery Services vaults blade.
- ② Select the RSV1 vault.
- ③ On the Backup items blade, select the VM2 backup.
- ④ Click Stop.
- ⑤ Once the VM2 backup is stopped, go to the RSV2 vault.
- ⑥ On the Backup blade, click + Backup job.
- ⑦ In the Backup job blade, select the VM2 virtual machine.
- ⑧ Click Create.
- ⑨ The VM2 backup job will be created and started in RSV2.

upvoted 10 times

🗳️ 👤 **tfdestroy** 1 year, 4 months ago

Thank you so much for clarification, made sense after reading your comment!

upvoted 1 times

🗳️ 👤 **extopacct** 1 year, 8 months ago

You can only select VMs in the same region as the vault.

VMs can only be backed up in a single vault.

The correct answer is:

A. From the RSV1 blade, click Backup items and stop the VM2 backup

upvoted 1 times

🗳️ 👤 **Teroristo** 1 year, 9 months ago

Answer is From the RSV1 blade, click Backup items and stop the VM2 backup

VMs can only be backed up in a single Recovery Services Vault. You have to stop the VM2 backup from the RSV1 first. Otherwise you won't be able to find the VM2 in RSV2.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-move-recovery-services-vault#must-preserve-previous-backed-up-data>

<https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-first-look-arm>

upvoted 2 times

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

Selected Answer: A

tested in LAB (2023-05-31)

You can't associate secured VMs to other Recovery Vaults.

Option C is possible (this Option exist), but not available. Only after you disassociate the VM for the other Vault.

So the correct Answer is "A"

upvoted 5 times

🗨️ 👤 **Mandar15** 1 year, 11 months ago

Answer A

upvoted 2 times

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

Answer is From the RSV1 blade, click Backup items and stop the VM2 backup

VMs can only be backed up in a single Recovery Services Vault. You have to stop the VM2 backup from the RSV1 first. Otherwise you won't able find the VM2 in RSV2.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-move-recovery-services-vault#must-preserve-previous-backed-up-data>

<https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-first-look-arm>

upvoted 2 times

🗨️ 👤 **zva16** 2 years, 1 month ago

B is correct

upvoted 2 times

🗨️ 👤 **KrisJin** 2 years ago

Give a reason instead just say x is correct. It is non sense.

upvoted 4 times

You have a general-purpose v1 Azure Storage account named storage1 that uses locally-redundant storage (LRS).

You need to ensure that the data in the storage account is protected if a zone fails. The solution must minimize costs and administrative effort.

What should you do first?

- A. Create a new storage account.
- B. Configure object replication rules.
- C. Upgrade the account to general-purpose v2.
- D. Modify the Replication setting of storage1.

Correct Answer: C

Community vote distribution

C (97%)

🗳️ 👤 **klamar** Highly Voted 3 years, 11 months ago
Correct.

v1 supports GRS/RA-GRS but question was about least cost. Least cost is ZRS which is only supported for v2 and premium file/block storage.
Source: <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-storage-account-types>
upvoted 89 times

🗳️ 👤 **renzoku** 2 years, 8 months ago
But it's wondering about Zone fails then ZRS wouldn't an option else we should use GRS
upvoted 4 times

🗳️ 👤 **photon99** 1 year, 6 months ago
Actually the question says, A ZONE. That mean its not ALL OR SOME ZONE fail. So yeah, ZRS is suitable over GRS.
upvoted 1 times

🗳️ 👤 **mung** 2 years, 5 months ago
ZRS replicates data into multiple "Zones". So if your primary zone fails then the other two or more zones are available and will takeover the failed zone for you and your server will stay alive. So ZRS is great for zone failure.

GRS replicated your data into different geography.
For example, if you are in USA you will most likley be using NA geography.
And if you use GRS, your data will be replicated to a secondary gregraphy such as EU, Asia, etc.

So with GRS, even if the entire NA Azure servers failes and lose all your data, you will still have backed up data in a different geography.
upvoted 10 times

🗳️ 👤 **photon99** 1 year, 6 months ago
Microsoft MUST remove all the questions for the services they have planned deprecation. It make no sense to confuse new people between Storage V1 vs V2 or confuse us between Basic PublicIP vs Standard PublicIP.
upvoted 9 times

🗳️ 👤 **Mentalfloss** 9 months ago
I am guessing Microsoft did remove this question from the exam, but it lingers here for all eternity. :)
upvoted 2 times

🗳️ 👤 **Itson1** 2 years, 2 months ago
The answer is upgrading to gen 2 but say nothing about changing LRS to ZRS so I think D should be the answer
upvoted 3 times

🗳️ 👤 **vldt** 2 years, 1 month ago
again MS is playing with the words here. Note that the question is:
"What should you do FIRST?" so the answer is correct
upvoted 5 times

🗳️ 👤 **mwhoow** Highly Voted 3 years, 8 months ago
Answer is correct, and this is why :

General-purpose v2 storage accounts support the latest Azure Storage features and incorporate all of the functionality of general-purpose v1 and Blob storage accounts. General-purpose v2 accounts are recommended for most storage scenarios. General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices. General-purpose v2 accounts support default account access tiers of hot or cool and blob level tiering between hot, cool, or archive.

Upgrading to a general-purpose v2 storage account from your general-purpose v1 or Blob storage accounts is straightforward. You can upgrade

using the Azure portal, PowerShell, or Azure CLI. There is no downtime or risk of data loss associated with upgrading to a general-purpose v2 storage account. The account upgrade happens via a simple Azure Resource Manager operation that changes the account type.

Hope this helps
upvoted 44 times

  **Mozbius_** 3 years, 3 months ago

Nice pointing out. Also just to avoid any confusion the same doesn't apply to switching from Standard V2 to any of the Premium tiers. Doing such a switch requires a NEW storage account to be created and data to be copied over after.

Reference : Microsoft own AZ104 certified instructor.
upvoted 6 times

  **[Removed]** Most Recent 8 months ago

Selected Answer: C



C is corect
upvoted 1 times

  **01525bd** 1 year, 1 month ago

Standard general-purpose v1 = LRS/GRS/RA-GRS
Blob Storage = LRS/GRS/RA-GRS
Standard general-purpose v2 = LRS/ZRS/GRS/RA-GRS/GZRS/RA-GZRS
Premium block blobs = LRS/ZRS
Premium page blobs = LRS/ZRS
Premium file shares = LRS/ZRS
<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview>
upvoted 2 times

  **Amir1909** 1 year, 2 months ago

C is correct
upvoted 1 times

  **VikiAP** 1 year, 2 months ago

Still don't agree with the answer. Upgrading to Storagev2 does not automatically sets Zone Redundancy ... so this answer is not correct to me ..
upvoted 1 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: C

To protect data against a zone failure, you would typically use Zone-Redundant Storage (ZRS). However, General-Purpose v1 (GPv1) storage accounts do not support ZRS.

To take advantage of ZRS, you should use General-Purpose v2 (GPv2) storage accounts. After upgrading to GPv2, you can then modify the replication settings to use ZRS.

So, the correct first step would be:

C. Upgrade the account to general-purpose v2.

Once you've upgraded to GPv2, you can modify the Replication setting to use ZRS.
upvoted 5 times

  **Mehedi007** 1 year, 9 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-storage-account-types>
<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-upgrade?tabs=azure-portal>

Passed the exam on 26 July 2023. Scored 870. Exact question came.
upvoted 3 times

  **vanr2000** 2 years, 1 month ago

Selected Answer: C

You need to upgrade the storage account to General-purpose v2, which support ZRS replication support.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-storage-account-types>

The following link shows, how you can upgrade the storage account to version 2
<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-upgrade?tabs=azure-portal>
upvoted 3 times

  **UmbongoDrink** 2 years, 2 months ago



Selected Answer: C



It's C.
upvoted 2 times



  **abiurrunc** 2 years, 3 months ago

Selected Answer: C



General Purpose v2 offers all data services with all options for replication and access tiers where available.
upvoted 2 times



  **Davindra** 2 years, 5 months ago
It was in exam on 11/23
upvoted 4 times



  **lisley** 2 years, 5 months ago
Selected Answer: C
C makes sense
upvoted 1 times

  **NaoVaz** 2 years, 7 months ago
Selected Answer: C
C) "Upgrade the account to general-purpose v2"

The least cost type of storage account that supports zone failures is ZRS, that only supports general-purpose v2.
upvoted 5 times

  **EmnCours** 2 years, 7 months ago
Selected Answer: C
v1 supports GRS/RA-GRS but question was about least cost. Least cost is ZRS which is only supported for v2 and premium file/block storage.
Source: <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-storage-account-types>
upvoted 1 times

  **EmnCours** 2 years, 7 months ago
Selected Answer: A
v1 supports GRS/RA-GRS but question was about least cost. Least cost is ZRS which is only supported for v2 and premium file/block storage.
Source: <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-storage-account-types>
upvoted 1 times

  **Lazylinux** 2 years, 10 months ago
Selected Answer: C
C is correct
upvoted 3 times

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Type	Performance
storage1	StorageV2	Standard
storage2	BlobStorage	Standard
storage3	BlockBlobStorage	Premium
storage4	FileStorage	Premium

You plan to manage the data stored in the accounts by using lifecycle management rules.

To which storage accounts can you apply lifecycle management rules?

- A. storage1 only
- B. storage1 and storage2 only
- C. storage3 and storage4 only
- D. storage1, storage2, and storage3 only
- E. storage1, storage2, storage3, and storage4

Correct Answer: D

Community vote distribution

D (96%)

4%

- Tamilarasan**

Highly Voted

3 years, 11 months ago

Answer is correct .
The lifecycle management feature is available in all Azure regions for general purpose v2 (GPv2) accounts, blob storage accounts, premium block blobs storage accounts, and Azure Data Lake Storage Gen2 accounts.
upvoted 102 times
- ThatDowntownSmell**

2 years, 10 months ago

A bad question; storage account type and kind are mixed here. Also at this point, this is all legacy. Storage account types offered now without switching to legacy are simply standard (gpv2) and premium. Even in legacy, there isn't any such storage account type as "filestorage", so storage4 as listed is not valid, period.
upvoted 12 times
- ggogel**

1 year, 4 months ago

Yes, they mixed up type and kind here, but there indeed is a kind called FileStorage, which refers to "Premium file shares" and they are not legacy.
upvoted 3 times
- MitchellLauwers1993**

3 years, 5 months ago

<https://docs.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>
upvoted 5 times
- InvisibleShadow**

Highly Voted

3 years, 1 month ago

This question came in the exam today 8/Mar/2022.
I passed the exam, 95% questions came from here.
upvoted 41 times
- Vinod_Varma**

2 years, 8 months ago

Have you purchase Contributor Access ?
upvoted 9 times
- darkskullSB**

2 years, 5 months ago

Did you?
upvoted 3 times
- AK4U_111**

2 years, 2 months ago

I did. Test next week
upvoted 2 times
- AK4U_111**

2 years, 2 months ago

I did. Test next week
upvoted 2 times

  **cankayahmet** 2 years, 1 month ago

Lots of new questions from Contributor Access and also case study questions are there
upvoted 4 times

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

Selected Answer: D

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.
upvoted 1 times

  **Bravo_Dravel** 3 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview?tabs=azure-portal>
upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: D

D is corerct
upvoted 1 times

  **Amir1909** 1 year, 2 months ago

D is correct
upvoted 2 times

  **gargaditya** 1 year, 4 months ago

Though "Blob Storage" is legacy and Q should not have included this,
answer is Storage1 and Storage2 only(B).

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>
-Known issues and limitations

Tiering is not yet supported in a premium block blob storage account. For all other accounts, tiering is allowed only on block blobs and not for append and page blobs.

-Note

Tiering is not yet supported in a premium block blob storage account. For all other accounts, tiering is allowed only on block blobs and not for append and page blobs.

<https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview>
- Note

Setting the access tier is only allowed on Block Blobs. They are not supported for Append and Page Blobs.

-Note

Data stored in a premium block blob storage account cannot be tiered to hot, cool, cold or archive by using Set Blob Tier or using Azure Blob Storage lifecycle management.

upvoted 1 times

  **gargaditya** 1 year, 4 months ago


The only contradictory line in first link is this, which should be ignored given the other write ups:
Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts. Lifecycle management doesn't affect system containers such as the \$logs or \$web containers
upvoted 1 times

  **gargaditya** 1 year, 4 months ago

My diagram summarizing the above: <https://learn-attachment.microsoft.com/api/attachments/6bcd9af2-6176-40e3-bb2f-232018a418a7?platform=QnA>
upvoted 1 times

  **gargaditya** 1 year, 4 months ago

□ Azure storage offers different access tiers, allowing you to store blob object data in the most cost-effective manner.
□ Tiers are a way to organize your data based on how frequently it will be accessed and how long it will be retained, with the end goal of optimising cost.
NOTES:
-Hot/Cool/Archive tiering applies to 'blobs,' not files/queues/tables (other performance options exist for these)
-Further, Setting the access tier is only allowed on Block Blobs. They are not supported for Append and Page Blobs.
-Blobs in GPV2 storage account can be set to Hot/Cool/Archive.
Premium Block Blob storage account - Data stored in a premium block blob storage account cannot be tiered to hot, cool, or archive using Set Blob Tier or using Azure Blob Storage lifecycle management.
upvoted 2 times

  **fe0b3b4** 1 year, 3 months ago

As I understand it, lifecycle management can be used for automatically changing the tier, but also for automatically deleting the data. Therefore a lifecycle management policy on a premium block blob is supported and can be used for deleting data, just not for changing the data tier.
upvoted 2 times

  **MCI** 1 year, 3 months ago

"Getting the access tier is only allowed on Block Blobs. They are not supported for Append and Page Blobs". Just found this on your 2nd link.

upvoted 1 times

🗲️ 👤 **Kalzonee3611** 1 year, 6 months ago

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts. Lifecycle management doesn't affect system containers such as the \$logs or \$web container

upvoted 2 times

🗲️ 👤 **GoldenDisciple2** 1 year, 8 months ago

Exam be like: Memorize every little thing you need to know in order to be an Azure Admin

Real life be like: Works a job where you wait for something to go wrong. When something goes wrong, you go to Google and Microsoft documentation on what could truly be the problem because you ain't gonna remember any of this... even if you did, probably won't help you irl.

upvoted 31 times

🗲️ 👤 **Mehedi007** 1 year, 9 months ago

Selected Answer: D

"Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts."

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 10 months ago

Answer is correct:

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.

upvoted 2 times

🗲️ 👤 **KrisJin** 2 years ago

To be a cloud admin/architect, I do not need to know how to google, but I need to memorize which storage type supports lifecycle management.

upvoted 13 times

🗲️ 👤 **Roy010** 1 year, 10 months ago

Honestly this whole exam should allow you to Google things, or they should make it shorter and remove such nonsense questions.

upvoted 7 times

🗲️ 👤 **shadad** 2 years, 2 months ago

Selected Answer: D

I took Exam of Azure- 104 at 27/2/2023

I score 920 points out of 1000 points. This was on it and my answer was: D

upvoted 9 times

🗲️ 👤 **et20230303** 2 years, 1 month ago

how long did it take you to finish the exam?

upvoted 3 times

🗲️ 👤 **zelck** 2 years, 3 months ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.

upvoted 3 times

🗲️ 👤 **Ashfaque_9x** 2 years, 3 months ago

Selected Answer: D

Passed today on 29Jan23 with a score of 970. This question was in the exam.

D. storage1, storage2, and storage3 only

upvoted 5 times

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

Does anyone know the rational behind not including file storage?

upvoted 3 times

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

Aside from it not being listed. Like why did MS choose File storage to no receive this feature.

upvoted 4 times



🗲️ 👤 **prem007** 2 years, 4 months ago

Selected Answer: D

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.

link: <https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>

upvoted 3 times

  **rmsdg** 2 years, 5 months ago

correct -
Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.

upvoted 1 times

You create an Azure Storage account named contosostorage.

You plan to create a file share named data.

Users need to map a drive to the data file share from home computers that run Windows 10.

Which outbound port should you open between the home computers and the data file share?

- A. 80
- B. 443
- C. 445
- D. 3389

Correct Answer: C

Community vote distribution

C (100%)

  **sk1803** Highly Voted 3 years, 7 months ago

Correct answer is port 445, as this is port for SMB protocol to share files

Incorrect:

Port 80: HTTP, this is for web

Port 443: HTTPS, for web too

Port 3389: Remote desktop protocol (RDP)

upvoted 72 times

  **ohana** Highly Voted 3 years, 6 months ago

Took the exam today on 17 Oct. Similar question came out. Know the usage for all your ports! Ans:445

upvoted 25 times

  **SK_2_SK** 3 years, 5 months ago

Thanks for the info!

upvoted 2 times

  **knarik** Most Recent 1 month ago

Selected Answer: C

on exam 1/4/2025


upvoted 1 times

  **[Removed]** 8 months ago

Selected Answer: C

C is corerct

upvoted 1 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: C

To map a drive to the Azure file share from home computers that run Windows 10, you need to open outbound port 445.

So the correct answer is:

C. 445

This port is used for SMB (Server Message Block) protocol, which is what Windows uses for file sharing. Note that some ISPs block this port, so if you experience issues, a VPN or Azure ExpressRoute connection may be necessary to allow the traffic. Always ensure you are following security best practices when opening ports, especially when dealing with potentially sensitive data.

upvoted 4 times

  **Mehedi007** 1 year, 9 months ago



Selected Answer: C

445.

<https://learn.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows#prerequisites>



Passed the exam on 26 July 2023. Scored 870. Exact question came.



upvoted 4 times



  **itguyeu** 1 year, 10 months ago



I used free version access for this site and it helped me pass the exam. Some questions that I had on the exams, I took the exam more than once, are not available under the free tier access, but 80% of the questions came from here. I do recommend investing a bit of money and getting full access to this site. I didn't memorise answers but analysed them and studied as Microsoft does tweak them a bit.

This Q was on the exam.
upvoted 1 times

  **zzreflexzz** 2 years ago
on exam 4/29/23
upvoted 3 times



  **Aluksy** 2 years ago
Correct answer port 445, came out in my exam today 8th April 2023.
upvoted 2 times



  **NJTH** 2 years ago
Simular question was on todays exam.
(7th April 2023)
upvoted 2 times



  **Ligteagle** 2 years, 1 month ago

Selected Answer: C

445 smb port
upvoted 1 times



  **Gaskonader** 2 years, 1 month ago
On Exam 30/03/2023
upvoted 3 times



  **AzZnLuVaBol** 2 years, 1 month ago
On the Exam 3/29/23.
upvoted 3 times



  **shadad** 2 years, 2 months ago
I took Exam of Azure- 104 at 27/2/2023
I score 920 points out of 1000 points. This was on it and my answer was: C

think about it like this:
Port 80: HTTP/ web
Port 443: HTTPS/web
Port 3389: Remote desktop protocol (RDP)

then that leave you with what? :) 445 which is for SMB/ share files
upvoted 4 times



  **SimonSM178** 2 years, 1 month ago
in your opinion how many questions were taken from this dump?
upvoted 1 times

  **bloodtech** 2 years, 2 months ago
On exam 24/02/2023
upvoted 2 times

  **UmbongoDrink** 2 years, 2 months ago

Selected Answer: C

Port 445
upvoted 1 times

  **UmbongoDrink** 2 years, 2 months ago
Port 445.
upvoted 1 times

You have an Azure subscription named Subscription1.
You have 5 TB of data that you need to transfer to Subscription1.
You plan to use an Azure Import/Export job.
What can you use as the destination of the imported data?

- A. Azure File Storage
- B. an Azure Cosmos DB database
- C. Azure Data Factory
- D. Azure SQL Database

Correct Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **JESUSBB** Highly Voted 👍 3 years, 4 months ago
In exam today 11-DEC-2021 ans: A
upvoted 25 times

🗲️ 👤 **Lu5ck** Highly Voted 👍 2 years, 7 months ago
same as Q22 & Q28 (BLOB & FILE STORAGE)
upvoted 7 times

🗲️ 👤 **[Removed]** Most Recent 🕒 8 months ago
Selected Answer: A
A is corerct
upvoted 1 times

🗲️ 👤 **Mehedi007** 1 year, 9 months ago
Selected Answer: A
Azure File Storage
<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>
upvoted 1 times

🗲️ 👤 **karrey** 2 years, 1 month ago
Selected Answer: A
A is the correct answer
upvoted 3 times

🗲️ 👤 **UmbongoDrink** 2 years, 2 months ago
Selected Answer: A
It's A
upvoted 1 times

🗲️ 👤 **zelck** 2 years, 3 months ago
Same as question 54.
<https://www.examttopics.com/discussions/microsoft/view/93820-exam-az-104-topic-3-question-54-discussion>
upvoted 1 times

🗲️ 👤 **zelck** 2 years, 3 months ago
Selected Answer: A
A is the answer.

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service>
Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.
upvoted 1 times

🗲️ 👤 **JN62** 2 years, 7 months ago
Selected Answer: A
yes, correct answer is A
upvoted 2 times

🗄️ 👤 **NaoVaz** 2 years, 7 months ago

Selected Answer: A

A) "Azure File Storage"

<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>
upvoted 2 times

🗄️ 👤 **epomatti** 3 years ago

Selected Answer: A

Correct, only Blob and Files are supported.
upvoted 2 times

🗄️ 👤 **ajayasa** 3 years, 1 month ago

this question was there on 16/03/2022 with same question and passed with 900 percent
upvoted 4 times

🗄️ 👤 **gharbi** 3 years, 2 months ago

same as #26
upvoted 1 times

🗄️ 👤 **WS_21** 3 years, 2 months ago

Selected Answer: A

<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service>
upvoted 1 times

🗄️ 👤 **pappkarcsiii** 3 years, 3 months ago

Selected Answer: A

Azure File Storage - <https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service>
upvoted 1 times

🗄️ 👤 **drainuzzo** 3 years, 4 months ago

correct: A
upvoted 1 times

🗄️ 👤 **MrMacro** 3 years, 4 months ago

Azure File Storage is the correct answer. Ref here: <https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service>

"The WAImportExport tool is available in two versions, version 1 and 2. We recommend that you use:

Version 1 for import/export into Azure Blob storage.

Version 2 for importing data into Azure files."

upvoted 1 times

HOTSPOT -

You have an Azure subscription that contains an Azure Storage account named storageaccount1.

You export storageaccount1 as an Azure Resource Manager template. The template contains the following sections.

```
{
  "type": "Microsoft.Storage/storageAccount",
  "apiVersion": "2019-06-01",
  "name": "storageaccount1",
  "location": "eastus",
  "sku": {
    "name": "Standard_LRS",
    "tier": "Standard"
  },
  "kind": "StorageV2",
  "properties": {
    "networkAcls": {
      "bypass": "AzureServices",
      "virtualNetworkRules": [],
      "ipRules": [],
      "defaultAction": "Allow",
    },
    "supportsHttpsTrafficOnly": true,
    "encryption": {
      "services": {
        "file": {
          "keyType": "Account",
          "enabled": true
        },
        "blob": {
          "keyType": "Account",
          "enabled": true
        }
      }
    },
    "keySource": "Microsoft.Storage"
  },
  "accessTier": "Hot"
}
```

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

NOTE: Each correct selection is worth one point

Hot Area:

Answer Area



Statements	Yes	No
A server that has a public IP address of 131.107.103.10 can access storageaccount1	<input type="radio"/>	<input type="radio"/>
Individual blobs in storageaccount1 can be set to use the archive tier	<input type="radio"/>	<input type="radio"/>
Global administrations in Azure Active Directory (Azure AD) can access a file share hosted in storageaccount1 by using their Azure AD credentials	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area



Statements	Yes	No
A server that has a public IP address of 131.107.103.10 can access storageaccount1	<input checked="" type="radio"/>	<input type="radio"/>
Individual blobs in storageaccount1 can be set to use the archive tier	<input checked="" type="radio"/>	<input type="radio"/>
Global administrations in Azure Active Directory (Azure AD) can access a file share hosted in storageaccount1 by using their Azure AD credentials	<input type="radio"/>	<input checked="" type="radio"/>

Reference:
<https://docs.microsoft.com/en-us/azure/templates/microsoft.storage/storageaccounts?tabs=json>

  **MrMacro** Highly Voted 3 years, 4 months ago
Box 1- Yes. VirtualNetworkRules & IpRules are blank, with the default action Allow.
Box 2- Yes. Individual blobs can be set to the archive tier - ref.<https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview>
Bob 3. No. To access blob data in the Azure portal with Azure AD credentials, a user must have the following role assignments:

A data access role, such as Storage Blob Data Contributor
The Azure Resource Manager Reader role



Ref.<https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access?tabs=portal>
upvoted 127 times

  **Mozbius_** 3 years, 3 months ago
Box 2 is VERY TRICKY- Answer appears to be NO



The ARM Template storage is of type StorageV2. It is true that BLOB LifeCycles exist for "StorageV2 (which supports blobs), Premium Page Blob, Premium Block Blob". That being said the link you provided is only subtly inferring that the "ARCHIVE" tiers can be enabled only at hardcore Blobs storages NOT "StorageV2".



"While the Hot and Cool tiers can be enabled at the storage account level or at the blob level, the Archive tier can only be enabled at the blob level. All three storage access tiers can exist in the same storage account and the default tier for a blob is inherited from the account level setting."



Reference:
<https://cloud.netapp.com/blog/storage-tiers-in-azure-blob-storage-find-the-best-for-your-data#:~:text=%20How%20to%20Switch%20Between%20Storage%20Tiers%20in,account%2C%20browse%20to%20the%20Storage%20account-%3EBlob...%20More%20>
upvoted 8 times

  **Mozbius_** 3 years, 3 months ago
I take it back!!! In Azure I have created a Standard V2 based storage account and when I go to upload a Blob in a container "Hot", "Cool" and "Archive" are access tiers can be selected.

So based on that test it appears that it is not possible to change the a Standard V2 based "storage account" tier to "Archive" (because life cycles apply only to Blobs and not to Files, Tables or Queues) but it is possible to indeed set the access tier to individual blobs within a StandardV2 storage account (which I must say makes a lot of sense).
upvoted 44 times

  **Mozbius_** 3 years, 3 months ago
Box 2 is YES (moderator please delete my initial response to prevent further confusion. Thanks).
upvoted 69 times

  **KingHalik** 1 year, 5 months ago
I agree:
"Only storage accounts that are configured for LRS, GRS, or RA-GRS support moving blobs to the archive tier. The archive tier isn't supported for ZRS, GZRS, or RA-GZRS accounts. For more information about redundancy configurations for Azure Storage, see Azure Storage redundancy."
<https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview>
upvoted 3 times

  **beem84** Highly Voted 3 years, 4 months ago
1: Yes. Defaultaction is allow. IP is allowed.
2: Yes. Storagev2 allows tiering.
3: No. File share access requires SAS.
upvoted 76 times

- lahirudk

Most Recent

7 months ago

Active question as of today
upvoted 4 times
- [Removed]

8 months ago

CORRECT

Yes (defaultAction is allowed)
Yes (Storagev2 supports tiering)
No (File share access requires SAS ehich is not mentioned)
upvoted 3 times
- ajay01avhad

9 months, 1 week ago

Analysis: The IP 193.77.134.1 is not within the allowed IP address range specified (which is from 193.77.134.10 to 193.77.134.50). Therefore, any attempt to connect from this IP will be denied.
Answer:
Will have no access
Analysis: The IP 193.77.134.50 falls within the allowed IP range. Permissions granted include Read, Write, Delete, and List. Given that the scenario occurs within the allowed date range and uses a permitted IP, the access will be granted according to the specified permissions.
Answer:
Will have read, write, and list access
upvoted 1 times
- varinder82

11 months, 2 weeks ago

1: Yes. Defaultaction is allow. IP is allowed.
2: Yes. Storagev2 allows tiering.
3: No. File share access requires SAS.
upvoted 2 times
- tashakori

1 year, 1 month ago

Given answer is right
upvoted 1 times
- 1828b9d

1 year, 2 months ago

This question was in exam 01/03/2024
upvoted 4 times
- sjsaran

1 year, 7 months ago

Only Azure Services option is enabled, it can be enabled only in the selected network option (option 2 in the network blade), and if there is no IP added that mean no access from any public network, so the answer to the question 1 might be NO
upvoted 1 times
- redD

1 year, 8 months ago

Box 1 - No, because the optional parameter "publicNetworkAccess" NOT specified! Ref Allow or disallow public network access to STORAGE ACCOUNT. Value is optional but if passed in, must be 'Enabled' or 'Disabled' <https://learn.microsoft.com/en-us/azure/templates/microsoft.storage/storageaccounts?pivots=deployment-language-arm-template#property-values-1>
upvoted 1 times
- eduardokm

1 year, 9 months ago

Box 2 - Yes - <https://learn.microsoft.com/en-us/rest/api/storageservices/set-blob-tier?tabs=azure-ad>
upvoted 1 times
- danrodcad

1 year, 9 months ago

Box1- Yes -DefailtAction = "Allow"
Box2-No - if the storage account's access tier is set to "Hot," you cannot directly set individual blobs within that storage account to the "Archive" access tier.
box3- ?? Keytype ="Account"
upvoted 2 times
- GPerez73

1 year, 8 months ago

Agree with Box1 and Box2 (archive is greyed out). I'm not sure about box3, but file share let you to set up AAD access. So I would say yes YNY for me
upvoted 3 times
- Richard1205

1 year, 10 months ago

Box1: Y NetworkACLs are blank. Default Action Allow
Box2: Y Individual blobs can be set to the archive tier
<https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview?tabs=azure-portal>
Watch : The following table summarizes how tier changes are billed.
Box3: N In the List no allowSharedKeyAccess type ,the allowSharedKeyAccess default is True
Indicates whether the storage account permits requests to be authorized with the account access key via Shared Key. If false, then all requests, including shared access signatures, must be authorized with Azure Active Directory (Azure AD). The default value is null, which is equivalent to true.
upvoted 4 times
- AzZnLuVaBol

2 years, 1 month ago

On the Exam 3/29/23.

upvoted 10 times

  **nidhogg** 2 years, 2 months ago

yyY
learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal


"The classic subscription administrator roles Service Administrator and Co-Administrator include the equivalent of the Azure Resource Manager owner role. The Owner role includes all actions, including the Microsoft.Storage/storageAccounts/listkeys/action, so a user with one of these administrative roles can also access blob data with the account key.

upvoted 1 times

  **nidhogg** 2 years, 2 months ago

Global admin AzAD role is given the service admin role at subcription level, thus it could access anything on a Storage Account.
I guess that it'd be Y - Y - Y
<https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

upvoted 2 times

  **fits08pistils** 1 year, 10 months ago

This is not true, also it's not mentioned anywhere in the URL you provided, so the answer is still YYN
upvoted 2 times

  **samzurcher** 2 years, 6 months ago

Box 1 - probably No. You can not access content of the storage account unless you set Public Access on the Blob-Level i think.
upvoted 1 times

  **OliwerCiecwierz** 2 years, 5 months ago

Don't think
upvoted 4 times

You have an Azure subscription that contains a storage account named storage1.
You have the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Linux
Device3	macOS

From which devices can you use AzCopy to copy data to storage1?

- A. Device 1 only
- B. Device1, Device2 and Device3
- C. Device1 and Device2 only
- D. Device1 and Device3 only

Correct Answer: B

Community vote distribution

B (100%)

- NaoVaz**

Highly Voted

2 years, 7 months ago

Selected Answer: B

B) "Device1, Device2 and Device3"

AzCopy is supported in all these three operating systems: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#download-azcopy>

upvoted 29 times
- nanasonaeh**

Highly Voted

2 years, 8 months ago

Selected Answer: B

Source: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

upvoted 6 times
- fallkore**

Most Recent

3 months, 3 weeks ago

Selected Answer: B

Anytime you see a question that makes Azure look more compatible/cooler/better/etc you know how to answer.

upvoted 2 times
- lahirudk**

7 months ago

As of 1st Oct, 2024 this question is valid, and there's a fourth option as "Android".

upvoted 3 times
- [Removed]**

8 months ago

Selected Answer: B

B is corerct

upvoted 1 times
- tashakori**

1 year, 1 month ago

B is correct

upvoted 1 times
- 1828b9d**

1 year, 2 months ago

This question was in exam 01/03/2024

upvoted 3 times
- Indy429**

1 year, 4 months ago

They can just never create a normal exam without any trick questions can they?

Obviously AzCopy is supported for all OSeS but questions like these always make you second-guess, like "am I missing something?" Ugh.

upvoted 2 times

🗨️ 👤 **BIOKU** 1 year, 6 months ago

Selected Answer: B

AzCopy is a CLI cmdlet and will work on All operating systems
upvoted 2 times

🗨️ 👤 **Mehedi007** 1 year, 9 months ago

Selected Answer: B

Device1, Device2 and Device3
<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#download-azcopy>
upvoted 1 times

🗨️ 👤 **xRiot007** 1 year, 11 months ago

AzCopy works on all three OS, so the answer would be B - Device1, Device2 and Device 3.
upvoted 1 times

🗨️ 👤 **JayLearn2022** 2 years, 2 months ago

B) "Device1, Device2 and Device3"
AzCopy is supported in all three operating systems.

First, download the AzCopy V10 executable file to any directory on your computer. AzCopy V10 is just an executable file, so there's nothing to install.

Windows 64-bit (zip)
Windows 32-bit (zip)
Linux x86-64 (tar)
Linux ARM64 Preview (tar)
macOS (zip)

Note:

If you want to copy data to and from your Azure Table storage service, then install AzCopy version 7.3.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>
upvoted 5 times

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

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#download-azcopy>
upvoted 1 times

🗨️ 👤 **zellck** 2 years, 3 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#download-azcopy>
upvoted 2 times

🗨️ 👤 **F117A_Stealth** 2 years, 8 months ago

Selected Answer: B

Device1, Device2 and Device3
upvoted 2 times

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

Selected Answer: B

Device1, Device2 and Device3
upvoted 2 times

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

Thats correct
<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>
upvoted 2 times

You have an Azure Storage account named storage1 that contains a blob container named container1.
You need to prevent new content added to container1 from being modified for one year.
What should you configure?

- A. the access tier
- B. an access policy
- C. the Access control (IAM) settings
- D. the access level

Correct Answer: B

Community vote distribution

B (100%)

- rrabeya**

Highly Voted

3 years, 5 months ago

Answer B
Time-based retention policies: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten.
upvoted 68 times
- rrabeya**

3 years, 5 months ago

<https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview?tabs=azure-portal>
upvoted 4 times
- duomianhu**

3 years ago

More specific: <https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-time-based-retention-policy-overview>
upvoted 6 times
- Carlosadan10**

2 years, 2 months ago

Thanks
upvoted 1 times
- breakerboyz09**

Highly Voted

3 years, 7 months ago

B is correct.

Because Access policy can set retention policy.
upvoted 30 times
- [Removed]**

Most Recent

8 months ago

Selected Answer: B

B is corerct
upvoted 1 times
- Amir1909**

1 year, 2 months ago

B is correct
upvoted 1 times
- babakeyfgir**

1 year, 3 months ago

It was in EXAM, thanks Examtopic.
upvoted 3 times
- Mehedi007**

1 year, 9 months ago

Selected Answer: B

Access policy
"While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes."
<https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview?tabs=azure-portal>
upvoted 4 times

Richard1205

1 year, 10 months ago

Answer B
A stored access policy provides an additional level of control over service-level shared access signatures (SASs) on the server side. Establishing a stored access policy serves to group shared access signatures and to provide additional restrictions for signatures that are bound by the policy.

You can use a stored access policy to change the start time, expiry time, or permissions for a signature. You can also use a stored access policy to

revoke a signature after it has been issued.

The following storage resources support stored access policies:

Blob containers
File shares
Queues
Tables

upvoted 3 times

  **Mehul078** 1 year, 10 months ago

Answer B



Link: <https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-policy-configure-container-scope?source=recommendations&tabs=azure-portal#configure-a-retention-policy-on-a-container>

upvoted 1 times

  **Gaskonader** 2 years, 1 month ago

On Exam 30/03/2023

upvoted 5 times

  **zelck** 2 years, 3 months ago



Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview>

Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

upvoted 3 times

  **NaoVaz** 2 years, 7 months ago



Selected Answer: B

B) "an access policy"

Using SAS in conjunction with a stored Access Policy the desired outcome can be achieved: "You can use a stored access policy to change the start time, expiry time, or permissions for a signature. You can also use a stored access policy to revoke a signature after it has been issued." -

<https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy>

upvoted 8 times

  **Burnie** 2 years, 7 months ago

Answer B: Tested in LAB

Time-based retention policies: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten.

upvoted 1 times

  **EmnCours** 2 years, 8 months ago

Selected Answer: B

Answer B

Time-based retention policies: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten.

upvoted 1 times

  **epomatti** 3 years ago

Selected Answer: B

Correct B - Need to use Access Policy of the type immutable.



upvoted 1 times

  **Valunchai** 3 years, 1 month ago

Selected Answer: B

Answer : B

upvoted 1 times

  **zr79** 3 years, 2 months ago

A. access tier is for Hot, Cool, and Archive

C. IAM is for RBAC roles



D. Never heard of it

upvoted 7 times

  **epomatti** 3 years ago

D access level controls anonymous access configuration.

upvoted 2 times

  **WS_21** 3 years, 2 months ago

Selected Answer: B

<https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-policy-configure-container-scope?tabs=azure-portal>
upvoted 1 times

HOTSPOT -

You have an Azure Storage account named storage1 that contains a blob container. The blob container has a default access tier of Hot. Storage1 contains a container named conainer1.

You create lifecycle management rules in storage1 as shown in the following table.

Name	Rule scope	Blob type	Blob subtype	Rule block	Prefix match
Rule1	Limit blobs by using filters.	Block blobs	Base blobs	If base blobs were not modified for two days, move to archive storage. If base blobs were not modified for nine days, delete the blob.	container1/Dep1
Rule2	Apply to all blobs in storage1.	Block blobs	Base blobs	If base blobs were not modified for three days, move to cool storage. If base blobs were not modified for nine days, move to archive storage.	Not applicable

You perform the actions shown in the following table.

Date	Action
October 1	Upload three files named Dep1File1.docx, File2.docx, and File3.docx to container 1.
October 2	Edit Dep1File1.docx and File3.docx.
October 5	Edit File2.docx.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On October 10, you can read Dep1File1.docx.	<input type="radio"/>	<input type="radio"/>
On October 10, you can read File2.docx.	<input type="radio"/>	<input type="radio"/>
On October 10, you can read File3.docx.	<input type="radio"/>	<input type="radio"/>

Answer Area	Statements	Yes	No
Correct Answer:	On October 10, you can read Dep1File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
	On October 10, you can read File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>
	On October 10, you can read File3.docx.	<input checked="" type="radio"/>	<input type="radio"/>

 **NZure** Highly Voted 3 years, 7 months ago



I don't think this is correct
Rule1 archives blobs(aka files) after 2 days of inactivity and deletes after 9
Rule2 moves to cool tier after 3 days and archive tier after 9
Of the three files, Rule1 only applies to Dep1File1.docx, while the other files have Rule2 applied.

The question asks if you can read the files on the 10th, not if they still exist. Files in the archive tier CANNOT be read as documented by Microsoft: "While a blob is in archive storage, the blob data is offline and can't be read or modified. To read or download a blob in archive, you must first rehydrate it to an online tier."
<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

Dep1File1.docx was last updated 8 days ago, and would be in archive tier
File2.docx was last updated 5 days ago, and would be in cool tier
File3.docx was last updated 8 days ago and would be in cool tier

Dep1File1 > No cannot be read
File2 > Yes cannot be read
File3 > Yes can be read



upvoted 227 times

  **S3ktar** 3 years, 4 months ago

Correct Answer - No - Yes - Yes
Dep1File1.docx is in archive, meaning the only way to pull it out and read it is to "rehydrate" the file
File2 and File3 can continue to be read, even in the cool tier
upvoted 27 times

  **examprepboy** 7 months, 2 weeks ago

no
yes
yes
you wrote "cannot" im assuming typo
upvoted 3 times

  **jecaine** 3 years, 7 months ago

i'm so sick of this site and their questionable answers. Sigh. i never know who to trust, the site or the forum.
upvoted 33 times

  **stormshaun** 3 years, 2 months ago

Personally, the purpose of this site is for me to get a glimpse of the questions and search for the correct answers myself hence me learning not just passing the exam.

If you only look for correct answers here, you are failing yourself.



Good luck on your future exams.
upvoted 11 times

  **Paimon** 3 years ago


Agreed. I get a feel for the questions and spend a lot of time researching.
upvoted 4 times

  **Megabyte10** 8 months, 1 week ago

Dude, you come for the questions, and the answers.. you gotta check the work. Its part of the process.
upvoted 4 times

  **Hyrydar** 2 years, 8 months ago

if you expect to show up here and have all the right answers handed to you so that you can go to the exam room and recite them, then i honestly believe you do not belong to this forum. We have healthy debates here..some right and some wrong. The idea is for you to do your research and contribute if you can. You have not paid anyone to provide you with the right answers. you should consider yourself lucky we have a site that provides us with the flavor and style of the questions we might encounter in the exam, it is a priviledge...quit complaining and go to work.
upvoted 35 times

  **TinyRunner** 2 years, 2 months ago

Thank you NZure
upvoted 2 times



  **Quantigo** Highly Voted  3 years, 7 months ago

Correct Answer N Y Y
Dep1File1 is hit by rule 1 which will archive the file by the 10th rendering it unreadable
File 2 and file3 are missed by the first rule and gets hit by the 2nd rule, which will make them still readable by the 10th

<https://docs.microsoft.com/en-us/azure/storage/blobs/archive-rehydrate-overview#:~:text=While%20a%20blob%20is%20in,the%20hot%20or%20cool%20tier>.
upvoted 71 times

  **d6f865d** 5 months, 2 weeks ago

Dep1File1 is edited on Oct 2, still gets hit by the archive rule but that wont happen until the 11th since the file was last modified on the 2nd not the 1st
upvoted 1 times

  **itgg11** 3 years, 4 months ago



NY Y. Agree with Quantigo. An archived file needs to be rehydrated first which may take up to 15 hours.
The question is poorly worded.
"Standard priority: The rehydration request will be processed in the order it was received and may take up to 15 hours."
<https://docs.microsoft.com/en-us/azure/storage/blobs/archive-rehydrate-overview#:~:text=While%20a%20blob%20is%20in,the%20hot%20or%20cool%20tier>
upvoted 6 times

  **Karaole** Most Recent  3 months ago

You cannot directly read data from the Archive tier.
When data is in the Archive tier, it's cold storage that is optimized for infrequent access, and to retrieve it, you need to perform a rehydrate operation. This involves restoring the data to a more accessible tier (like Hot or Cool) before you can read it. The question ask if you can read the files but note once a file is in Archive you can't read it until you rehydrate it. N,Y,N
When data is in the Archive tier, it's cold storage that is optimized for infrequent access, and to retrieve it, you need to perform a rehydrate

operation. This involves restoring the data to a more accessible tier (like Hot or Cool) before you can read it. The question ask if you can read the files but note once a file is in Archive you can't read it until you rehydrate it. N,Y,N

upvoted 2 times

  **areait** 2 months, 1 week ago

That's what i thought, so i also would answer N Y N
upvoted 1 times

  **fouserd** 6 months ago

Should the correct answer be the one provided? The Dept1File1.docx got edited on October 2 there for by the 10th it should still be able to be read. or am i wrong?
upvoted 1 times

  **lahirudk** 7 months ago

This question is valid as per 1st Oct, 2024
upvoted 4 times

  **[Removed]** 8 months ago

WRONG

No

Yes

Yes

upvoted 2 times

  **Megabyte10** 8 months, 1 week ago


The answer is: No, Yes, Yes

No - On October 10 you can not read the Dep1File1.docx file, because its being applied by Rule 1 only. Rule 1 says if blobs not modified for 2 days it will be moved to archive storage and needs to be re-hydrated, which takes several hours. After 9 days its deleted, but its only 8 days old.. so no worries.

-Yes on October 10, you can read File2.docx because rule #2 is applying to here - since it was last edited October 5, only 5 days have passed. After 3 days its moved to cool storage - and files in cool storage are readable!

Yes - File3 is readable because it was last edited on October 2, which throws it in cool storage, and not enough time has passed for it to move to archive storage.

upvoted 1 times

  **Terisssss** 8 months, 4 weeks ago

The reason I agree with given answer is because a prefix in a blob is like creating a vitrual directory structure in a blob container. So, when giving a prefix of Dep1/ it means that a vitrual folder gets created that blobs can get saved into. The question does not specify where the blobs get uploaded so I assume that they get uploaded to container1. Based on that, in order for rule1 to apply to any given blob, the blob would need to have a prefix of Dep1/. The first blob does not have said prefix, it's just that it's name starts with Dep1 which is different from the Dep1/ prefix that creates the folder. For the first question to be NO as everyone says, Dep1File1.txt blob would need to have a prefix of Dep1/ meaning, Dep1/Dep1File1.txt. Basically the only rule that applies here is rule2 and since every blob has a maximum modify date of 9 days we can access every blob.

Correct answer is YYY

upvoted 3 times

  **1964L84Fulie** 9 months ago

Taking the October 1 "Action" literally, the 3 files were uploaded to the Container not the folder /Dep1. Therefor on October 10 you would be able to read Dep1File1.docx.

azcopy cp

/path/to/local/file.txt: The path to your local file.

[account]: Your Azure Storage account name.

[container]: The name of the target container.

[path/to/blob]: The desired path within the container (optional).

upvoted 2 times

  **frantzelopoulos87** 11 months ago

How can the answers for Dep1File1.doc.x and File3 be different, given that I don't see any difference in their lifecycle? They were both created in the same container on the same day and later modified again, but again on the same day. So why do so many people treat them as if they are in different containers or have something different? Or am I just missing something?

upvoted 1 times



  **[Removed]** 8 months, 3 weeks ago

Rule1 only applies to objects/blobs whose names begins with 'Dep1', hence the difference.



Reference: <https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#optionally-enable-access-time-tracking>:~:text=filters%20on%20blobs%20whose%20name%20begins%20with%20log%20in%20a%20container%20called%20sample%2Dcontainer.

ner.

upvoted 3 times

  **tashakori** 1 year, 1 month ago

Given answer is right
upvoted 2 times



  **gil906** 1 year, 2 months ago

I don't get why Dep1File1.docx and File3.docx where uploaded the same day (October 1st), edited the same day (Oct 2nd) and still one can be acceded and the other not on October 10 (Question 1 and 3), I think either both are archived or both are in cool storage, what am I missing?
upvoted 3 times

  **[Removed]** 8 months, 3 weeks ago

Rule1 only applies to objects/blobs whose names begins with 'Dep1', hence the difference.

Reference: <https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#optionally-enable-access-time-tracking>:~:text=filters%20on%20blobs%20whose%20name%20begins%20with%20log%20in%20a%20container%20called%20sample%2Dcontainer.
upvoted 1 times

  **jecampos2** 1 year, 2 months ago



The correct answer should ne NYY.
<https://learn.microsoft.com/en-us/azure/storage/blobs/archive-blob?tabs=azure-portal>
While a blob is in the archive tier, it can't be read or modified. To read or download a blob in the archive tier, you must first rehydrate it to an online tier, either hot or cool.
upvoted 2 times

  **Saurabh_Bhargav** 1 year, 2 months ago

1. No.
You can not read Dept1File.docx , YOu can not read file in archive tier
2. Yes.
Because file is modified on 5 Oct, after 2 days it moved to cool storage and on 10th oct its still in cool storage. You can read file in cool storage.
3. Yes.
Same as File 2 its still in cool storage, because its modified on 2nd oct it still has one day to move to archive tier.
upvoted 6 times

  **PhoenixAscending** 1 year, 3 months ago

This was on my exam, but the rule block was different.
upvoted 1 times

  **adilkhan** 1 year, 3 months ago

N Y Y is 100% correct no need to further discuss this as:
Dep1File1 is hit by rule 1 which will archive the file by the 10th rendering it unreadable
upvoted 1 times

  **SkyZeroZx** 1 year, 3 months ago

Correct Answer N Y Y
Dep1File1 is hit by rule 1 which will archive the file by the 10th rendering it unreadable
File 2 and file3 are missed by the first rule and gets hit by the 2nd rule, which will make them still readable by the 10th

<https://docs.microsoft.com/en-us/azure/storage/blobs/archive-rehydrate-overview#:~:text=While%20a%20blob%20is%20in,the%20hot%20or%20cool%20tier>.
upvoted 2 times



You are configuring Azure Active Directory (Azure AD) authentication for an Azure Storage account named storage1. You need to ensure that the members of a group named Group1 can upload files by using the Azure portal. The solution must use the principle of least privilege. Which two roles should you configure for storage1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.


- A. Storage Account Contributor
- B. Storage Blob Data Contributor
- C. Reader
- D. Contributor
- E. Storage Blob Data Reader

Correct Answer: BC

Community vote distribution

BC (67%)12%9%8%



-   **NaoVaz**

Highly Voted 



 2 years, 7 months ago



Selected Answer: BC



B) "Storage Blob Data Contributor" & C) "Reader"



The following line says it all:
"The Reader role is an Azure Resource Manager role that permits users to view storage account resources, but not modify them. It does not provide read permissions to data in Azure Storage, but only to account management resources. The Reader role is necessary so that users can navigate to blob containers in the Azure portal. For example, if you assign the Storage Blob Data Contributor role to user Mary at the level of a container named sample-container, then Mary is granted read, write, and delete access to all of the blobs in that container. However, if Mary wants to view a blob in the Azure portal, then the Storage Blob Data Contributor role by itself will not provide sufficient permissions to navigate through the portal to the blob in order to view it. The additional permissions are required to navigate through the portal and view the other resources that are visible there." - <https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access?tabs=portal>
upvoted 78 times
-   **maxsteele** 1 year, 7 months ago



"ou are configuring Azure Active Directory (Azure AD) authentication for an Azure Storage account named storage1. You need to ensure that the members of a group named Group1 can upload files by using the Azure portal"



Nowhere does it ask to limit the roles to Blob only. B is incorrect. You need A and C
upvoted 3 times
-   **3b66239** 10 months, 4 weeks ago



I may be wrong but File Storage does not accept Azure AD, only SAS no?
upvoted 1 times
-   **Batiste2023** 1 year, 6 months ago

Least privilege ;-) You're supposed to be able to upload SOMETHING, but not more than that, B is more constricted than A, so that should be correct...
upvoted 4 times
-   **Alscoran** 1 year, 5 months ago



Storage Account Contributor has no DataActions. Therefore it cannot add data.
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-account-contributor>
upvoted 2 times
-   **marcosviniciuscb** 5 months ago

but it's telling you with less privileges, and option E gives you less privileges than option C
upvoted 1 times
-   **KennethLZK** 2 years, 3 months ago

Why not BE? "Storage Blob Data Contributor" & " Storage Blob Data Reader"?
upvoted 5 times
-   **Driede** 2 years ago

The "Storage Blob Data Reader" doesn't let you see the storage account in the portal.
upvoted 13 times
-   **klexams** 2 years, 6 months ago

How can it be C. It says to upload files. Surely not reader
upvoted 3 times



  **Citmerian** 2 years, 6 months ago
BC - The two combined roles accomplish "last privilege" is the key
upvoted 5 times

  **AK4U_111** Highly Voted  2 years, 2 months ago
TESTED IN LAB:




Assigning the Storage Account Contributor and Storage Blob Data Reader rolls to the group and having the user (which is a part of that group) sign in to the portal, the storage account isn't even listed under storage accounts.



After removing the Storage Blob Data Reader and assigning the Reader roll to the group, the storage account is listed and the users of the group can creat blobs/fileshares etc.

ANSWER: BC
upvoted 14 times

  **maxsteele** 1 year, 7 months ago
"ou are configuring Azure Active Directory (Azure AD) authentication for an Azure Storage account named storage1.
You need to ensure that the members of a group named Group1 can upload files by using the Azure portal"

Nowhere does it ask to limit the roles to Blob only. B is incorrect. You need A and C
upvoted 2 times

  **lumax007** Most Recent  2 months, 1 week ago
Selected Answer: AC
Upload & read the data in the storage account not in the blob.
upvoted 1 times

  **OjayL** 4 months, 2 weeks ago
Selected Answer: BE
To ensure that the members of Group1 can upload files to the Azure Storage account named storage1 using the Azure portal, while adhering to the principle of least privilege, you need to assign them roles that provide the minimum required permissions.

The most appropriate roles are:



Storage Blob Data Contributor (Option B): This role allows users to read, write, and delete blobs in the storage account. It's specific to blob data operations, which is what you need for uploading files.

Storage Blob Data Reader (Option E): This role allows users to read blob data. It's complementary to the Data Contributor role, ensuring users can also read the data they upload.



So the correct answer remains:



B. Storage Blob Data Contributor



E. Storage Blob Data Reader
upvoted 1 times



  **aaqibkhan123** 4 months, 2 weeks ago
Answer is A and B.
"You need to ensure that the members of a group named Group1 can upload files by using the Azure portal."

You cannot upload files using the reader role
upvoted 1 times

  **[Removed]** 8 months ago
Selected Answer: BC
B & C are correct
upvoted 1 times

  **c035d62** 11 months, 4 weeks ago
You don't know if You need to charge blobs or files
upvoted 2 times

  **tashakori** 1 year, 1 month ago
B and C is correct
upvoted 1 times

  **jecampos2** 1 year, 2 months ago
Selected Answer: BC
B) "Storage Blob Data Contributor" & C) "Reader"
upvoted 1 times

- PhoenixAscending

1 year, 3 months ago

This was on my exam. Most likely the correct answer is provided by NaoVaz.

upvoted 1 times
- adilkhan

1 year, 3 months ago

B, C is correct!

upvoted 1 times
- FlaShhh

1 year, 3 months ago

I am confused as to why everyone is choosing B) Storage Blob Data Contributor. The question does not explicitly say that the files will be uploaded to blobs, the files to be uploaded may be uploaded to file shares, so wont A) Storage Account Contributor be the more appropriate choice?

upvoted 1 times
- knowakuk

4 months, 3 weeks ago

Storage account is for resources not for data. It's like with linux.
You have a file in a folder. You can have write/read on a file (data permission) but if you dont have at least read on folder (resource) you won't be able to get to the file.

upvoted 1 times
- hotspot02103

1 year, 3 months ago

Selected Answer: AC

ebanie

upvoted 3 times
- Aniruddha_dravyakar

1 year, 7 months ago

Answer is BC

upvoted 1 times
- iamchoy

1 year, 7 months ago

Selected Answer: BC

To ensure that members of Group1 can upload files using the Azure portal while adhering to the principle of least privilege, you need to assign roles that give them just enough permissions to perform the task without any extraneous permissions.

B. `Storage Blob Data Contributor`: This role allows for reading, writing, and deleting Azure Storage blobs (object data). This role is necessary for members to be able to upload files.

C. `Reader`: This role gives the user read access to see the storage account and its properties but doesn't allow for any modifications. This role would be needed to navigate to the storage account in the Azure portal.

Assigning these roles should give Group1 members the ability to upload files to the storage account via the Azure portal without giving them more permissions than they need.

upvoted 3 times
- obaemf

1 year, 7 months ago

Storage Blob Data Contributor limits the scope to just blobs. Question clearly say we need to be able to upload files to the storage account. How would we be able to upload a file to a FileShare? Don't you think a Storage Account Contributor would expand the scope to include other file types?

upvoted 3 times
- rikininetsix

1 year, 7 months ago

Selected Answer: AC

You need to ensure that the members of a group named Group1 can upload files by using the Azure portal.

Files is clearly mentioned in the question, by selecting 'Storage Blob Data Contributor' your scope is limited to only containers & blobs.

So, in my opinion A & C are the correct options.

upvoted 6 times
- maxsteele

1 year, 7 months ago

Exactly, Storage Blob options are unnecessarily limiting the role. The question never states that Blob access is the only access needed. It states that access is needed to the Storage Account in general, so A & C are correct.

upvoted 1 times
- Gregsenn

1 year, 8 months ago

Question is still relevant, came on exam today

upvoted 6 times
- CarlosMarin

1 year, 8 months ago


On mine as well 31/08/2023

upvoted 4 times
- alverdiyev91

1 year, 4 months ago

so what was the answer?? oh man why you put comments without answers?? what's wrong with you??

upvoted 2 times

 **sakibmas** 1 year, 8 months ago

Selected Answer: BC

To Browse the Storage Account in Azure Portal, the Reader role is required
upvoted 1 times

HOTSPOT -

You have an Azure Storage account named storage1 that stores images.

You need to create a new storage account and replicate the images in storage1 to the new account by using object replication.

How should you configure the new account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Account type:

StorageV2 only

StorageV2 or FileStorage only

StorageV2 or BlobStorage only

StorageV2, BlobStorage, or FileStorage

Object type to create in the new account:

Container

File share

Table

Queue

Correct Answer:

Answer Area

Account type:

StorageV2 only

StorageV2 or FileStorage only

StorageV2 or BlobStorage only

StorageV2, BlobStorage, or FileStorage

Object type to create in the new account:

Container

File share

Table

Queue

Reference:
<https://docs.microsoft.com/en-us/azure/storage/blobs/object-replication-overview>

- Ewong

Highly Voted

3 years ago

Account type: StorageV2 or BlobStorage only

Object type to create in the new account: Container

Object Replication supports General Purpose V2 and Premium Blob accounts.
Blob versioning should be enabled on both the source and destination storage account.
Change feed is enabled on the source storage account.



upvoted 91 times
- [Removed]

2 years, 4 months ago

Object replication is supported by Storage V2 and Premium Block Blob storage. Legacy Block blob storage does not support object replication. BlobStorage specifically refers to Legacy Block Blob storage while Premium Block Blob storage is always referenced as BlockBlobStorage. In

short we can only use StorageV2 in this case.

upvoted 23 times

  **ggogel** 1 year, 4 months ago

I agree.
StorageV2 only
Container
upvoted 3 times

  **[Removed]** 2 years, 4 months ago

Correction: BlobStorage specifically refers to Legacy Blob storage
upvoted 5 times

  **tableton** 1 year, 1 month ago

Don't agree
Account type: StorageV2 only
Object replication is supported for general-purpose v2 storage accounts and premium block blob accounts Blobstorage is not premium
Object replication is supported for general-purpose v2 storage accounts and premium block blob accounts
upvoted 5 times

  **tableton** 1 year, 1 month ago

Extracted from <https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-overview>
upvoted 1 times

  **majerly** Highly Voted 2 years, 7 months ago

today in exam
1) Account type: "StorageV2 or Blobstorage only"
2) Object type to create in the new account: "Container"
upvoted 34 times

  **Rams_84z06n** 2 years, 1 month ago

The answer for (1) is incorrect. It should be "Storage V2 only". <https://docs.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview#rule-actions>
Object replication is supported for general-purpose v2 storage accounts and premium block blob accounts. Blob Storage is standard blob account, not premium.
upvoted 10 times

  **Firststack** Most Recent 2 months, 3 weeks ago

The giving answer is correct - <https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-overview>
upvoted 1 times

  **Bravo_Dravel** 3 months, 1 week ago

Account type: StorageV2 only
it is only available for General-purpose v2 storage accounts and premium block blob accounts
Object type to create in the new account: Container
upvoted 1 times

  **[Removed]** 6 months ago

CORRECT
upvoted 2 times

  **[Removed]** 7 months, 3 weeks ago

WRONG

Account type: StorageV2 only
Object type: Container

Object replication is supported for general-purpose v2 storage accounts and PREMIUM block blob accounts.

Blob Storage mentioned here is not premium.

<https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-overview#:~:text=Object%20replication%20is%20supported%20for%20general%2Dpurpose%20v2%20storage%20accounts%20and%20premium%20block%20blob%20accounts.>

upvoted 2 times

  **[Removed]** 6 months ago

ignore this, after some researches, i found out that both General-purpose v2 (GPv2) and Blob Storage are supported for object replication.

given answer is CORRECT
upvoted 2 times

  **Y2** 9 months ago

Hi guys just passed the exam with a 886!! most of the questions were from here, but there were new questions mainly about encryption, keys and container commands (creating and applying a image to one).

A WHOLE NEW case study on keys, encryption(Win and Linux VM's with different disks and they asked which ones can be encrypted, attribute assignment roles (go over)

There was also one question that asked what's the easiest way to give a v-net and your home network access to a storage account without using p2s. - Confusion!!!!

Here some of the questions I remember (please note you questions will not be exactly the same) I have my page setup to show 50 questions per page -

upvoted 2 times

🗄️ 👤 **Y2** 9 months ago

1.26,36
2.25
3.68
4.26,31,41,43,44,48,49,53,57,59(different question but same reasoning)
5.68,84,9,14,16,17,18,19
6.24.27,29,49,55,
7.72,95,1
8.20,22,49
9.90,94
10.32,41

And connection monitor question from here that asked how many you need - there were 2 regions so I said 2

upvoted 3 times

🗄️ 👤 **Y2** 9 months ago

Note - if you open MLearn close it wait 4-5 sec's before you get to the next question
My exam crashed 3 times before I tried this

Good luck!!!!!!

upvoted 2 times

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

Account type: StorageV2 or BlobStorage only

Object type: Container

upvoted 1 times

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

Object replication supports general-purpose v2 storage and premium block blob accounts. not Blob Storage

upvoted 3 times

🗄️ 👤 **MOSES3009** 1 year, 5 months ago

Not right answer. IMHO, there must be

StorageV2 only

Container

upvoted 7 times

🗄️ 👤 **SgtDumitru** 1 year, 5 months ago

Agree, only StorageV2 & BlockBlobStorage(Premium Block Blobs) supports object replication.

upvoted 3 times

🗄️ 👤 **athli** 1 year, 6 months ago

Object replication is supported for general-purpose v2 storage accounts and premium block blob accounts. Both the source and destination accounts must be either general-purpose v2 or premium block blob accounts. Object replication supports block blobs only; append blobs and page blobs aren't supported.

upvoted 3 times

🗄️ 👤 **Aniruddha_dravyakar** 1 year, 7 months ago

Account type: StorageV2 or BlobStorage only-- since requirement is to store image

Object type to create in the new account: Container containers can store image

upvoted 1 times

🗄️ 👤 **Mehedi007** 1 year, 9 months ago

1) StorageV2 only.

Because 'Blobstorage' is a legacy storage a/c type. 'BlockBlobstorage' is a premium storage a/c type which supports object replication.

"Object replication is supported for general-purpose v2 storage accounts and premium block blob accounts."

<https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-overview#prerequisites-and-caveats-for-object-replication>

2) Container

upvoted 8 times

🗄️ 👤 **Mehedi007** 1 year, 9 months ago

Find 'Blobstorage' & 'BlockBlobstorage' here.

<https://learn.microsoft.com/en-us/azure/templates/microsoft.storage/storageaccounts?pivots=deployment-language-arm-template#storageaccounts-1>

upvoted 1 times

🗨️ 👤 **RandomNickname** 1 year, 10 months ago

Answer incorrect

Blob is legacy and not block blob which is premium

Q1:StorageV2

Q2:Container

See;

<https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-overview>

"Object replication is supported for general-purpose v2 storage accounts and premium block blob accounts. Both the source and destination accounts must be either general-purpose v2 or premium block blob accounts. Object replication supports block blobs only; append blobs and page blobs aren't supported."

upvoted 9 times

🗨️ 👤 **Driede** 2 years ago

The Account Type should be "StorageV2 only". As stated in <https://learn.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-powershell> BlobStorage refers to legacy blob storage which does not support object replication.

upvoted 5 times

🗨️ 👤 **NJTH** 2 years ago

Exactly the same question was on today's exam.

(7th April 2023)

upvoted 9 times

🗨️ 👤 **AzZnLuVaBol** 2 years, 1 month ago

On the Exam 3/29/23.

upvoted 9 times

🗨️ 👤 **AK4U_111** 2 years, 2 months ago

StorageV2 only

Container

"Object replication is supported for general-purpose v2 storage accounts and premium block blob accounts. Both the source and destination accounts must be either general-purpose v2 or premium block blob accounts. "

Source:

<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-sync-group-and-a-cloud-endpoint>

upvoted 12 times

You have an on-premises server that contains a folder named D:\Folder1.

You need to copy the contents of D:\Folder1 to the public container in an Azure Storage account named contosodata.

Which command should you run?

- A. `https://contosodata.blob.core.windows.net/public`
- B. `azcopy sync D:\folder1 https://contosodata.blob.core.windows.net/public --snapshot`
- C. `azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive`
- D. `az storage blob copy start-batch D:\Folder1 https://contosodata.blob.core.windows.net/public`

Correct Answer: C

Community vote distribution

C (100%)

  **mlantonis** Highly Voted 3 years, 11 months ago

Correct Answer: C

A: URL of the Storage Account.

B: The `azcopy sync` command replicates the source location to the destination location. However, the file is skipped if the last modified time in the destination is more recent.

C: The `azcopy copy` command copies a directory (and all the files in that directory) to a blob container. The result is a directory in the container by the same name.

D: The `az storage blob copy start-batch` command copies multiple blobs to a blob container.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>
upvoted 142 times

  **naveener** Highly Voted 4 years, 9 months ago



copies a directory (and all of the files in that directory) to a blob container:-

`azcopy copy 'C:\myDirectory' 'https://mystorageaccount.blob.core.windows.net/mycontainer' --recursive`

To copy to a directory within the container :-

`azcopy copy 'C:\myDirectory' 'https://mystorageaccount.blob.core.windows.net/mycontainer/myBlobDirectory' --recursive`

upvoted 40 times

  **Shailen** 3 years, 10 months ago

Basically given answer is correct.



upvoted 4 times

  **[Removed]** Most Recent 8 months ago

Selected Answer: C

C is corerct

upvoted 1 times

  **tashakori** 1 year, 1 month ago



C is right

upvoted 1 times

  **Amir1909** 1 year, 2 months ago



C is correct

upvoted 1 times

  **NU88** 1 year, 4 months ago

I personally feel none of them is correct command. The C barely is close but can't run successfully. The Blob storage needs to be accessed with authentication. In this case a SAS string on the container needs to be attached to the command.

upvoted 1 times

  **mantik** 1 year, 4 months ago

You can use env variable to auth with sas token ;-)

upvoted 1 times

🗨️ **Aniruddha_dravyakar** 1 year, 7 months ago

Answer is C
upvoted 1 times

🗨️ **iamchoy** 1 year, 7 months ago

Selected Answer: C

The correct command to recursively copy all contents of `D:\Folder1` to the specified Azure Blob container is:

C. `azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive`

Here's the breakdown:

- `azcopy copy`: This command is used to copy data.
- `D:\folder1`: This is the source directory.
- `https://contosodata.blob.core.windows.net/public`: This is the destination URL of the blob container.
- `--recursive`: This flag ensures that the operation goes through all directories and subdirectories in the source to copy the data.

Remember to make sure you are authenticated with `azcopy` (using `azcopy login` or another authentication method) and have the necessary permissions to access the target blob container.

upvoted 1 times

🗨️ **UmbongoDrink** 2 years, 2 months ago

Selected Answer: C

C) " azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive"

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>

upvoted 4 times

🗨️ **zelck** 2 years, 3 months ago

Same as question 51.

<https://www.examttopics.com/discussions/microsoft/view/93898-exam-az-104-topic-3-question-51-discussion>

upvoted 1 times

🗨️ **zelck** 2 years, 3 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>

Copies source data to a destination location

upvoted 1 times

🗨️ **NaoVaz** 2 years, 7 months ago

Selected Answer: C

C) " azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive"

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>

upvoted 2 times

🗨️ **EmnCours** 2 years, 8 months ago

Selected Answer: C

Correct Answer: C

upvoted 1 times

🗨️ **Lazylinux** 2 years, 10 months ago

Selected Answer: C

I C so i agree

upvoted 3 times

🗨️ **epomatti** 3 years ago

Selected Answer: C

azcopy recursive - C is correct

upvoted 2 times

🗨️ **techie_11** 3 years ago

On exam 4/12/2022. Answer is correct

upvoted 2 times

🗨️ **benvdw** 3 years, 1 month ago

on exam 13/3/2022

upvoted 3 times

You have an Azure subscription.

In the Azure portal, you plan to create a storage account named storage1 that will have the following settings:

- ☞ Performance: Standard
- ☞ Replication: Zone-redundant storage (ZRS)
- ☞ Access tier (default): Cool
- ☞ Hierarchical namespace: Disabled

You need to ensure that you can set Account kind for storage1 to BlockBlobStorage.

Which setting should you modify first?

- A. Performance
- B. Replication
- C. Access tier (default)
- D. Hierarchical namespace

Correct Answer: A

Community vote distribution

A (100%)

🗳️  **sk1803** Highly Voted 👍 3 years, 7 months ago

Answer is correct

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal>

Select Standard performance for general-purpose v2 storage accounts (default). This type of account is recommended by Microsoft for most scenarios. For more information, see Types of storage accounts.

Select Premium for scenarios requiring low latency. After selecting Premium, select the type of premium storage account to create. The following types of premium storage accounts are available:

Block blobs
File shares
Page blobs
upvoted 55 times

🗳️  **Bere** Highly Voted 👍 3 years, 4 months ago

Answer is A. Performance.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-cli>

These are the supported values for the kind parameter:

StorageV2 = Standard general-purpose v2
BlockBlobStorage = Premium block blobs
FileStorage = Premium file shares
StorageV2 = Premium page blobs
Storage = legacy Standard general-purpose v1
BlobStorage = legacy blob storage

As you can see above BlockBlobStorage is only available for Premium_LRS or Premium_ZRS.

So we must change the Performance from Standard to Premium.

upvoted 36 times

🗳️  **Dankho** Most Recent ⌚ 6 months, 4 weeks ago

Selected Answer: A

Given answer is correct.

upvoted 1 times

🗳️  **[Removed]** 8 months ago



Selected Answer: A



A is corerct

upvoted 1 times

🗳️  **Roee1** 9 months, 2 weeks ago



I don't really understand the question, if someone can explain further.
specifically about setting storage kind to block blob and what is the difference between the storage account kind to the storage account type
upvoted 4 times



  **Limobakry** 6 months, 3 weeks ago
The setting you need to modify first is A. Performance, because BlockBlobStorage requires Premium performance. Therefore, the performance setting must be changed to Premium before you can set the Account kind to BlockBlobStorage.
upvoted 4 times



  **WeepingMaplte** 1 year ago

Selected Answer: A



<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-create?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json&tabs=azure-portal#:~:text=Supported%20values%20for%20the%20kind%20parameter>
upvoted 1 times

  **tashakori** 1 year, 1 month ago
B is correct
upvoted 1 times

  **tashakori** 1 year, 1 month ago
B is right
upvoted 1 times



  **Prashanthk5814** 1 year, 1 month ago
Answer is Replication



Azure Storage Replication Types:
General-purpose v1:
Supports Locally Redundant Storage (LRS) and Geo-Redundant Storage (GRS)/Read-Access Geo-Redundant Storage (RA-GRS).
General-purpose v2:
Supports LRS, Zone-Redundant Storage (ZRS), GRS/RA-GRS, and Geo-Zone-Redundant Storage (GZRS)/Read-Access Geo-Zone-Redundant Storage (RA-GZRS).
Block Blob Storage:
Supports only LRS.
Blob Storage:
Supports LRS and GRS/RA-GRS
upvoted 2 times



  **chrillelundmark** 3 months, 4 weeks ago
Don't know where you been looking but that's wrong. BlokBlobStorage supports LRs and ZRS.



<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal#storage-account-type-parameters>

BUT! Does BlockBlobStorage support Storage Tiers??? And if not, is this the first one we need to change?
upvoted 1 times

  **Amir1909** 1 year, 2 months ago
A is correct
upvoted 1 times

  **clg003** 1 year, 6 months ago
I agree it needs to be Premium... but what does the tiering option do when you try and move it to premium since premium doesn't support tiering?
upvoted 3 times

  **Aniruddha_dravyakar** 1 year, 7 months ago
Answer is A since blockblob supports premium performance
upvoted 1 times

  **iamchoy** 1 year, 7 months ago

Selected Answer: A

The "BlockBlobStorage" account kind is specialized for storing block blobs and append blobs. It is optimized for high transaction rates.

To set the account kind to "BlockBlobStorage", the storage account must have:
- Performance: Premium
- Replication: Locally-redundant storage (LRS) or Zone-redundant storage (ZRS)

Given the provided settings, the "Performance" setting is set to "Standard", which is not compatible with the "BlockBlobStorage" account kind. Therefore, you should modify:

A. Performance

You would need to set it to "Premium" to be able to select "BlockBlobStorage" as the account kind.
upvoted 4 times

  **Mehedi007** 1 year, 9 months ago



Selected Answer: A

Performance.

Because BlockBlobStorage is a premium account type.



<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal#basics-tab>

upvoted 2 times

  **ed79** 1 year, 11 months ago

but this is strange because you cannot change the performance kind once you create the account

upvoted 2 times

  **xRiot007** 1 year, 11 months ago

The questions says that you want to create one, not that one is already created. So, you are reviewing the options and you deem necessary to change the performance to Premium so you can have Block Blobs. Then, with the correct settings in place you can create it.

upvoted 2 times

  **Spam101198** 2 years, 2 months ago

A) Performance : Because Blockblob storage supported in premium not in Standard.

upvoted 3 times

  **AK4U_111** 2 years, 2 months ago

Portal > Create a storage account > Basics > If you need to create a legacy storage account type, please click here > Performance = Premium > Account kind = BlockBlobStorage

upvoted 1 times

Browse atleast **50%** to increase passing rate 



Viewing page 1 out of 1 pages.

Viewing questions **1-200** out of 606 questions