



Exam AZ-104 All Actual Questions

Question #1

Topic 2

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>

Comments

alen995454 Highly Voted 2 months, 2 weeks ago

The given answer is incorrect:

Box 1. Network Contributor on RG1

Box 2. Network Contributor on RG1

upvoted 159 times

Jaiiiee 1 day, 15 hours 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

Jaiiiee 1 day, 15 hours 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 1 times

Hyrydar 2 years, 5 months ago

There is something that we all seem to be forgetting here..and that is that Azure RBAC roles can be applied at three different scopes...management group, subscription, resource group and finally resource. So, LB1 and LB2 are resources that we want the Network Contributor role to manage, which by the way satisfies the principle of least privilege. When you apply the scope to the resource group, then it is applied to all the resources in the resource group which is not what we want. The question specifically referred to LB1 and LB2. These resources are atomic, therefore applying the scope to the two will affect just those two resources. Therefore the given answers are correct.

upvoted 245 times

A_GEE 2 years, 4 months ago

The question ask "LB1 and LB2" at the same time. So need the RG level contributor for it. The answer should be both on the RG level.

Network Contributor on RG1

upvoted 5 times

KingChuang 2 years, 1 month ago

Wrong Answer!

If you on RG1,you can managment other network resourece!

upvoted 3 times

KingChuang 2 years, 1 month ago

Orz.Correct answer:

Network Contributor on RG1

Network Contributor on RG1

Reason: These functions need access IP and VM.
If grant on resources, load balance can't access IP
upvoted 7 times

michaelmarkov 1 year, 8 months ago

Does it say anywhere that IP and VMs should be in the same resource group to work with LB?
upvoted 1 times

xRiot007 1 year, 6 months ago

"The question ask "LB1 and LB2" at the same time" - yes and if Admin has network contributor on LB1 and LB2 it will manage them at the same time. A user can have multiple roles.
upvoted 3 times

NTT_Sttg09 2 years, 1 month ago

netw. contributor on LB fulfilled the question1, also netw. contributor on LB2.
upvoted 4 times

DaviZZZZ 1 year, 4 months ago

Exactly!
upvoted 5 times

sca88 1 month ago

Can you provide a documentation link? I would answer LB contributor for both
upvoted 1 times

Abd99 Highly Voted 2 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 50 times

XristophD 2 years 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 message 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 28 times

FNog 1 year, 9 months ago

Both Load Balancers already exist, though...
Only management rights are requested so, LB1 and LB2.
upvoted 5 times

jackill 1 year, 4 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, 5 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

CloudEngJS Most Recent 2 weeks ago

Tested and confirmed in a lab, the correct answers are NetworkContributor on RG1

upvoted 1 times

jorex535 3 weeks, 5 days 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 1 month, 2 weeks 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 1 month, 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 1 month, 2 weeks ago

Network Contributor on LB can't add a health probe.

upvoted 1 times

Dankho 1 month, 2 weeks ago

I'm glad the discussion basically has every possibility.

upvoted 4 times

happpieee 1 month, 3 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 1 month, 3 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 2 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 3 times

Alandt 2 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 2 times

nmshrw 11 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

SeMo0o0o0o 2 months, 4 weeks ago

WRONG

- Network Contributor on RG1
 - Network Contributor on RG1
- upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

wrong

1st. Network Contributor on RG1
2nd. Network Contributor on RG1
upvoted 1 times

salihGamar 3 months, 4 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 1 times

divzrajshekhar123 4 months, 2 weeks 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 1 times

090200f 5 months, 2 weeks ago

When a backend pool is configured by IP address, it will behave as a basic load balancer with default outbound enabled. For secure by default configuration and applications with demanding outbound needs, configure the backend pool by NIC.

Box 1: Network Contributor on RG1

An Azure Load Balancer health probe is a feature that detects the health status of your application instances(each one separately)

Box2: Network contributor on LB2

upvoted 1 times

OscarFRitz 5 months, 2 weeks ago

Tested, both need Network Contributor on RG1

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #2

Topic 2

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. **Most Voted**
- C. Recreate AKS1.
- D. From AKS1, create a namespace.

Correct Answer: B

Community vote distribution

B (90%)

Other (10%)

Comments

AlleyC Highly Voted 2 years, 6 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 73 times

FredFrom 1 month, 3 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 1 times

tweedo 2 years, 4 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 1 year, 9 months ago

B is correct

upvoted 2 times

18c2076 Highly Voted 9 months 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 18 times

GlixRox 6 months, 1 week ago

Glad you said this because I had never heard of this during my course.

upvoted 3 times

Jaijee Most Recent 1 day, 15 hours 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 1 times

FredFrom 1 month, 3 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 1 month, 3 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 2 months 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 2 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 2 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 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

Witbaas13 3 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

Nico1973 5 months ago

To ensure that access to AKS1 can be granted to the users in the contoso.com Azure AD tenant, you should first:

A. From contoso.com, modify the Organization relationships settings.

Explanation:

By modifying the Organization relationships settings in the contoso.com Azure AD tenant, you can establish the necessary trust relationships and permissions required for users in the tenant to access and manage resources, such as the AKS1 cluster. This step is essential for enabling user access and control over AKS1 within the Azure environment. Once the Organization relationships settings are appropriately configured, users in the contoso.com Azure AD tenant will be able to grant access to AKS1 effectively.

upvoted 2 times

Nico1973 5 months ago

To ensure that access to AKS1 can be granted to the users in contoso.com, you should first select option A: From contoso.com,

modify the Organization relationships settings. This action will allow you to establish the necessary connections and permissions between the Azure AD tenant (contoso.com) and the AKS cluster (AKS1), enabling users in contoso.com to access and manage AKS1 effectively.

upvoted 1 times

Lazylinux 6 months, 1 week ago

Selected Answer: B

B is correct as per

<https://learn.microsoft.com/en-us/azure/aks/concepts-identity>

upvoted 2 times

3c5adce 7 months ago

D. From AKS1, create a namespace.

To manage access to Azure Kubernetes Service (AKS) clusters effectively, namespaces are used within Kubernetes to segment resources and provide a scope for access policies. By creating a namespace in AKS1, you can define Role-Based Access Control (RBAC) policies specifically for that namespace, which can then be used to grant appropriate permissions to users from the contoso.com Azure AD tenant. This is the first operational step in ensuring users can be granted access to specific parts of the AKS cluster without recreating the cluster or modifying authentication systems.

upvoted 2 times

trevax 3 months, 1 week ago

However, by default, the default namespace is used in AKS. We can apply RBAC directly to this namespace, so creating a new one may not be necessary for access management.

upvoted 1 times

3c5adce 7 months, 2 weeks ago

ChatGPT says D: D. From AKS1, create a namespace.

To grant access to the users in the contoso.com Azure AD tenant, you need to integrate AKS with Azure AD for authentication and authorization. One of the steps involved in this process is to create a Kubernetes namespace. Once the namespace is created, you can configure RBAC (Role-Based Access Control) to grant appropriate permissions to users and groups from the Azure AD tenant.

Options A and B are not relevant to granting access to AKS. Option C, recreating AKS1, is not necessary as the existing AKS cluster can be configured to integrate with Azure AD for user access control. Therefore, option D is the correct first step to enable access for contoso.com users.

upvoted 3 times

trevax 3 months, 1 week ago

true but by default, the default namespace is used in AKS. We can apply RBAC directly to this namespace, so creating a new one may not be necessary for access management.

Answer is still B i think

upvoted 1 times

Iron_Man_111 8 months, 3 weeks ago

Still confuse between A and B. Can someone provide more reasons to go for A or B whatever you feel the correct answer ?

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #3

Topic 2

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 **Most Voted**
- B. a Security group that uses the Assigned membership type
- C. a Microsoft 365 group that uses the Dynamic User membership type **Most Voted**
- 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 (92%)

Other (8%)

Comments

kennynelcon **Highly Voted** 2 years, 6 months ago

Selected Answer: AC

Correct Answer: A and C

Only O365 groups support automatic deletion after 180 days.

upvoted 56 times

jackdryan 1 year, 9 months ago

A and C are correct

upvoted 6 times

ConanBarb 2 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
- 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 8 times

MrBlueSky 1 year, 9 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 26 times

Lazylinux Highly Voted 2 years, 5 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 15 times

Afsan 1 year, 11 months ago

Thanks

upvoted 1 times

RealmTarget Most Recent 4 days, 3 hours 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 1 times

Mark74 5 days, 16 hours ago

Selected Answer: AC

A and C for me is correct

upvoted 1 times

Dankho 1 month, 2 weeks ago

Selected Answer: AC

Both related to SharePoint, others are not.

upvoted 3 times

FredFrom 1 month, 3 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 1 month, 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 2 months, 1 week 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 1 times

stanislaus450 2 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 1 times

Josh219 2 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

SeMoOo0o0o 3 months, 1 week ago

Selected Answer: AC

A & C are correct

upvoted 1 times

Nico1973 5 months ago

Answer: C and D

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 6 months, 1 week 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 1 month, 3 weeks ago

there are two different tenants

upvoted 1 times

Homedollars 6 months, 3 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 6 months, 3 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 1 month, 3 weeks ago

because each answer provide a complete solution.

upvoted 1 times

Amir1909 10 months ago

Correct

upvoted 1 times

reggina 11 months ago

365 Groups don't "ensure" deletion

<https://learn.microsoft.com/en-us/entra/identity/users/groups-lifecycle>

"Groups with user activities are automatically renewed as the expiration nears."

I don't get it

upvoted 1 times

suddin1 6 months, 3 weeks ago

now I'm confused about the answer

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #4

Topic 2

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: Review1

Description: (empty)

* Start date: 2018-11-22

Frequency: One time

Duration (in days): 1

End: Never

* Number of times: 0

* End date: 2018-12-22

Users

Users to review: Members of a group

Scope: Guest users only
 Everyone

* Group: Group1

Reviewers

Reviewers Group owners

Programs

Link to program

Default program >

v Upon completion settings

v 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>

Comments

AlleyC Highly Voted 2 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 205 times

Wheels90 1 year, 5 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 10 times

ggogel 1 year 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 4 times

Key94 2 years, 4 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 4 months, 3 weeks ago

Access Review supports nesting of groups.

upvoted 2 times

morito 1 year, 9 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, 6 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 55 times

MCLC2021 7 months, 1 week 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, 6 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, 4 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 4 times

Lazylinux 2 years, 5 months ago

U R right and Armina is WRONG..see my comments

upvoted 7 times

RVivek **Most Recent** 1 month 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 1 times

jamesf 1 month, 3 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 2 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

SeMo0o0o0o 2 months, 4 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 6 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 7 months ago

For this round going with NNY

upvoted 1 times

varinder82 7 months, 1 week ago

Final Answer: No No NO

upvoted 1 times

af68218 8 months, 1 week 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

l3gcertgrinders 9 months, 2 weeks 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 8 months, 2 weeks 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 10 months ago

CORRECT

upvoted 1 times

labsinghlab 11 months ago

3) NO because nested group

upvoted 2 times

Indy429 11 months, 4 weeks 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

WeepingMaplte 1 year, 1 month ago

User3 can perform an access review of UserB = Yes

Reference:

1. 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.
<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-perform-roles-and-resource-roles-review#approve-or-deny-access>

2. Microsoft 365 and Security group owner can create access review
<https://learn.microsoft.com/en-us/entra/id-governance/create-access-review>

upvoted 4 times

Batiste2023 1 year, 1 month ago

Apparently the answer is NO-NO-YES.

Although MS Learn states that access reviews for users with permissions through nested groups won't have any effect. But those users will show up for review.

Source: <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-perform-roles-and-resource-roles-review#approve-or-deny-access>

upvoted 3 times

Gnilre93 1 year, 2 months ago

I think that the simple solution here is this:

No/No/Yes

Reason is that the review in the picture points out that it's only searching for Guest users and User B is the Only quest user from the answer area.

User 1 is a member and User A is a member

upvoted 1 times

Gnilre93 1 year, 2 months ago

(Typo- User B is a guest user, not quest)

The criteria for the creation of the review:

Look at the picture and look for "Users". you will then find the scope is set to "Guest Users only".

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #5

Topic 2

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.

You can create a virtual machine in Subscription2.

You can add Subscription1 to ManagementGroup11.

Correct Answer:

Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create a virtual machine in Subscription2.	<input checked="" type="radio"/>	<input type="radio"/>
You can add Subscription1 to ManagementGroup11.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

Virtual networks are not allowed at the root and is inherited. Deny overrides allowed.

Box 2: Yes -

Virtual Machines can be created on a Management Group provided the user has the required RBAC permissions.

Box 3: Yes -

Subscriptions can be moved between Management Groups provided the user has the required RBAC permissions.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview> <https://docs.microsoft.com/en-us/azure/governance/management-groups/manage#moving-management-groups-and-subscriptions>



Comments

fedztedz Highly Voted 4 years ago

Answer is Wrong : It should Be NO NO NO

- subscription should be moved by can't be added to 2 groups.

upvoted 247 times

tita_tovenaar 3 years, 5 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 26 times

tita_tovenaar 3 years, 5 months ago

sorry, my bad. answer 2 is No. By allowing networks, you deny all the rest.

upvoted 15 times

Durden871 1 year, 8 months 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 57 times

alexn76 1 year, 8 months ago

N Y N

You can create VM on existing network

upvoted 2 times

KrisJin 1 year, 7 months ago

Who told you there is an existing VNET?

upvoted 9 times

Batiste2023 1 year, 1 month 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 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 3 times

ggogel 1 year 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 7 times

Zemar 1 year, 8 months 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 20 times

avidlearner 1 year, 4 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 6 times

Ruzhdi 8 months, 3 weeks ago

Answer 2: is Yes - ManagementGroup12 is allowed to create VNet as mentioned in the assignment.

upvoted 2 times

pieronegri 4 years ago

you are right, "move" is the right verb.

upvoted 2 times

dp846 1 year, 5 months ago

overrides property allows you to change the effect of a policy definition without modifying the underlying policy definition

upvoted 1 times

mlantonis Highly Voted 2 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

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 Subscription2 (ManagementGroup12).

Box 3: No

You cannot ADD Subscription1 to ManagementGroup11, but you can MOVE Subscription1 from ManagementGroup21 to ManagementGroup11. Subscriptions can only be a member of ONE ManagementGroup at a time.

upvoted 239 times

EIDakhli 1 year, 11 months ago

Perfect comment, thank you :)

upvoted 4 times

Harssh 3 years 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't member management groups inherit policies from host management group?

upvoted 1 times

Harssh 3 years 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 1 year, 12 months ago

Exactly, I do have same question. Can some help to understand

upvoted 1 times

joergsi 2 years, 11 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 Subscription2 (ManagementGroup12). But then the answer needs to be yes based on your argument, correct?

upvoted 4 times

kilowd 2 years, 6 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 2 years, 7 months 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

dp846 1 year, 5 months ago

Box 2 : No since overrides property allows you to change the effect of a policy definition without modifying the underlying policy definition

upvoted 2 times

Dankho **Most Recent** 1 month, 2 weeks ago

NYN -

1 - can't create the network

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 1 times

NickyDee 2 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 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 ManagementGroup11. Subscriptions can only be a member of ONE managementGroup at a time.

upvoted 9 times

oooMooo 3 years, 11 months ago

Thank you for this detailed response!

upvoted 2 times

Penagache 3 years, 11 months ago

Second question is for vm, not for vnet.

upvoted 8 times

Bruce_db 3 years, 10 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, 6 months ago

Good one! the verb "add" in CLI is confirmed as move.

upvoted 1 times

AubinBakana 2 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 2 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?

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 2 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 2 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 forbid 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

SeMo0o0o0o 2 months, 4 weeks ago

Wrong

NO

NO

NO

upvoted 1 times

lewisjcs300 3 months ago

Adding sub1 isn't the same as moving Sub1

upvoted 1 times

TheFivePips 4 months, 1 week ago

NYN. In general, policies 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 others have said, you cannot have a subscription in 2 management groups. It cannot be added, but it can be moved.

upvoted 1 times

TheFivePips 4 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 therefore VMs from being created. What a journey we've been on

upvoted 2 times

amurp35 5 months, 2 weeks 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 6 months 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 6 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 6 months, 3 weeks ago

Final Answer : NYN

upvoted 1 times

3c5adce 7 months ago

Going to go with NYN - will report back

upvoted 1 times

varinder82 7 months, 1 week ago

Final Answer : No No No

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #6

Topic 2

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/0e6fb866bf854f54accae2a9

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. **Most Voted**
- 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%)**Comments****Nalex9ja** Highly Voted 4 years ago

The Picked Option (B) is the correct option
upvoted 90 times

Ikrom 3 years, 12 months ago

Agree.
It says: Exclusions and RG1 is there.
upvoted 12 times

fedztedz Highly Voted 4 years ago

Answer is Correct. B
upvoted 37 times

minura Most Recent 2 weeks, 3 days agoSelected Answer: B

Answer is B
RG1 is excluded, so you can create SQL Servers
upvoted 1 times

SeMo0o0o0o 3 months, 1 week agoSelected Answer: B

B is corerct
upvoted 1 times

tashakori 9 months ago

B is right
upvoted 1 times

Amir1909 10 months ago

B is correct
upvoted 2 times

stanislaus450 10 months ago

B THIS ANSWER
upvoted 1 times

Awoyemi 1 year, 2 months agoSelected Answer: B

RG1 is excluded
upvoted 2 times

stonwall12 1 year, 6 months ago

The key is the "Exclusions" within the policy. Find that for answer.
upvoted 1 times

Firdous586 1 year, 7 months ago

B is correct
upvoted 1 times

habbey 1 year, 7 months ago

The answer is B. The exclusion negates any negatives statements in the option.

upvoted 2 times

Madbo 1 year, 8 months 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 1 year, 8 months ago

Selected Answer: B

Look at the exclusion from policy.

upvoted 1 times

myarali 1 year, 10 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 1 year, 8 months ago

lol thanks for just commenting with the exact answer given

upvoted 1 times

MarMar2022 1 year, 10 months ago

Selected Answer: B

B Correct.

upvoted 1 times

RN_ 1 year, 10 months ago

>>Exclusion<<

is the keyword !!!!

upvoted 1 times

goatbernard 2 years, 2 months ago

Selected Answer: B

so tricky

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #7

Topic 2

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

VNET1: Department: D1, and Label:Value1 only.

Tags applied to the resource group or subscription are not inherited by the resources.

Note: Azure Policy allows you to use either built-in or custom-defined policy definitions and assign them to either a specific resource group or across a whole

Azure subscription.

VNET2: Label:Value1 only.

Incorrect Answers:

RGROUP: RG6 -

Tags applied to the resource group or subscription are not inherited by the resources.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

Comments

Parmjeet Highly Voted 2 years, 6 months ago

Correct answer is:

VNET1 will only have Department: D1 tag & VNET 2 will only have Label : Value1 tag

upvoted 348 times

happpieee 1 month, 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 4 times

XristophD 2 years 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 24 times

Mucker973 2 years, 5 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

cnduknths 2 years, 1 month ago

Its not about OVERWRITTING... 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 10 times

amiban 2 years 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, 4 months ago

what is the answer? your answer seems not in the options?

upvoted 2 times

Dennis_SOn 2 years, 4 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, 4 months ago

tag. vnet1 --- Department: D1 only.

VNET1 - Department: D1 only VNET2 --- Label: Value1 only

upvoted 2 times

shashank Highly Voted 2 years, 6 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 189 times

Bernard_2nd 2 years, 6 months ago

Agree with you too.

The policy name "Apply tag and its default value" does not change previously tag of resource.

upvoted 6 times

Mucker973 2 years, 5 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, 4 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, 4 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 1 year, 7 months 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

DT95 Most Recent 1 month, 1 week ago

VNET1: "Department: D1 only"

VNET1: Department: D1 only
VNET2: "Label: Value1 only"

upvoted 2 times

kejo2 1 month, 2 weeks 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 2 times

mwhooo 1 month, 2 weeks ago

Well the mentioned policy is not even existing in azure. So we never know I guess.

upvoted 2 times

Chuong0810 2 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 1 times

ThatDowntownSmell 2 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 2 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 resources, 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

SeMo0o0o0o 2 months, 4 weeks ago

vvrong

VNET1: Department: D1 only

VNET2: Label: Value1 only

upvoted 3 times

lewisjcsc300 3 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

SeMo0o0o0o 3 months, 1 week ago

Wrong

VNET1: Department: D1 only

VNET2: Label: Value1 only

upvoted 1 times

3c5adce 7 months ago

Finally the definitive answer. Thanks for sharing.

VNET1 = Department:D1

VNET2 = Label: Value1

upvoted 6 times

Nushin 7 months, 4 weeks 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 8 months, 4 weeks ago

- Department: D1 only

- Label: Value1 only

upvoted 3 times

Pirand92 9 months, 2 weeks 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

HdiaOwner 9 months, 3 weeks ago

D1

Value1

upvoted 1 times

MNotABot 10 months ago

Instead of manually applying tags or searching for resources that aren't compliant, you create a policy that automatically applies the needed tags during deployment. Tags can also now be applied to existing resources with the new Modify effect and a remediation task.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #8

Topic 2

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 Most Voted
- D. RVAULT1 only

Correct Answer: C

Community vote distribution

C (76%)

A (24%)

Comments

mlantonis Highly Voted 2 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>

resourcegrouprecoveryservices

upvoted 167 times

klexams 2 years, 1 month ago

Yep. In saying that, there are some limitations on some resources eg. standard LB resource cannot be moved.

upvoted 15 times

OmarMac Highly Voted 2 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

Chuong0810 Most Recent 2 months ago

Selected Answer: A

All resource can move but not sure to be reused

upvoted 2 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: C

C is corerct

upvoted 1 times

divzrajshekhar123 4 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

23169fd 6 months 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 4 times

Blaze34tg 6 months ago

Selected Answer: C

C is correct. All cane be moved.

upvoted 2 times

23169fd 6 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 7 months ago

Going with C on this round

upvoted 1 times

tashakori 8 months, 4 weeks ago

C is correct

upvoted 1 times

Misty39 1 year, 3 months ago

Selected Answer: C

c is the only correct answer here

upvoted 1 times

DaisyJB 1 year, 4 months ago

Selected Answer: C

the answer is C. all can be moved to another subscription.

upvoted 1 times

marioZuo 1 year, 4 months ago

Resource Group is a logical resource. Everything under it can be moved to another group.

upvoted 1 times

Eliar2 1 year, 5 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftrecoveryservices>

Moving Recovery Services vaults for Azure Backup across Azure regions isn't supported.

In Recovery Services vaults for Azure Site Recovery, you can disable and recreate the vault in the target region.

upvoted 1 times

pinguinomaster 1 year, 5 months ago

You are wrong since the question is not about moving the store to a different region, but about moving it to a new subscription.

upvoted 1 times

sk4shi 1 year, 5 months ago

The question doesn't mention that it needs to be moved to another region

upvoted 1 times

Eliar2 1 year, 5 months ago

the correct answer is A,

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftrecoveryservices>

upvoted 2 times

Ivanvazovv 2 months, 3 weeks ago

In this link it clearly says that you CAN move to another subscription.

upvoted 1 times

dhivyamohanbabu 1 year, 5 months ago

Correct Answer: C

upvoted 1 times

Stappers 1 year, 7 months ago

Ans C: I lab'd this. All moved

upvoted 6 times



Exam AZ-104 All Actual Questions

Question #9

Topic 2

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 **Most Voted**
- D. From the Azure portal, assign the Billing administrator role to Admin1

Correct Answer: C

Community vote distribution

C (100%)

Comments

mlantonis Highly Voted 3 years, 6 months ago

Correct Answer: C

Set-AzMarketplaceTerms -Publisher <String> -Product <String> -Name <String> [-Accept] [-Terms <PSAgreementTerms>] [-DefaultProfile <IAzureContextContainer>] [-WhatIf] [-Confirm] [<CommonParameters>]

upvoted 264 times

Techfall 1 year, 9 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 42 times

umavaja 10 months, 3 weeks ago

The correct url for documentation

<https://learn.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-11.2.0>

upvoted 4 times

lingxian 3 years, 6 months ago

I found mlantonis's answers are the most credible.

upvoted 61 times

kennynelcon 2 years, 7 months ago

I will sit for one in few weeks and I am following his answers, a gem

upvoted 10 times

xclusivetp3 Highly Voted 4 years, 4 months ago

answer is correct

upvoted 26 times

lionleo Most Recent 4 days, 14 hours ago

Selected Answer: C

The answer is correct, check the following link

<https://about-azure.com/accept-legal-terms-using-powershell-to-deploy-arm-templates/>

upvoted 1 times

Darkfire 2 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-12.3.0>

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

3c5adce 7 months ago

ChatGPT 4 says C

upvoted 1 times

tashakori 8 months, 4 weeks ago

C is correct

upvoted 1 times

Tallgeese 10 months ago

Selected Answer: C

The answer is C because everyone else said so.

upvoted 2 times

oopspruu 1 year, 3 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 1 year, 8 months 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 10 months, 3 weeks ago

<https://learn.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-11.2.0>

upvoted 1 times

lokii9980 1 year, 8 months 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 1 year, 9 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 1 year, 10 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 1 year, 11 months ago

C no doubt

upvoted 1 times

coskun3firat 2 years ago

answer is correct;)

upvoted 1 times

NaoVaz 2 years, 2 months ago

C) " From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet"

Set-AzMarketplaceTerms - "Accept or reject terms for a given publisher id(Publisher), offer id(Product) and plan id(Name). Please use Get-AzMarketplaceTerms to get the agreement terms."

<https://docs.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-8.3.0>

upvoted 3 times

EmnCours 2 years, 3 months ago

Selected Answer: C

Correct Answer: C

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #10

Topic 2

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 **Most Voted**
- C. From the Groups blade, invite the user account to a new group

Correct Answer: B

Community vote distribution

B (100%)

Comments

mlantonis **Highly Voted** 3 years, 6 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 144 times

ik96 3 years, 2 months ago

B is correct.

upvoted 14 times

dan7777 **Highly Voted** 4 years, 4 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 75 times

SeMo0o0o0o **Most Recent** 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

3c5adce 7 months 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 2 times

tashakori 8 months, 4 weeks ago

B is correct

upvoted 2 times

MarMar2022 1 year, 2 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 3 times

Hades231 1 year, 3 months ago

Selected Answer: B

B is correct.

upvoted 1 times

dhivyamohanbabu 1 year, 5 months ago

Correct Answer: B

upvoted 1 times

Madbo 1 year, 8 months 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 1 year, 9 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

upvoted 2 times

Luisgar 1 year, 11 months ago

B no doubt

upvoted 1 times

daerlnaxe 2 years 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 1 year, 9 months ago

Can confirm this is now Assigned Roles.

upvoted 2 times

NaoVaz 2 years, 2 months ago

Selected Answer: B

B) "From the Directory role blade, modify the directory role"

upvoted 3 times

EmnCours 2 years, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

Lazylinux 2 years, 5 months ago

Selected Answer: B

Roles and administrators under AZ AD

upvoted 1 times

manalshowaei 2 years, 6 months ago

Selected Answer: B

B. From the Directory role blade, modify the directory role

upvoted 1 times

epomatti 2 years, 7 months ago

Selected Answer: B

Although creating a Group would scalable and easier to manage in practice, the question still focus specifically on the assignment.

B is the correct. one.

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #11

Topic 2

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 **Most Voted**
- 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 (93%)

B (7%)

Comments

mlantonis **Highly Voted** 3 years, 6 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 182 times

sreekan 3 years, 4 months ago

yes its true!!! apart from this we need to add location of User also

upvoted 15 times

zyta **Highly Voted** 4 years, 4 months ago

that's true - licences need to be assigned

upvoted 56 times

MackD **Most Recent** 4 weeks ago

Answer us in correct.

Adding, removing, and reprocessing licensing assignments is only available within the M365 Admin Center.
upvoted 2 times

Bolthen 1 month, 2 weeks ago

Deprecated. You can now assign licenses only from the M365 portal.
upvoted 4 times

hstorm 2 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 opinion "best answer" is B - The only answer that could be TRUE, guessing question is a little different in real exam, under any circumstances something has to be done for each of the users...
upvoted 1 times

OmegaGeneral 4 years, 3 months ago

You need to assign P2 license to users specifically.
upvoted 7 times

HHT 4 years, 3 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, 2 months ago

My opinion is that you shouldn't comment if you don't know the right answer.
upvoted 26 times

balfearchen 3 years, 11 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 2 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, 1 month ago

Bien explicado, muchas gracias.
upvoted 1 times

theelicht 3 months ago

As of September 1st 2024 none of the above are correct. However, the answer mlantonis gave up until now was correct.

upvoted 2 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

3c5adce 7 months 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, 1 month 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, 2 months ago

Correct A

upvoted 1 times

TamerX 1 year, 4 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, 5 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups>

upvoted 1 times

dhivyamohanbabu 1 year, 5 months ago

Correct Answer: A

upvoted 1 times

theGwyn 1 year, 5 months ago

Selected Answer: A

No doubt

upvoted 2 times

BowSec 1 year, 7 months ago

Selected Answer: A

Correct Answer: A

upvoted 3 times

Madho 1 year, 8 months ago

Mauro 1 year, 6 months ago

A. From the Licenses blade of Azure AD, assign a license.

To enable users to use all the Azure AD Premium features, you need to assign the purchased Azure AD Premium P2 licenses to 10 users in the tenant. This can be done from the Licenses blade of Azure AD. From there, you can select the 10 users to assign the licenses to and assign them the Azure AD Premium P2 licenses. This will enable them to use all the Azure AD Premium features.

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #12

Topic 2

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) Most Voted
- D. Create a notification

Correct Answer: C

Community vote distribution

C (76%)

B (18%)

A (6%)

Comments

mlantonis Highly Voted 3 years, 6 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 159 times

OmegaGeneral Highly Voted 4 years, 3 months ago

Correct, you can use the connector to bridge them together

upvoted 34 times

tita_tovenaar 3 years, 5 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 13 times

d0bermannn 2 years, 10 months ago

hi! for a&b as always ms need the simplest way to go, technically a&b may be implemented

upvoted 2 times

VictorVE [Most Recent] 2 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 4 times

kklohit 2 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 1 times

jackill 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

3c5adce 7 months 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 8 months, 4 weeks ago

C is right

upvoted 1 times

[Removed] 1 year, 5 months ago

Selected Answer: C<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-classic.overview>

upvoted 1 times

Madbo 1 year, 8 months 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 1 year, 11 months ago**Selected Answer: B**

On the 09/01/2023 exam

upvoted 3 times

alirasouli 2 years, 2 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, 2 months ago

Today in exam, is C

upvoted 1 times

NaoVaz 2 years, 2 months ago**Selected Answer: C**

C) " Deploy the IT Service Management Connector (ITSM)"

upvoted 2 times

EmnCours 2 years, 3 months ago**Selected Answer: C**

Correct Answer: C

upvoted 1 times

viveksen1 2 years, 3 months ago

C is correct - Use a connector bridge

upvoted 1 times

minhnhpq 2 years, 4 months ago

C is correct

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #13

Topic 2

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 Most Voted
- 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%)

Comments

mlantonis Highly Voted 2 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 211 times

Gde360 3 years, 4 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

magichappens 2 years, 8 months 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 3 times

muhammadazure 2 years, 6 months ago

you are true legend mlantonis

upvoted 5 times

OmegaGeneral Highly Voted 4 years, 3 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 2 months ago

Is mlantonis back or is someone playing a cruel joke?□

upvoted 2 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

A is corerct

upvoted 1 times

3c5adce 7 months 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, 5 months ago

Selected Answer: A

A

upvoted 1 times

morito 1 year, 9 months ago

This answer is a possible way, its considered best practice regarding least privilege. However please note that all Global Admins are automatically administrators on the joined devices.

upvoted 2 times

kklohit 1 year, 9 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 1 year, 9 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:

Please go to the following link:

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 1 year, 11 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 ago

A is correct

upvoted 1 times

NaoVaz 2 years, 2 months ago

Selected Answer: A

A) " Device settings from the Devices blade "

upvoted 1 times

EmnCours 2 years, 3 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

viveksen1 2 years, 3 months ago

A is correct

upvoted 1 times

libran 2 years, 3 months ago

Selected Answer: A

Device settings from the Devices blade

upvoted 1 times

Lipegj 2 years, 4 months ago

RESPOSTA A

upvoted 1 times

Lazylinux 2 years, 5 months ago

Selected Answer: A

A is correct

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #14

Topic 2

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"/>

Correct Answer:

Answer Area

**STATEMENTS****Yes****No****User1 can add Device2 to Group1**

User2 can add Device1 to Group1

User2 can add Device2 to Group2

Box 1: Yes -

User1 is a Cloud Device Administrator.

Device2 is Azure AD joined.

Group1 has the assigned to join type. User1 is the owner of Group1.

Note: Assigned groups - Manually add users or devices into a static group.

Azure AD joined or hybrid Azure AD joined devices utilize an organizational account in Azure AD

Box 2: No -

User2 is a User Administrator.

Device1 is Azure AD registered.

Group1 has the assigned join type, and the owner is User1.

Note: Azure AD registered devices utilize an account managed by the end user, this account is either a Microsoft account or another locally managed credential.

Box 3: Yes -

User2 is a User Administrator.

Device2 is Azure AD joined.

Group2 has the Dynamic Device join type, and the owner is User2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/overview>

Comments

Armina Highly Voted 2 years, 6 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 272 times

go4adil 10 months, 3 weeks 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 7 times

Durden871 1 year, 9 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 1 month, 3 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, 2 months ago

User administrator role has the permission to update group membership, but only users, not devices.

upvoted 1 times

chair123 1 year, 2 months ago

it says Group 1 & 2 owner is User 12?.

upvoted 2 times

klasbeatz 2 years, 5 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 1 times

klasbeatz 2 years, 3 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, 3 months ago

Confusing you would think a cloud device admin could....Just reviewing this question again during my studies.

upvoted 2 times

klexams 2 years, 6 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, 6 months ago

Take a second look. User1 does not own any of the Groups. Answer is No.

upvoted 21 times

[Removed] 11 months ago

[REMOVED] 11 months ago

But the answer says that User1 is Owner of Group1. So the question is wrong.

upvoted 1 times

jeru81 10 months ago

How can be a question wrong? User2 is clearly Owner of both Groups. ANSWER is wrong.

upvoted 4 times

FabryDev 11 months, 2 weeks ago

Read the details carefully please before answering, you are causing confusion. User2 is the owner of both groups.

upvoted 7 times

Lazylinux Highly Voted 2 years, 5 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 121 times

Hrydar 2 years, 3 months ago

the best and straight forward explanation lazylinux. good job

upvoted 2 times

micro9000 1 year, 11 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 1 year, 9 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, 1 month ago

User Admin CANNOT ADD devices.

upvoted 5 times

Asfajaf 2 years, 1 month ago

User2 is owner of Group2, User2 can add/remove members regardless of role

upvoted 6 times

darthfodio 1 year, 11 months ago

Group2 is dynamic, therefore no one, including the owner, can manually add an object.

upvoted 4 times

MeysamBayani 1 year, 10 months ago

but he/she can add new role for add devices. in question mention user2 can ...

upvoted 1 times

Durden871 1 year, 9 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, "Y/N". The way the question is loaded makes it "N/Y".

upvoted 1 times

GreenTick Most Recent 1 month 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 1 month, 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 1 month, 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-a>

upvoted 1 times

mwhooo 1 month, 2 weeks ago

No one can add any device to group2 because its a dynamic group, Static members cant be added.

upvoted 1 times

Mshaty 2 months, 2 weeks 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 1 times

cloudy_man 2 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

NavigatiOn 2 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.

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 2 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

SeMo0o0o0o 2 months, 4 weeks ago

Wrong

No

Yes

No

Owner = User2

User2 + Azure AD registered + Assigned

upvoted 1 times

lethuccrma 3 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 1 times

DJHASH786 4 months, 2 weeks ago

NYN

Generally registered devices would be users personal devices, mobile phones or laptops etc.. they log into the device with their personal credentials.

An Entra ID joined device is connected to your organization, and users can log into the devices with their work account.

upvoted 1 times

76d5e04 6 months ago

Conflicting with the question.

In question User2 is the owner of Group1 & 2 but in the answer section it is mentioned "Group1 has the assigned join type, and the owner is User1."

Examtopics in-charge please fix the contents as we rely on the details mentioned here

upvoted 1 times

varinder82 6 months, 3 weeks ago

Final Answer : N Y N

upvoted 1 times

3c5adce 7 months ago

Going to go with NYN

upvoted 1 times

3c5adce 7 months ago

Retracting and going with this one instead:

NNY

User1 can add Device2 to Group1: No

User2 can add Device1 to Group1: No

User2 can add Device2 to Group2: Yes

upvoted 1 times

varinder82 7 months, 1 week ago

Final Answer : No Yes No

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #15

Topic 2

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
SQLDB01	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 Most Voted
- D. Delete sa001

Correct Answer: C

Community vote distribution

C (100%)

Comments

NaoVaz Highly Voted 2 years, 2 months ago

Selected Answer: C

C) "Stop the backup of SQLDB01"

VMs 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 10 times

BenStokes Highly Voted 3 years, 5 months ago

Answer is correct - C

upvoted 9 times

villanz 3 years, 5 months ago

Yes correct - c

upvoted 1 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: C

C is corerct

upvoted 1 times

leoiq91 7 months, 1 week ago

Stop the Backup of SQL =CORRECT!

upvoted 2 times

Shif 7 months, 2 weeks ago

Ans is C.

upvoted 1 times

tashakori 8 months, 3 weeks ago

C is right

upvoted 1 times

Wojer 10 months, 4 weeks 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 6 times

Mehedi007 1 year, 4 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, 5 months ago

Selected Answer: C

It should be C

upvoted 1 times

bcristella 1 year, 8 months 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

zelleck 1 year, 10 months ago

Selected Answer: C

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, 2 months ago

Today in exam, is C

upvoted 2 times

EmnCours 2 years, 3 months ago

Selected Answer: C

Correct Answer: C

upvoted 2 times

Azure_daemon 2 years, 8 months ago

Tested in lab and C is the correct answer

upvoted 3 times

Moezey 2 years, 9 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 2 years, 9 months ago

Answer is C

upvoted 1 times

Az_dasappan 2 years, 10 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



Exam AZ-104 All Actual Questions

Question #16

Topic 2

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. **Most Voted**
- 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%)

Comments

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

agree, its B

upvoted 13 times

Madbo **Highly Voted** 1 year, 8 months 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 9 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

mtc9 1 year, 2 months ago

Any variation of Contributor role does not allow to grant roles to other users. Contributor can be understood as resource read/write permission. To assign roles to other users you need some variation of Owner to resource 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, 3 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, 4 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, 5 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 1 year, 8 months ago

Right answer is B.

Contributor = Can't grant access to others

User Access Administrator = Manage user access to Azure resources

upvoted 2 times

GoldBear 1 year, 8 months 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 1 year, 9 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 1 year, 9 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 1 year, 9 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

zelleck 1 year, 10 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

Aliciuza 2 years ago

Selected Answer: B

Access administrator

upvoted 1 times

Thanesh 2 years, 2 months ago

User administrator role

upvoted 2 times

SubbuWorld 2 years, 2 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, 2 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, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 2 times

EleChie 2 years, 3 months ago

OR

Assign User1 the Owner role for VNet1

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #17

Topic 2

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 **Most Voted**

B. NSEC

C. PTR

D. RRSIG

Correct Answer: A

Community vote distribution

A (100%)

Comments

ms70743 **Highly Voted** 3 years, 11 months ago

TXT and MX are valid answers.

upvoted 102 times

sidharthwader **Highly Voted** 3 years, 7 months 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 83 times

e_karma 3 years ago

I didn't know mx was there usually it is txt record ..thanks for this

upvoted 7 times

sairaj9396 2 years, 7 months ago

same here. i thought mx is explicitly for mail exchange
upvoted 7 times

Howard20717 7 months, 3 weeks ago

yea, me too. Never use MX record for this purpose
upvoted 1 times

Amrinder101 2 years 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 8 times

jackill 1 year, 5 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 2 times

JayBee65 3 years, 6 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 16 times

Lamini 3 years, 1 month 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

Mark74 Most Recent 5 days, 14 hours ago

Selected Answer: A

Mx record for me is correct

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

A is corerct

upvoted 1 times

Amir1909 10 months ago

A is correct

upvoted 1 times

DWILK 1 year, 1 month ago

Why would a Mail Exchange record have to be created? Mail isn't mentioned in the question. This has to be wrong
upvoted 2 times

nmmn22 1 year, 2 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, 3 months ago

Selected Answer: A

upvoted 2 times

itguyeu 1 year, 5 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, 5 months ago

Selected Answer: A

Of the available options this is MX (A)

upvoted 1 times

Madbo 1 year, 8 months 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 2 times

kklohit 1 year, 9 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, 2 months ago

Selected Answer: A

A) "MX".

Both "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, 3 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

libran 2 years, 3 months ago

Selected Answer: A

MX is the Answer

upvoted 1 times

Lazylinux 2 years, 5 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

Sillyon 2 years, 6 months ago

Selected Answer: A

Correct answer is A.

--> MX or TXT is valid.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #18

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (100%)

Comments

mlantonis **Highly Voted** 2 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 82 times

Lilyli 3 years, 5 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 2 years, 8 months 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, 1 month ago

Clearly No, Azure DevTest Labs is a service that has nothing to do with Logic App

upvoted 22 times

chaudha4 3 years, 6 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 9 times

minura Most Recent 2 months, 1 week ago

Correct Answer: B

<https://learn.microsoft.com/en-us/azure/devtest-labs/devtest-lab-add-devtest-user>

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: B

B is correct

On Dev, you assign the Contributor role to the Developers group.

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corerct

upvoted 1 times

3c5adce 7 months 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 9 months ago

No is right

upvoted 1 times

Madbo 1 year, 8 months 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

zelliCK 1 year, 10 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, 2 months ago

Today in exam is B

upvoted 1 times

NaoVaz 2 years, 2 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, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

cryptostud 2 years, 3 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, 3 months ago

Selected Answer: B

B NO is the Answer

upvoted 1 times

Dannxx 2 years, 3 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, 5 months ago

Agreed B is answer

upvoted 2 times

Sillyon 2 years, 6 months ago

Selected Answer: B

Correct Answer: B (No)

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #19

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (100%)

Comments

mlantonis **Highly Voted** 3 years, 6 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-secluding-a-logic-app>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-operator>
upvoted 85 times

OmarMac Highly Voted 4 years ago

Logic App Operator Role - Lets you read, enable, and disable logic apps, but not edit or update them.
upvoted 35 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

tashakori 9 months ago

No is right
upvoted 1 times

Mehedi007 1 year, 4 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 2 times

Madbo 1 year, 8 months 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 1 year, 8 months ago

The answer is B even the Dev users group should have Access only for RSG not to entire subscription.

upvoted 1 times

zellck 1 year, 10 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, 2 months ago

Today in exam is B

upvoted 2 times

NaoVaz 2 years, 2 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, 3 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

Dannxx 2 years, 3 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, 5 months ago

Agreed B is the correct answer
upvoted 1 times

Sillyon 2 years, 6 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

manalshowaei 2 years, 6 months ago

Selected Answer: B

Answer: B. No
upvoted 1 times

Marusyk 2 years, 7 months ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

Azure_daemon 2 years, 9 months ago

To create Logic App you need the Contributor role not operator, so the correct answer is B
upvoted 1 times



Exam AZ-104 All Actual Questions

Question #20

Topic 2

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

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

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 **Most Voted**

B. No

Correct Answer: A

Community vote distribution

A (100%)

Comments

mlantonis **Highly Voted** 3 years, 6 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 70 times

fedztedz **Highly Voted** 4 years ago

Answer is Correct. YES (A)

Contributor role can create logic apps

upvoted 43 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: A

A is correct
upvoted 1 times

Madbo 1 year, 8 months 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 1 year, 9 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

zellick 1 year, 10 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 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, 2 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, 3 months ago

Selected Answer: A

Correct Answer: A
upvoted 1 times

Dannxx 2 years, 3 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, 5 months ago

A is correct
upvoted 1 times

Sillyon 2 years, 6 months ago

Selected Answer: A

Correct answer is A.
upvoted 1 times

manalshowaei 2 years, 6 months ago

Selected Answer: A

A. Yes is correct
upvoted 1 times

Marusyk 2 years, 7 months ago

Selected Answer: A

Answer is Correct. YES (A)
upvoted 1 times

Azure_daemon 2 years, 9 months ago

Obviously A is the correct answer
upvoted 1 times

Prano 2 years, 12 months ago

Ans : A
Contributor can create logic apps
upvoted 1 times

mse89 2 years, 12 months ago

answer is correct, the role contributor is applied to the resource group
upvoted 1 times



Exam AZ-104 All Actual Questions

Question #21

Topic 2

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.
Assign a tag to each resource.	From the Cost analysis blade, filter the view by tag.
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:



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>

Comments

mlantonis Highly Voted 3 years, 6 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 255 times

Takloy 3 years, 1 month ago

Yup! also tested it.

upvoted 13 times

Jey117 2 years, 5 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, 3 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 20 times

allyQ 1 year, 9 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, 6 months ago

thank you mlantonis

upvoted 3 times

moekyisin Highly Voted 4 years ago

Ans is correct

upvoted 18 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

correct

upvoted 1 times

rocky48 1 year, 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 3 times

testoneAZ 1 year, 11 months ago

Answer is correct

upvoted 1 times

Yugang 1 year, 12 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 ago

correct as defined in the result box

upvoted 1 times

mahtab 2 years, 1 month ago

Correct

upvoted 1 times

NaoVaz 2 years, 2 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, 3 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, 5 months ago

Given answer is correct

upvoted 2 times

manalshowaei 2 years, 6 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 2 years, 9 months ago

vwas 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 2 years, 11 months ago

Correct Answer
upvoted 1 times

Sara_Mo 3 years ago

Correct Answer
upvoted 1 times

flash007 3 years, 4 months ago

You tag individual resources not groups
upvoted 3 times

klasbeatz 2 years, 5 months ago

No you tag resource group and resources inherit the tag. You can also tag individual resources
upvoted 1 times

ScreamingHand 3 years, 6 months ago

Confirmed in lab - answer is correct
upvoted 2 times



Exam AZ-104 All Actual Questions

Question #22

Topic 2

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" **Most Voted**
- C. select * from Event where EventType == "error"
- D. search in (Event) * | where EventType -eq "error"

Correct Answer: B

Community vote distribution

B (92%)

D (8%)

Comments

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

Correct B

Tested in lab Home>>Monitor>>Logs

All command queries return syntax error except Search in (Event) "error"

upvoted 45 times

djhyfdgjk 9 months, 4 weeks ago

Just testet in actual Azure LAW. "B" returns syntax error.

upvoted 1 times

NaoVaz **Highly Voted** 2 years, 2 months ago

Selected Answer: B

B) 'search in (Event) "error"'

Seems to be the correct option. Tested in lab.

upvoted 7 times

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

Selected Answer: B

<https://learn.microsoft.com/en-us/kusto/query/search-operator?view=microsoft-fabric#search-a-specific-table>
upvoted 1 times

Sifon_n 1 month, 2 weeks ago

Selected Answer: B

Definitely B
upvoted 1 times

happpieee 1 month, 2 weeks ago

Selected Answer: B

B, with correct KQL syntax.
upvoted 1 times

mcc 2 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 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corerct
upvoted 1 times

Neel2211 3 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 9 months ago

Event | where EventLevelName == "Error"

upvoted 2 times

ricardona 1 year, 1 month 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, 4 months ago

Selected Answer: B

Tested in lab.

upvoted 1 times

Andreas_Czech 1 year, 6 months ago

Selected Answer: B

like GepeNova

Correct is B

Tested in LAB

upvoted 2 times

Mysystemad 1 year, 7 months ago

B correct

upvoted 1 times

Exilic 1 year, 7 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, 2 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, 6 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, 6 months ago

Lab tests show B is the correct option. This should override whatever OpenAI answered.

upvoted 3 times

hz78 1 year, 8 months 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, 4 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

Madbo 1 year, 8 months ago

Option B is not a valid query language syntax for Azure Log Analytics. Option D is the correct answer, which uses the search operator to search the Event table and filter the results by EventType equal to "error". Thank you for bringing this to my attention and please let me know if you have any further questions.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #23

Topic 2

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_B2s"
    },
    "osProfile": {
      "computerName": "VM2",
      "adminUsername": "AzureAdmin",
      "adminPassword": "[parameters('adminPassword')]"
    },
    "storageProfile": {
      "imageReference": "[variables('image')]",
      "osDisk": {
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"
        }
      ]
    }
  }
}

```

```
  "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>

Comments

pakman Highly Voted 3 years, 2 months ago

YES
YES
NO

upvoted 109 times

rigonet 3 years, 2 months ago

How do you know VM2-NI is connected to VNET1?

upvoted 47 times

alsmk2 3 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 4 times

alex_p 3 years, 2 months ago

the question actually is - "VM1 and VM2 can connect VNET1 ? - Yes, they can because both are in the same region where VNET1 is.

upvoted 48 times

Philly_cheese_steak 3 years, 1 month ago

NO YES NO

There is no mention of VM2NI connected to VNET1??

upvoted 43 times

alsmk2 4 months ago

Surely it is implied by the fact it says the two VMs are deployed? You can't deploy a VM without an underlying vNET, and the only vnet mentioned is VNET1. The template makes no reference to either, so the clear assumption to be made is that they are both connecting to the only available vNET.

upvoted 1 times

Hyrydar 2 years, 3 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 7 times

klexams 2 years, 1 month ago

Nic to vm but all within a vnet

upvoted 1 times

ZooZoo72 2 years, 2 months ago

Yes but you also connected those cards to a network...hopefully.

upvoted 7 times

xRiot007 1 year, 6 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, 5 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 7 times

76d5e04 6 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 10 months, 1 week 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, 2 months ago

No because VM2NI is not connected to VNET1

Yes

No

upvoted 68 times

a4andrew 3 years, 1 month 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 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 2 years, 9 months 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, 6 months ago

VM2NI does not even exist.

upvoted 2 times

binhdortmund 9 months, 3 weeks ago

ARM was successfully deployed => VM2-NI exists and connected to VNET cause u cant create VM2-NI without VNet

upvoted 3 times

junkz Most Recent 1 month 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 2 times

Stunomatic 1 month, 3 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 vnet1000000000000000. haha NYN

upvoted 1 times

EmnCours 2 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 2 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 2 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

SeMo0o0o0o 3 months, 1 week ago

correct

upvoted 1 times

CheMetto 4 months, 2 weeks 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()]]"  
},
```

Altough 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 7 months ago

Final Answer: Y Y N

upvoted 2 times

af68218 8 months, 1 week 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 9 months, 3 weeks ago

Correct

upvoted 1 times

dhiii 10 months, 1 week 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 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 they are in different data centers a.k.a zones
3. NO - Both VMs are in same Region

upvoted 2 times

SgtDumitru 1 year 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 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, 2 months ago

YES, YES, NO

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

upvoted 1 times

Babustest 1 year, 2 months ago

Nowhere it's mentioning VM2-NI is in VNET1.

upvoted 2 times

Chris76 1 year, 3 months ago

N - "Can connect" vs "Can Be connected" two different things. Only VM1 "Can Connect to VNET1" Because it says it "VM1-NI" is connected to "VNET 1"

Y - Because of zone: 1, zone:2

N - Both zones are in EastUS2

upvoted 8 times

MissCisco 6 months ago

if one can be on when one zone failure its mean vm1 and vm2 are in# zone

Zone = Each zone consists of one or more data centers equipped with independent power, cooling, and networking
then vm1 and Vm2 are ob different Vnet

the answer are No Yes No

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #24

Topic 2

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. **Most Voted**
- 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%)

Other (14%)

Comments

mlantonis Highly Voted 3 years, 6 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 127 times

Veks 2 years, 7 months 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

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 18 times

klexams 2 years, 6 months ago

@veks, so you're saying A is wrong then?!

upvoted 2 times

Ajinkyakore 2 years, 6 months ago

So technically there will be no any migration or transfer happens?

upvoted 2 times

bryant12138 1 year, 1 month ago

yeah I think you're right, both rg and subscription are ideological management tools

upvoted 1 times

klasbeatz 2 years, 5 months ago

Your right.....New-AzAppServicePlan -Location "North Central US" -ResourceGroupName DestinationAzureResourceGroup -Name DestinationAppServicePlan -Tier Standard

upvoted 1 times

klasbeatz 2 years, 5 months ago

But the question suggest that it is being moved...not "cloned"

upvoted 4 times

mcclane654 10 months, 3 weeks ago

just to add to this. as I found the policy confusing. if they are talking about Azure policy:

An evalution 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 ago

A is correct

upvoted 43 times

kejo2 Most Recent 2 months, 1 week ago

Tested in my Lab. A is correct

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

A is corerct

upvoted 1 times

TheFivePips 4 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 1 times

robsoneuclides 6 months, 2 weeks ago

Esta correta

unvoted 1 times

upvoted 1 times

camwilson04 8 months, 1 week 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 9 months 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 2 times

93d821b 1 year ago

https://www.youtube.com/watch?v=QBAOI2dZS_c

Answer is B

upvoted 2 times

2d153f5 3 weeks, 3 days ago

Noooooooooo. In the video, the answers are changed positions.

upvoted 2 times

Andmachado 6 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

c1g003 1 year 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

c1g003 1 year, 2 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 3 times

mtc9 1 year, 2 months ago

Resouce 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, 4 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, 4 months ago

you cannot change an App Service plan's region.

upvoted 2 times

Rogit 1 year, 4 months ago

Selected Answer: A

Came in test yesterday

upvoted 3 times

Az_Amit 1 year, 5 months ago

Selected Answer: A

Answer A is correct. Verified and found that we can only change(Move) the RG2 of WebApp1. All other associated resources will be in same reason and same RG1. The activity is independent of app service plan. Even after moving the WebApp1 to RG2 the WebApp1 location will be West Europe only.

upvoted 4 times

Abiram 1 year, 7 months ago

I tried this in a lab today, and the answer is C.

The Policy 1 was carried along when I moved the web app from RG1 to RG2.

I kept a simple policy to append tag and its default (policy1: name: RGroup ; value RG1; policy2: RGroup RG2). and the same tag remained as is when the web app was moved RG2

upvoted 2 times

lulzsec2019 1 year, 6 months ago

please don't give wrong answer.

upvoted 3 times

klexams 2 years, 1 month ago

Selected Answer: A

It never says it moves region. It just moves RG. There are some limitations in moving some resources. In case of webapps, it shouldn't have any issue.

upvoted 6 times



Exam AZ-104 All Actual Questions

Question #25

Topic 2

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": [

 "**"

],

 "additionalProperties": {},

 "dataActions": [],

 "notActions": [

"Microsoft.Authorization/**"
"Microsoft.Resources/**"
"Microsoft.Security/**"

}

Correct Answer:

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": []  
        }  
    ]  
],
```

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles> <https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources>

Comments

mlantonis Highly Voted 3 years, 6 months ago

Correct Answer:

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"
"Microsoft.Authorization/"

upvoted 342 times

Awot 1 year, 2 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 6 times

Slimus 1 year, 6 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 ago

So often I have the feeling; This HAS to be wrong. And finding the community confirming my thoughts is nice :)

upvoted 14 times

Mitazure7 1 year, 2 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

fedzedz Highly Voted 3 years, 12 months ago

The Answer is Wrong.

First part should be "/Subscription/subscription_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 "/subscription/subscription_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 240 times

JayBee65 3 years, 6 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, 6 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 3 years, 8 months 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, 4 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 that 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 2 years, 10 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 if you use "/subscription/subscription_id/resourceGroups/resource_group_name" then you need the resource_group_name

upvoted 1 times

rikininetysix Most Recent 2 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 1 times

SeMo0o0o0o 2 months, 4 weeks ago

WRONG

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"

"Microsoft.Authorization/*"

upvoted 1 times

Amir1909 9 months, 4 weeks ago

Correct Answer: "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"

"Microsoft.Authorization/"

upvoted 2 times

Mitazure7 1 year, 2 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, 2 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#assignablescopes>

upvoted 1 times

Josete1106 1 year, 4 months ago

Correct Answer:

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"

"Microsoft.Authorization/"

upvoted 3 times

Aluksy 1 year, 8 months ago

Correct Answer :

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"

"Microsoft.Authorization/"

Came out in my exam today 8th April 2023. Passed 830.

upvoted 10 times

rocky48 1 year, 8 months ago

Correct Answer:

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"

"Microsoft.Authorization/"

upvoted 4 times

orionduo 1 year, 10 months ago

It should be "/Subscription/subscription_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/subscription_id/resourceGroups/resource_group_name"

"Microsoft.Authorization/" is right

upvoted 2 times

CoachV 1 year, 10 months ago

<https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>

upvoted 1 times

CoachV 1 year, 10 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, 5 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 1 year, 10 months ago

Dang the provided answer was /subscription/sub_id/resourceGroups. What you posted here is not the same thing.

upvoted 2 times

geisonferreira 1 year, 10 months ago

Why are wrong answers not corrected? This site is sometimes more confused than helpful.

upvoted 11 times

NaoVaz 2 years, 2 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, 4 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/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx/resourceGroups/RG1

upvoted 7 times

Lazylinux 2 years, 5 months ago

Given Answer is Wrong.. as RG name need be specified and even then applies to one particular RG but questions ask for all RGs and subsc can have multiple RGs and hence should be applied at Subsc level as per below

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"

"Microsoft.Authorization/"

upvoted 5 times



Exam AZ-104 All Actual Questions

Question #26

Topic 2

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 **Most Voted**
- B. a public load balancer
- C. an Azure Content Delivery Network (CDN)
- D. Traffic Manager
- E. an Azure Application Gateway **Most Voted**

Correct Answer: AE

Community vote distribution

AE (92%)

AB (8%)

Comments

mlantonis **Highly Voted** 3 years, 6 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 532 times

Veks 2 years, 7 months 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 4 times

ShaulS 3 years, 1 month ago

A: what do you mean by "internal LB is enough"?

upvoted 2 times

e_karma 3 years ago

It means that nobody is accessing the resources through public ip ..So no need of a public load balancer.

upvoted 26 times

juniорccs 3 years, 4 months ago

Very nice and complete explanation, thanks a lot!

upvoted 3 times

Sh4kE 2 years, 10 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, 6 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, 6 months ago

there is a reason why people use VPN.

upvoted 1 times

zr79 2 years, 9 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 ago

i would say A and E is the correct answer.

upvoted 88 times

CloudEngJS Most Recent 1 week, 2 days 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 4 days, 9 hours ago

NB! You have a line-of-business-app named App1 that runs on several Azure virtual machine.

upvoted 1 times

CloudEngJS 4 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 1 month, 2 weeks ago

Selected Answer: AE

Wouldn't pick the public one so....

upvoted 1 times

GuessWhoops 2 months, 1 week 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 can't decide here between AAG/PLB.

upvoted 1 times

lokii9980 2 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 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: AE

A & E are correct

upvoted 1 times

SefOne 1 year, 2 months ago

Selected Answer: AE

No doubt about it AE

upvoted 1 times

itguyeu 1 year, 5 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 is A, E.

upvoted 1 times

upvoted 2 times

Mazinger 1 year, 9 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 1 year, 11 months ago

Correct Answer: A and E

Given that the application is a webapp.

upvoted 1 times

Uniteck 2 years ago

A & E is the correct answer

upvoted 1 times

alirasouli 2 years, 1 month ago

Selected Answer: AE

Quote from Microsoft's documentation:

Azure provides a suite of fully managed load-balancing solutions for your scenarios:

- * If you are looking to do DNS based global routing and do not have requirements for Transport Layer Security (TLS) protocol termination ("SSL offload"), per-HTTP/HTTPS request or application-layer processing, review Traffic Manager.
- * If you want to load balance between your servers in a region at the application layer, review Application Gateway.
- * If you need to optimize global routing of your web traffic and optimize top-tier end-user performance and reliability through quick global failover, see Front Door.

upvoted 2 times

majerly 2 years, 2 months ago

Today in exam AE

upvoted 5 times

NaoVaz 2 years, 2 months ago

Selected Answer: AE

A) "an internal load balancer" & E) "an Azure Application Gateway"

No Public LB is required since the connections are established through VPN.

CDN and Traffic Manager aren't used for LoadBalancing.

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #27

Topic 2

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 **Most Voted**
- C. Metrics
- D. Customer insights

Correct Answer: B

Community vote distribution

B (100%)

Comments

waterzhong **Highly Voted** 3 years, 10 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 112 times

mlantonis **Highly Voted** 3 years, 6 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 102 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

Amir1909 9 months, 3 weeks ago

Correct

upvoted 1 times

Mehedi007 1 year, 4 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

NavigatiOn 1 year, 4 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 1 year, 8 months 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 1 year, 9 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

NanVaz 2 years, 2 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, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

eporr 2 years, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

RichardBill 2 years, 3 months ago

Selected Answer: B

Its the Advisor

upvoted 1 times

Lazylinux 2 years, 5 months ago

Selected Answer: B

I luv Honey because it is B

upvoted 3 times

manalshowaei 2 years, 6 months ago

Selected Answer: B

B. Advisor

upvoted 1 times

Racinely 2 years, 6 months ago

Azure Advisor

upvoted 1 times

Azure_daemon 2 years, 9 months ago

Advisor is the correct answer

upvoted 1 times

Fusionaddware 2 years, 9 months ago

Selected Answer: B

Advisor is correct

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #28

Topic 2

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>

Comments

fedztedz 3 years, 12 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 301 times

Bigbluee 1 year, 9 months 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 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, 7 months ago

Thanks for the great description. Very helpful.

upvoted 16 times

Shadoken 2 years, 5 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, 6 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 146 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

correct

upvoted 1 times

rocky48 1 year, 8 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 2 times

CoachV 1 year, 10 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 7 times

AndreLima 1 year, 11 months ago

Respostas bem confusas.

upvoted 1 times

NaoVaz 2 years, 2 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, 3 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, 5 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, 3 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, 6 months ago

Answer is correct

upvoted 1 times

Jvp21 2 years, 10 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_ 2 years, 10 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_ 2 years, 10 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 2 years, 10 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, 6 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, 5 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, 3 months ago

The answer is correct?

upvoted 3 times

omw2wealth 3 years, 2 months ago

Yes it is correct
upvoted 1 times

mkoprivnj 3 years, 6 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

saddamakhtar 3 years, 7 months ago

Answer is correct
upvoted 1 times

mg 3 years, 9 months ago

Answer is correct
upvoted 1 times

ZUMY 3 years, 9 months ago

Given answer is correct

1.user or groups

2.apps

3.grant or deny

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #29

Topic 2

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. **Most Voted**
- 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%)

Comments

moekyisin **Highly Voted** 4 years ago

correct answer checked in portal .
Go to Azure AD--users--user settings --scroll down.--External users
Manage external collaboration settings
upvoted 181 times

Acai 3 years, 4 months ago

Yep Yep Yep
upvoted 15 times

Gor12 3 years, 2 months ago

Your excitement is awesome!
upvoted 27 times

Mentalfloss 4 months, 3 weeks ago

Your excitement about Acaí's excitement is awesome! \m/
upvoted 4 times

fedztedz Highly Voted 3 years, 12 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 76 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

tashakori 8 months, 4 weeks ago

D is right

upvoted 1 times

Amir1909 10 months ago

- From the Users blade, modify the External collaboration settings

A is correct

upvoted 1 times

azahar08 11 months, 2 weeks ago

yes lo mismo pienso yo

upvoted 1 times

NavigatiOn 1 year, 4 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 1 year, 8 months 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 1 year, 8 months ago

A is correct

upvoted 1 times

Mazinger 1 year, 9 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, 2 months ago

Selected Answer: A

A) "From the Users settings blade, modify the External collaboration settings."

upvoted 3 times

EmnCours 2 years, 3 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

libran 2 years, 3 months ago

Selected Answer: A

A is the right answer

upvoted 1 times

manalshowaei 2 years, 6 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

epomatti 2 years, 7 months ago

Selected Answer: A

A is correct. External collaboration settings, there's where you configured the Guest permissions.

upvoted 1 times

Eitant 2 years, 7 months ago

Selected Answer: A

This is the answer

upvoted 1 times

Azure_daemon 2 years, 9 months ago

Guest invite settings

Guest invite restrictions

Learn more

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

Only users assigned to specific admin roles can invite guest users

No one in the organization can invite guest users including admins (most restrictive)

upvoted 5 times



Exam AZ-104 All Actual Questions

Question #30

Topic 2

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. **Most Voted**
- D. Create a new management group and delegate User1 as the owner of the new management group.

Correct Answer: C

Community vote distribution

C (86%)

Other (14%)

Comments

mlantonis Highly Voted 3 years, 6 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 314 times

JoeGuan 1 year, 2 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 11 times

Alscoran 1 year ago

It cannot be A or B simply because subscriptions are underneath Management groups. So doing anything 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 10 times

Techo1980 6 months, 3 weeks ago

@Alscoran, you say B is close or you mean C is close?

upvoted 2 times

SunitaMaurya 5 months, 1 week ago

Does anyone have contributor access then please help me.

upvoted 1 times

itgg11 2 years, 12 months ago

Answer is C. Just tested in the lab.

upvoted 24 times

mumu_myk 3 years 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 would've 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 9 times

Rajash Highly Voted 3 years, 7 months 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 63 times

brainmind 3 years, 5 months ago

The answer is C, the user should be a GA and then elevate themselves to gain access.

upvoted 3 times

Negrinho 3 years, 7 months ago

No, the correct 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, 6 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, 6 months ago

B can't be right because the owner access is given at subscription level only.

upvoted 5 times

mdyck 3 years, 6 months ago

This is right. Check the chart in this link. Owners assign policy.

upvoted 5 times

rawkadia 3 years, 5 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

happpieee Most Recent 1 month, 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 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: C

it's C

upvoted 1 times

amurp35 5 months, 2 weeks 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 7 months ago

ChatGPT4 says C

upvoted 3 times

3c5adce 7 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 7 months, 4 weeks 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 8 months, 2 weeks 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 8 months, 4 weeks ago

C is right

upvoted 2 times

Cg007 9 months 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 9 months, 3 weeks 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 9 months, 4 weeks ago

Correct Answer: C

reasoning: because

upvoted 2 times

stanislaus450 10 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 resources 12.

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 role 12. Once User1 has the Owner role, they can configure access management for Azure resources, including assigning policies to the tenant root management group 12.

upvoted 1 times

HdiaOwner 10 months, 1 week ago

Selected Answer: C

Answer should be C

upvoted 2 times

BluAlien 10 months, 4 weeks ago

Doc says:

The Microsoft official documentation (<https://learn.microsoft.com/en-us/azure/governance/management-groups/overview#root-management-group-for-each-directory>) says that:

"The Azure AD Global Administrator needs to elevate themselves to the User Access Administrator role of this root group initially. " So I would go for C but I tried in lab it doesn't work because Global Administrator can elevate himself to User Access Administrator but the scope of these roles isn't on, or inherited to Tenant Root Management Group so the user1 can't access the overview page of Tenant Root Management Group neither the Access Control (IAM) blade and in this way it's impossible to him to assign any policy.

The only two possible ways are:

- 1) Grant User Access Administrator and Resource Policy Contributor to User1 on Tenant Root Management Group
- 2) Assign Owner role to User1 on Tenant Root Management Group

Only after one of these, User1 is able to apply policy to the Tenant Root Management Group.

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #31

Topic 2

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	<i>Not applicable</i>

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:	<table border="1"><tr><td>Group1 only</td></tr><tr><td>Group2 only</td></tr><tr><td>Group3 only</td></tr><tr><td>Group1 and Group2 only</td></tr><tr><td>Group1 and Group3 only</td></tr><tr><td>Group2 and Group3 only</td></tr><tr><td>Group1, Group2, and Group3</td></tr></table>	Group1 only	Group2 only	Group3 only	Group1 and Group2 only	Group1 and Group3 only	Group2 and Group3 only	Group1, Group2, and Group3
Group1 only								
Group2 only								
Group3 only								
Group1 and Group2 only								
Group1 and Group3 only								
Group2 and Group3 only								
Group1, Group2, and Group3								

User2:	<table border="1"><tr><td>Group1 only</td></tr><tr><td>Group2 only</td></tr><tr><td>Group3 only</td></tr><tr><td>Group1 and Group2 only</td></tr><tr><td>Group1 and Group3 only</td></tr><tr><td>Group2 and Group3 only</td></tr><tr><td>Group1, Group2, and Group3</td></tr></table>	Group1 only	Group2 only	Group3 only	Group1 and Group2 only	Group1 and Group3 only	Group2 and Group3 only	Group1, Group2, and Group3
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>

Comments

pakman Highly Voted 3 years, 2 months ago

Correct answer.

User 1: Group 1 only

User 2: Group 1 & 2

upvoted 143 times

SofiaLorean 6 months, 3 weeks ago

please help to explain why user 1 not be in group 3? Thanks.

upvoted 3 times

DevOpposite 3 years, 2 months ago

why cant user 1 not be in grp 3 plz?

upvoted 12 times

nsknexus478 3 years, 2 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 64 times

DevOpposite 3 years, 2 months ago

thank you

upvoted 2 times

Mozbius_ 2 years, 10 months ago

Thank you for the clarification.

upvoted 1 times

upvoted 1 times

Chi1987 3 years, 2 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, 2 months ago

license has nothing to do with it.
upvoted 25 times

sk1803 3 years, 2 months ago

<https://www.examtopics.com/discussions/microsoft/view/20714-exam-az-103-topic-3-question-11-discussion/>
upvoted 4 times

BeastOfCloud 1 year, 9 months ago

Correct aim we only focus on Membership not o365 license cause you just limit them.
upvoted 4 times

GepeNova Highly Voted 3 years, 2 months ago

Tested in lab.
User 1: Group 1 only
User 2: Group 1 & 2
upvoted 51 times

JPA210 Most Recent 1 month 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

learn254 2 months, 1 week 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 3 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

SeMo0o0o0o 3 months, 1 week 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 1 times

upvoted 1 times

Bobip 3 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 4 months 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 7 months, 2 weeks 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 4 times

LovelyGroovey 7 months, 3 weeks 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 7 months, 3 weeks 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 6 months, 1 week ago

Was wondering this, thank you!

upvoted 1 times

tashakori 8 months, 3 weeks ago

Given answer is correct

upvoted 1 times

SkyZeroZx 11 months, 1 week 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 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 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, 4 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, 6 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, 3 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

AZcheck 1 year, 6 months ago

User 1: Group 1 only

User 2: Group 1 & 2 only

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #32

Topic 2

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>

Comments

mlantonis Highly Voted 3 years, 6 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 333 times

LovelyGroovey 9 months, 1 week 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 4 times

TechThameem 6 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 2 times

Mozbius_ 2 years, 10 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 98 times

NadirM_18 2 years, 8 months 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, 5 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 11 times

abhmala1 2 years, 9 months ago

microsoft's course is shit

upvoted 82 times

Asymptote 2 years, 1 month 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 1 year, 10 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 it as such.

upvoted 9 times

zman_83 2 years, 3 months ago

Damn your GOOD!, please keep up your work. The community need you for sure!!!:)

upvoted 18 times

obaali1990 1 year, 9 months ago

I am having problem understanding what the Box 1 actually requires. There are AD, Window Server Active Directory and Microsoft Account. How do I link these to the question?

upvoted 1 times

hakanbabu Highly Voted 4 years ago

I've checked on my AAD, answer is correct

upvoted 52 times

Somewhatbusy 3 years, 11 months ago

Yes its correct. 100% agreed

upvoted 6 times

Kiano 3 years, 7 months ago

I have also checked but I can see that you can change both job title and usagelocation 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, 6 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 be updated directly in Azure AD, although Jobtitle could be overwritten by the sync.

upvoted 9 times

Mozbius_ 2 years, 10 months ago

Thank you for the info.

upvoted 1 times

Shnash 2 years 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

SeMo0o0o0o Most Recent 3 months, 1 week ago

correct

Correct

upvoted 2 times

mojo86 4 months 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 9 months, 1 week 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 4 times

LovelyGroovey 9 months, 2 weeks 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 9 months, 4 weeks ago

Correct

upvoted 1 times

Babustest 1 year, 2 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 1 month, 2 weeks ago

Welcome to Microsoft testing, courses are just one small piece of the learning experience.

upvoted 1 times

Mehedi007 1 year, 4 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 1 year, 8 months 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 1 year, 8 months ago

Sorry my bad, answers are correct from ET

upvoted 2 times

Nitestorm 1 year, 8 months 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 1 year, 8 months ago

so what was the answer?

upvoted 1 times

Vivek88 1 year, 9 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 1 year, 10 months ago

Correct Answer. Tested in Lab

Box 1: User1 and User3

Box 3 : User1,User2 and User3

upvoted 5 times

NaoVaz 2 years, 2 months ago

JobTitle = User1 and User3 only

UsageLocation = User1, User2 and User3

upvoted 3 times

EmnCours 2 years, 3 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 1 year, 10 months ago

Why on earth are you copy and pasting someone else's opinion?

upvoted 5 times

HorseradishWalrus 2 years, 3 months ago

WHY on earth should I know this to pass this exam? This detail is sooo unimportant. Whether you know it or not does not tell anything about your qualification. Yet too many questions are like this...

upvoted 9 times

Mucker973 2 years, 5 months ago

Any user account sourced from on-prem AD CANNOT have ANY attribute changed in Azure AD. This is simply because of the "source of truth" rule with any form of identity in sync - there must be only one source of truth otherwise data gets dirty. In this case it is on-prem AD.

My other point is that I do think you can say that the guest account can have their attributes updated either; technically you can, but since they feel the need to tell you it is a guest account, it is implied that is in another tenant, so you won't access to update it. This is poorly worded question with some key info missing making it difficult to conclude in the guest user can be edited or not. It does

say "YOU" want to edit, but it does not say if you have admin rights of the other tenant where the guest account resides. So...poor question

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #33

Topic 2

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

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

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 **Most Voted**

B. No

Correct Answer: A

Community vote distribution

A (73%)

B (27%)

Comments

mlantonis **Highly Voted** 3 years, 6 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 137 times

twambala 3 years, 3 months ago

how can you

upvoted 5 times

twambala 3 years, 3 months ago

how can one manage something if he does not have access to it

upvoted 2 times

rsharma007 3 years, 2 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_ 2 years, 10 months ago

Thank you for clarifying! Much appreciated.

upvoted 1 times

RithuNethra Highly Voted 4 years ago

correct answer

upvoted 22 times

RVivek Most Recent 1 month 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 1 times

dirkxi 2 months, 1 week 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 2 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 4 times

blackwhites 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

SeMo0o0o0o 3 months ago

Owner & Network Contributor can enable Traffic Analytics

upvoted 1 times

Matsane 8 months ago

A is the correct answer

upvoted 1 times

abhikeshu 8 months ago

Selected Answer: A

as Microsoft document Allowed Roles Owner, Contributor, Network contributor (1) and Monitoring contributor (2),

1. Network contributor doesn't cover Microsoft.OperationalInsights/workspaces/* actions.

2. Only required when using traffic analytics to analyze VNet flow logs (preview). For more information, see Data collection rules in Azure Monitor and Data collection endpoints in Azure Monitor.

upvoted 3 times

bobothewiseman 8 months, 2 weeks ago

Selected Answer: A

Correct Answer: A - Yes

upvoted 2 times

tashakori 8 months, 3 weeks ago

Yes is right

upvoted 1 times

Cg007 9 months ago

Selected Answer: B

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 allows users to manage network resources, such as virtual networks and subnets, but it does not grant permissions to enable Traffic Analytics specifically. To enable Traffic Analytics, Admin1 needs permissions related to monitoring and analytics, which are not provided by the Network Contributor role.

Instead, Admin1 should be assigned a role that includes permissions to manage monitoring and analytics services, such as the Monitoring Contributor role or a custom role with the necessary permissions to enable Traffic Analytics.

upvoted 2 times

Wojer 9 months ago

Selected Answer: B

Traffic analytics requires the following prerequisites:

-A Network Watcher enabled subscription.

-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.

-An Azure Log Analytics workspace (1)with read and write access.

(1)Network contributor doesn't cover Microsoft.OperationalInsights/workspaces/* actions.

upvoted 2 times

kond 9 months, 1 week ago

just to enable traffic analytics network contributor role is enough ? - Copilot says NO, assigning the Network Contributor role is not enough to enable Traffic Analytics for an Azure subscription. The Network Contributor role provides permissions related to network resources, but it does not specifically grant access to configure or manage Traffic Analytics settings. To achieve the goal, you should assign the appropriate role related to Traffic Analytics, such as Log Analytics Contributor or Network Watcher Contributor. These roles provide the necessary permissions to enable and manage Traffic Analytics effectively.

upvoted 1 times

learnboy123 12 months ago

Selected Answer: B

b

upvoted 3 times

Gpsn 11 months, 2 weeks ago

It clearly states that Network Contributor role can access Traffic Analytics. So answer should be A - Yes.

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites>

One of the built in roles - Owner, Contributor, Network contributor, Monitoring contributor

upvoted 1 times

mtc9 1 year, 2 months ago

is subscription-level Reader role enough to modify network settings?

upvoted 1 times

GODUSGREAT 1 year, 1 month ago

No , you won't be able manage it

upvoted 1 times

Basimane_1 1 year, 2 months ago

MORNING GUYS WHATED TO ASK WHY ARE THEY SAYING THIS ...these questions will not appear in the review screen.?

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #34

Topic 2

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

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

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 **Most Voted**

B. No

Correct Answer: A

Community vote distribution

A (84%)

B (16%)

Comments

mlantonis **Highly Voted** 3 years, 6 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 70 times

Rockysekhon 1 year ago

mlantonis i read the question to enable not to view only etc.
upvoted 1 times

RithuNethra Highly Voted 4 years ago

correct answer
upvoted 13 times

SeMo0o0o0o Most Recent 2 months, 4 weeks ago

Selected Answer: A

A is correct

Owner & Network Contributor can enable Traffic Analytics
upvoted 2 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

A is correct
upvoted 1 times

3c5adce 7 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 8 months, 3 weeks ago

Yes is right
upvoted 1 times

kond 9 months, 1 week 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 4 months, 4 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 12 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>
upvoted 1 times

EwoutBI 10 months, 3 weeks 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, 4 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, 4 months ago

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner>

upvoted 1 times

[Removed] 1 year, 5 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, 6 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 1 year, 7 months ago

Yes. A is correct. Owner have full access to resources.

upvoted 1 times

kklohit 1 year, 9 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 1 year, 9 months 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, 1 month 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.OperationalInsights/workspaces/* actions.)

upvoted 1 times

KennethLZK 1 year, 11 months ago

Selected Answer: A

Correct

upvoted 2 times

MayurSingh 1 year, 11 months ago

Selected Answer: A

A is correct

upvoted 2 times

NaoVaz 2 years, 2 months ago

A) "Yes"

One of the following Azure built-in roles needs to be assigned to your account:

- Owner
- Contributor
- Reader
- Network Contributor

Reference: <https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements>

upvoted 2 times

DrMiyu 2 years, 5 months ago

Agree that YES the Owner gives enough right to do it BUT it gives too much also. The purpose is to "assign the required role to enable Traffic Analytics". Not to more ... So I wouldn't give the owner ship ... This is tricky question, it should be removed from the exam as it can lead to miss configuration.

upvoted 5 times

techtest848 2 years, 2 months ago

Agreed. Otherwise the question should say using 'least privilege'

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #35

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (81%)

A (19%)

Comments

asmodeus **Highly Voted** 4 years 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 100 times

visave 4 years ago

As per your description the answer is A. could you please paste the source of the information.

upvoted 2 times

visave 4 years 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 3 years, 8 months 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, 6 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, 5 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, 2 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

nNeo 3 years, 6 months ago

Although the article specified, but reader role can't change (or enable) "Traffic Analytics status" setting in NSG flow log settings.
IMO, that article should be edited.

upvoted 13 times

mlantonis Highly Voted 3 years, 6 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, 5 months ago

I think the answer is correct as it's assumed that the prerequisites to use traffic analytics are already met. Referring to

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, 5 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 21 times

Mozbius_ 2 years, 10 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, 3 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, 1 month ago

You should try standup comedy as an alternative career. Got into wrong profession.

upvoted 5 times

JeremyChainsaw Most Recent 2 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

SeMoOoOoOo 3 months, 1 week ago

Selected Answer: B

im going with B

upvoted 1 times

mojo86 4 months ago

Subscription Reader Role:

Permissions: The Subscription Reader role has read-only access to the Azure resources within a subscription

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 5 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 5 months, 2 weeks 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 6 months 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 6 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 6 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 7 months ago

No. Access but not enable.

upvoted 1 times

SinopsysHK 7 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

upvoted 2 times

3c5adce 7 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 7 months, 3 weeks 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 7 months, 3 weeks ago

Selected Answer: B

It seems reader role cannot enable traffic analytics. It can view it.

upvoted 4 times

6f80f6c 7 months, 3 weeks ago

Selected Answer: B

Answer is B, NO.

supporting : <https://learn.microsoft.com/en-us/answers/questions/1330227/what-role-is-required-to-be-enabled-at-subscriptio>

upvoted 2 times

Nushin 7 months, 4 weeks ago

Owner

Contributor

Network contributor 1 and Monitoring contributor 2

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #36

Topic 2

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 **Most Voted**
- D. Virtual Machine Administrator Login

Correct Answer: C

Community vote distribution

C (93%)

B (7%)

Comments

wooyourdaddy **Highly Voted** 4 years ago

Should the answer be C. Contributor? Answer B, only allows the managing of the VMs and not the Virtual Networks as stated in the question.

upvoted 232 times

brakonda 3 years, 2 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 3 years, 9 months ago

I agree

upvoted 1 times

Miles19 3 years, 8 months 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

upvoted 2 times

ciscogeek 3 years, 8 months 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 2 times

Gadzee 2 years, 10 months ago

I would go for B taking into account that they say "least privilege"

upvoted 5 times

Broniac 2 years, 9 months ago

yes but, with B you can only achieve to manage VMs not Vnets which is also mentioned.

upvoted 10 times

Deputy7 2 years, 9 months ago

Bro, It is User1 can deploy virtual machines and manage virtual networks. So, Definitely C.

upvoted 2 times

brico 3 years, 5 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 2 years, 9 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, 6 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 150 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: C

C is corerct

upvoted 2 times

brandon4sam 9 months, 3 weeks ago

Question is tricky, but it states "Least privilege" So answer C is correct

upvoted 1 times

Amir1909 9 months, 4 weeks ago

C is correct

upvoted 1 times

stanislaus450 10 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 10 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] 11 months, 1 week ago

Selected Answer: C

Contributor

upvoted 1 times

TSKARAN 1 year 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, 4 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, 5 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, 6 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, 6 months ago

Keyword here is & Networks. Only the contributor role can manage the VM's and the Networks.

upvoted 2 times

hz78 1 year, 7 months 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 1 year, 10 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 doesn't having write access to Microsoft.Network/virtualNetworks
Microsoft.Network/publicIPAddresses
Microsoft.Network/networkSecurityGroups
which stops VM creation.

upvoted 1 times

Raj70 2 years, 1 month ago

Virtual Machine Contributor can only do "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.", so it is clear that there is nothing it can do with VNET's and therefore the answer is C.

upvoted 1 times

klasbeatz 2 years, 2 months ago

So Contributor and VM Contributor are different

upvoted 1 times

NaoVaz 2 years, 2 months ago

Selected Answer: C

C) "Contributor"

Like already stated, the "Virtual Machine Contributor", lacks the ability to manage virtual networks: "This role does not grant you management access to the virtual network or storage account the virtual machines are connected to."

Reference: <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #37

Topic 2

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 i <input type="text" value="Search by name or email"/>	Type i <input type="text" value="All"/>	Role i <input type="text" value="Owner"/> <input type="text" value="Search for a role"/> <input checked="" type="checkbox"/> Select all <input checked="" type="checkbox"/> Owner
Scope i <input type="text" value="All scopes"/>	Group by i <input type="text" value="Role"/>	

1 items (1 Users)

<input type="checkbox"/>	NAME	TYPE	ROLE	SCOPE
--------------------------	------	------	------	-------

OWNER

 Admin3 Admin3@Cont...	User	Owner i	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

a93d91a6-faca-4fa6-a749-f6c25469152e



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 type="radio"/>	<input checked="" 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"/>

Box 1: No -

Only Admin3, the owner, can assign ownership.

Box 2: Yes -

Box 3: No -

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/add-change-subscription-administrator>

Comments

mlantonis Highly Voted 3 years, 6 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 531 times

Dankho 1 month, 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 1 times

schvantz 2 years, 7 months ago

crystal clear

upvoted 5 times

Takloy 3 years, 1 month ago

Unless configure the elevated access for Admin 2 right? making admin2 user access administrator.

upvoted 2 times

kastanov 2 years, 4 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, 6 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 61 times

ashish2201 3 years, 6 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 113 times

Praveen66 3 years, 3 months ago

Even if you're 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

ToxicTwins Most Recent 1 month, 1 week ago

Correct answers :

Box 1 = YES

Box 2 = YES

Box 3 = YES , as a Global Admin, you can elevate 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

teralberti 1 month, 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 2 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 2 times

Lazylinux 2 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 then 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, 5 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

SeMo0o0o0o 3 months, 1 week ago

wrong

Yes

Yes

No

upvoted 2 times

Makoporosh 5 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] 5 months, 4 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 6 months, 3 weeks ago

Answer should be : Yes Yes No

upvoted 2 times

3c5adce 7 months ago

I believe the more recent and tested answer which is YYN

upvoted 2 times

3c5adce 7 months ago

Answer is YYN

upvoted 2 times

Nateramj 8 months 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 8 months, 2 weeks ago

YES YES NO

Admin3 can elevate his permissions but in this question only Admin 1 has elevated his permissions

upvoted 1 times

tashakori 8 months, 3 weeks ago

No no no

upvoted 1 times

allyou 9 months, 3 weeks ago

I tested them in the lab, the answers are Y, Y, Y.

the questions are somewhat nuanced, if I rephrase it like this: is the AdminX user capable/has the possibility of... It becomes obvious to answer with Y, Y, Y because Admin2 can elevate access like Admin1 to control the subscription.

<https://learn.microsoft.com/fr-fr/azure/role-based-access-control/elevate-access-global-admin>

upvoted 1 times

Trs223333 1 year ago

Yes, Yes, and No

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #38

Topic 2

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 **Most Voted**
- 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%)

B (13%)

Comments

mlantonis **Highly Voted** 3 years, 6 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 260 times

itgg11 2 years, 4 months ago

A is a correct answer. Just tested in the lab and first you need to create a managed identity

upvoted 4 times

Kalzonee3611 1 year, 2 months ago

he is goat
upvoted 2 times

Dankho 1 month, 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 2 times

kilowd 2 years, 6 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 1 times

zman_83 2 years, 3 months ago

Trust in Superman(mlantonis)!!!
upvoted 24 times

BaldFury401 2 years, 2 months ago

mlantonis is a savage
upvoted 6 times

AzureGoD 2 years, 1 month ago

i promise he is LOL
upvoted 4 times

supershysherlock 2 years, 1 month ago

What ho, jolly good show that man!
upvoted 4 times

ment0s 1 year, 3 months ago

Right-O good chap, no faffing about, tally-ho!
upvoted 2 times

fedztedz Highly Voted 3 years, 10 months ago

Answer is correct "A" Modify Managed Identities.
upvoted 55 times

RVivek Most Recent 1 month 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 shoud modify that setting, then step B
upvoted 2 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

A is corerct
upvoted 2 times

mojo86 4 months 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 6 months 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 7 months 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 7 months ago

A. From the Azure portal, modify the Managed Identity settings of VM1

upvoted 1 times

stanislaus450 9 months, 4 weeks 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

sismir 11 months, 2 weeks 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 8 months, 4 weeks 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, 3 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, 3 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, 4 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, 6 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, 7 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 1 year, 7 months 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 1 year, 8 months 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



Exam AZ-104 All Actual Questions

Question #39

Topic 2

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 **Most Voted**
- 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



Comments

mlantonis Highly Voted 3 years, 6 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 296 times

Gyanshukla 3 years, 3 months ago

correct
upvoted 2 times

monus 3 years, 2 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, 3 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, 3 months ago

sorry, I meant Dev/Test environment. Think CI/CD.
upvoted 1 times

zr79 2 years, 9 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 8 times

mabdullah 1 year, 11 months ago

Thanks.
upvoted 2 times

Dips88 Highly Voted 3 years, 7 months ago

Answer should be B. A recovery service vault can not be deleted unless all its backups are deleted permanently. And along with that definitely resource lock has to be removed on vnet
upvoted 125 times

poplovic 3 years, 5 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, 5 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 2 years, 10 months ago

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault?tabs=portal>
vault manually deleted because it stays there 14 days.. B , is correct answer, if it was sql you need to shutdown sql instances for backup

Backup

upvoted 2 times

mmtechsolutionsinc 2 years, 9 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

Mazinger **Most Recent** 2 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

SeMo0o0o0o 3 months, 1 week ago**Selected Answer: B**

it's B

upvoted 1 times

CheMetto 4 months, 2 weeks 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 6 months 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 1 times

3c5adce 7 months 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 7 months ago

B. Remove the resource lock from VNET1 and delete all data in Vault1

upvoted 1 times

gio 8 months, 2 weeks 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 backed up data inside

upvoted 2 times

Cg007 9 months 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 9 months, 3 weeks 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 10 months ago

B is correct

upvoted 1 times

HdiaOwner 10 months, 1 week ago

Answer should be B

upvoted 1 times

MYR55 11 months, 1 week 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 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 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

ziggy1117 1 year, 1 month ago

Selected Answer: B

You do not need to turn off VMs to delete them. I made so many of those studying for AZ104 and i never had to turn off any VM before deleting it. Also you need to delete the contents of a vault before you can delete it. There is actually a lengthy checklist of things you need to do in the vault before you can delete it besides deleting its backup.

upvoted 3 times

pal40sg 1 year, 1 month ago

Selected Answer: D

What should you do **first**?

The answer is D. Turn off VM1 and delete all data in Vault1.

This is the correct answer because the question asks what should be deleted first before deleting TestRG. According to the current web page context, TestRG contains a virtual machine named VM1, a virtual network named VNET1, and a recovery services vault named Vault1. The web page context also states that VM1 is connected to VNET1 and that Vault1 contains backup data for VM1. Therefore, before deleting TestRG, we need to delete the resources that depend on it or have a resource lock. In this case, VM1 depends on VNET1 and Vault1 has a resource lock. To delete VM1, we need to turn it off first. To delete Vault1, we need to delete all the data in it first. Therefore, the first step is to turn off VM1 and delete all data in Vault1.

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #40

Topic 2

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. **Most Voted**
- 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%)

Comments

mlantonis Highly Voted 3 years, 6 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 233 times

suriyaswamy 3 years, 4 months ago

Nice Explanation. Many Thanks
upvoted 2 times

Tom34 2 years, 10 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 3 years, 10 months ago

All the best for your Exam guys:))

upvoted 169 times

omw2wealth 3 years, 2 months ago

Thank you i guess

upvoted 11 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: A

A is corerct

upvoted 1 times

tashakori 8 months, 3 weeks ago

A is right

upvoted 1 times

Athul07 1 year, 6 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 1 year, 8 months 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=WyDQhIRDad8&t=2s>

upvoted 4 times

Mazinger 1 year, 9 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] 1 year, 11 months ago

I'm not seeing any DNS questions on the recent test

upvoted 1 times

NaoVaz 2 years, 2 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, 3 months ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

Lazylinux 2 years, 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

manalshowaei 2 years, 6 months ago

Selected Answer: A

A. Create an NS record named research in the adatum.com zone.

upvoted 1 times

Chrys941 2 years, 8 months 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 2 years, 9 months ago

Selected Answer: A

<https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain>

upvoted 2 times

EleChie 2 years, 9 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, 2 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, 4 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 1 times



Exam AZ-104 All Actual Questions

Question #41

Topic 2

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>

Comments

mumu_myk Highly Voted 3 years ago

I bought a domain just to test this. The answer is correct. Please like me.

upvoted 1357 times

hehuo 1 year, 10 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 16 times

junaid001 1 year, 2 months ago

inspiring

upvoted 11 times

fene Highly Voted 3 years, 7 months ago

As I'm a smart guy I can confirm this to be the proper answer

upvoted 160 times

xheo 2 years, 9 months ago

I like your confidence :)

upvoted 5 times

maki999 11 months ago

me too :)

upvoted 2 times

rolling_potato_ 2 years, 9 months ago

Seems legit

upvoted 21 times

RVivek Most Recent 1 month 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 1 month, 1 week ago

this is the right answer

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

correct

upvoted 1 times

23169fd 6 months 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 7 months, 1 week ago

1- Create an Azure DNS Zone.

2- Add a record to the public contoso.com DNS zone.

3- Verify the domain.

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 4 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 8 months, 3 weeks ago

Given answer is correct

upvoted 1 times

897dd59 1 year, 2 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, 4 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, 2 months ago

It was purposefully called custom name to trick you into choosing "Create an Azure DNS Zone"

upvoted 2 times

NavigatiOn 1 year, 4 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

lolek997 1 year, 6 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, 4 months ago

very clear for me! LIKE

upvoted 1 times

etanvandan7 1 year, 7 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 1 year, 10 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 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, 1 month 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

NaoVaz 2 years, 2 months ago

1) "Add a custom domain"

2) "Add a record to the public contoso.com DNS zone"

3) "Verify the domain"

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#add-your-custom-domain-name-to-azure-ad>

upvoted 6 times



Exam AZ-104 All Actual Questions

Question #42

Topic 2

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" Most Voted
- C. select * from Event where EventType == "error"
- D. search in (Event) * | where EventType == "error"

Correct Answer: B

Community vote distribution

B (88%)

C (12%)

Comments

NaoVaz Highly Voted 2 years, 2 months ago

Selected Answer: B

B) 'Event | search "error"'

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial>
upvoted 11 times

AnKiLa 1 year, 10 months ago

Agree. Found another reference too:

<https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuredatexplorer>
upvoted 1 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

3c5adce 7 months, 1 week 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 2 times

MCLC2021 7 months, 1 week ago

Selected Answer: B

Repeated question Topic2.Question22

Correct answer B

upvoted 3 times

Amir1909 9 months, 4 weeks ago

B is correct

upvoted 1 times

Oryx360 1 year, 3 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 11 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, 5 months ago

Event

| where SeverityLevel == "Error"

Correct Answer: B

upvoted 1 times

Athul07 1 year, 6 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, 4 months ago

select * from Event where EventType == "error" is an example of SQL (Structured Query Language) whereas Log Analytics uses KQL (Azure Log Analytics Query Language).

KQL (Kusto Query Language). The correct answer is B
upvoted 5 times

gauravit43 1 year, 10 months ago

B - Tested in lab (Event | search "error")
upvoted 2 times

virgilpza 2 years, 3 months ago

Selected Answer: B

Correct Answer: B
upvoted 2 times

KSoul 2 years, 3 months ago

Selected Answer: B

Event | search "error"
upvoted 2 times

libran 2 years, 3 months ago

Selected Answer: B

Correct Answer: B
upvoted 2 times

EmnCours 2 years, 3 months ago

Selected Answer: B

Correct Answer: B
upvoted 2 times



Exam AZ-104 All Actual Questions

Question #43

Topic 2

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. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

Eltooth **Highly Voted** 3 years, 1 month 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 55 times

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

D. Modify the NS records in the DNS domain registrar.

upvoted 18 times

SeMo0o0o0o **Most Recent** 3 months, 1 week ago

Selected Answer: D

D is corerct

upvoted 1 times

CheMetto 4 months, 2 weeks 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 2 times

23169fd 6 months 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 8 months, 3 weeks ago

D is right

upvoted 1 times

tashakori 8 months, 4 weeks ago

D is right

upvoted 1 times

Lowe6 11 months, 1 week 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, 6 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 1 year, 8 months 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 1 year, 9 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] 1 year, 11 months ago

Not seeing DNS questions in the 2 tests I took

upvoted 5 times

Marge_Simpson 1 year, 10 months ago

Neither have I

upvoted 2 times

NaoVaz 2 years, 2 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, 3 months ago

Selected Answer: D

this is pretty easy, D

upvoted 2 times

EmnCours 2 years, 3 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 2 years, 9 months ago

Selected Answer: D

<https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

upvoted 2 times

edengoforit 2 years, 9 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



Exam AZ-104 All Actual Questions

Question #44

Topic 2

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.

You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.

You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.

Correct Answer:

Answer Area

Statements

Yes No

You can assign the Storage File Data SMB Share Contributor role to User1 for share1.

You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.

You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.



Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azure-portal>

Comments

ech Highly Voted 3 years, 2 months ago

Yo cannot give share-level priviledges to a computer object. Ans is correct.

upvoted 47 times

ExamWolf 1 year ago

You can if you add the computer object to a group first :)

upvoted 1 times

nir977 2 years, 11 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 25 times

allyQ 1 year, 9 months ago

I have created an AAD user (not synched from the WinDC) and can give it the Storage file data SMB Elev. Contributor role.

upvoted 8 times

ubiquituz 1 year 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 2 years, 9 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 21 times

Announcement Most Recent 3 weeks, 1 day 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 1 month ago

User1 is creataed in ADDS but synced to Entra AD so Yes.

Computer account cannt 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 1 times

SeMo0o0o0o 3 months, 1 week ago

correct

upvoted 2 times

mojo86 4 months 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 8 months, 3 weeks ago

Yes

No

No

upvoted 2 times

Amir1909 9 months, 2 weeks ago

Yes

No

No

upvoted 1 times

vsvaid 10 months, 2 weeks ago

Y -N -N,

Hybrid user will work

Computer and cloud users will not work

upvoted 1 times

31c21da 11 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 10 months, 2 weeks 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 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 3 times

GoldBear 12 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 4 times

897dd59 1 year, 2 months ago

should be Y-N-Y

1/ you cannot assign for object: computer

2/ user2 is a cloud user => can fully manage on cloud

upvoted 1 times

AMEHAR 1 year, 3 months ago

Y -N -N

upvoted 3 times

GoldenDisciple2 1 year, 3 months ago

Microsoft clearly states the user must have a hybrid identity therefore 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 3 times

Andy_S 1 year, 6 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 4 times

Andy_S 1 year, 6 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

RandomNickname 1 year, 6 months ago

Y,N,N

As per link:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azure-portal>

1: Hybrid users are supported

2: Because computer accounts don't have an identity in Azure AD, 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.

3: Authentication and authorization against identities that only exist in Azure AD, such as Azure Managed Identities (MSIs), aren't supported

upvoted 6 times

RandomNickname 1 year, 6 months ago

For 3rd question, changing it to Y.

It is a cloud user, however it is synced to on prem and visible there, so should be able to add since it doesn't "only exist in Azure AD" as per link

upvoted 2 times

CheMetto 4 months, 2 weeks ago

The sync is 2 way only for group. The user on the cloud won't be synced on prem

upvoted 1 times

Vanilla007 1 year, 7 months ago

Third option should be Y right? Because even though user 2 is cloud user, file share is in AZ storage account so he must be able to access if given access??

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #45

Topic 2

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>

Comments

pakman Highly Voted 3 years, 2 months ago

Correct.

Security admin can't add subnets.

Only owner can assign roles.

upvoted 83 times

NaoVaz Highly Voted 2 years, 2 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 70 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

correct

upvoted 2 times

Amir1909 9 months, 3 weeks ago

Correct

upvoted 2 times

[Removed] 1 year, 3 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, 1 month 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, 5 months ago

1.User1 and User3
2. User1 only because security admin can't add security roles
upvoted 2 times

Rams_84z06n 1 year, 8 months 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 1 year, 11 months ago

The provided answer is correct.

upvoted 2 times

EmnCours 2 years, 3 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 2 years, 9 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 2 years, 9 months ago

the answer is correct, only owner can assign reader role and owner and contributer can add subnet
upvoted 1 times

subhuman 3 years 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



Exam AZ-104 All Actual Questions

Question #46

Topic 2

HOTSPOT -

You have the Azure resources shown on the following exhibit.



Tenant Root Group



MG1



Sub1



RG1



VM1

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	

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>

Comments

GepeNova Highly Voted 3 years, 2 months ago

Correct answer.

Only can assign locks and tags to subscriptions, resource groups and resources. Tested in lab

upvoted 107 times

atospace 2 years, 1 month ago

Tenant parent group also a subscription so answer should be the last choice?

upvoted 1 times

xRiot007 1 year, 6 months ago

The tenant parent group is an MG, not a Sub.

upvoted 3 times

Omar_Aladdin Highly Voted 3 years, 2 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 31 times

Chuong0810 Most Recent 1 month, 2 weeks 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 1 times

SeMo0o0o0o 3 months, 1 week ago

correct

upvoted 2 times

Charumathi 6 months 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 2 times

3c5adce 7 months 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 8 months, 3 weeks ago

Given answer is correct

upvoted 1 times

Rams_84z06n 1 year, 8 months ago

tested it. Given answer is correct

upvoted 3 times

zellck 1 year, 10 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, 2 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, 2 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, 3 months ago

Correct Answer -

Locks: Sub1, RG1, and VM1 only

Tags: Sub1, RG1, and VM1 only

upvoted 1 times

EmnCours 2 years, 3 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_ 2 years, 9 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 2 years, 9 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 2 years, 9 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 2 years, 9 months ago

both answers are correct, you can only assign tags and locks to Subscriptions, Resource groups and resources

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #47

Topic 2

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 **Most Voted**
- 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%)

Comments

Mazinger Highly Voted 2 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 24 times

NaoVaz Highly Voted 2 years, 2 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

minura Most Recent 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corerct

upvoted 1 times

3c5adce 7 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 9 months, 3 weeks ago

B is correct

upvoted 1 times

ric2020 11 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 1 year, 9 months ago

If they were all that easy

upvoted 1 times

zelliCK 1 year, 10 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 1 year, 10 months ago

B is the correct answer

upvoted 1 times

majerly 2 years, 2 months ago

today in exam is B

upvoted 7 times

jesusalex1s 2 years, 2 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, 3 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, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

libran 2 years, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

EmnCours 2 years, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

vivij 2 years, 7 months ago

Correct answer. You can verify the same at: <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete#:~:text=To%20bulk%20delete%20users,-Sign%20in%20to&text=In%20Azure%20AD%2C%20select%20Users,value%20is%20User%20principal%20name.>

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #48

Topic 2

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

Storage1 has the Tag1:subscription, Tag2:IT, Tag3:value1, and Tag4:value4 tags assigned.

VNET1 has the Tag2:IT and Tag3:value2 tags assigned only



Correct Answer:

Answer Area

Statements

Yes No

RG1 has the Tag2:IT tag assigned only



Storage1 has the Tag1:subscription, Tag2:IT, Tag3:value1, and Tag4:value4 tags assigned.



VNET1 has the Tag2:IT and Tag3:value2 tags assigned only



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>

Comments

Lionred Highly Voted 2 years, 12 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:value4 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:value4.

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 223 times

DalyMasmoudi 3 days, 20 hours 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 1 times

S3ktar 2 years, 11 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 2 years, 11 months ago

Correct answer is y-n-n

upvoted 56 times

marioZuo 1 year, 4 months ago

I tested also, but the tag is appended automatically on my side.

upvoted 3 times

mufflon 2 years, 10 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 will add Tag4 with value: value4

upvoted 2 times

albergd 2 years, 9 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 68 times

Abdou001 1 year, 10 months ago

@Albergd, you convinced me. Thanks !

upvoted 3 times

dimsok 1 year, 10 months ago

Y-N-N, RG1 is excluded

upvoted 22 times

happieeee 1 month, 2 weeks 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 2 times

Mshaty 2 months, 2 weeks ago

RG1 is not excluded what is excluded Vnet1 which is in RG1

upvoted 3 times

juniorcecs 2 years, 7 months ago

this is just wron

upvoted 1 times

testmobile18 Highly Voted 2 years, 12 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 131 times

gofto 2 years, 11 months ago

doubt that this explanation is correct
upvoted 3 times

Edward2021 2 years, 12 months ago

I think the same!!! Y N N
upvoted 10 times

olsenOns 2 years, 12 months ago

Correct,
Y - RG1 has its own tag, and is excluded from policy
N
N
upvoted 7 times

maatkse 2 years, 11 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 2 years, 10 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.examtopics.com/exams/microsoft/az-104/view/9/#>
upvoted 1 times

bacana Most Recent 1 month 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 1 month 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 1 times

LinuxLewis 1 month, 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 1 month, 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 1 month, 2 weeks ago

there seems to be a lot 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

SeMo0o0o0o 3 months, 1 week ago

Wrong

Yes

No

No

upvoted 2 times

ELearn 3 months, 1 week 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 3 months, 1 week 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 4 months, 2 weeks 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 1 times

OpOmOp 5 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 6 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 7 months ago

ChatGPT4 - NNY

upvoted 1 times

Wassel_Laouini 7 months, 2 weeks 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

mkhlzsrf 8 months, 1 week 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 8 months, 3 weeks 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

Aadhithya 8 months ago

This is the best explanation for the exclusion criteria

upvoted 3 times

tashakori 8 months, 3 weeks ago

Given answer is right

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #49

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (98%)

A

Comments

GoldenFox **Highly Voted** 3 years 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 252 times

scottytohotty 3 months, 3 weeks ago

This is the way.

upvoted 2 times

maatkse 2 years, 11 months ago

Are you sure on Q.38 - reader role can only access not enable traffic analytics

upvoted 15 times

mmtechsolutionsinc 2 years, 9 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 2 years, 9 months 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 18 times

edd004 1 year, 6 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 12 times

flyingcolours87 1 year, 5 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 6 times

ABhi101 2 years, 11 months ago

GoldenFox is correct

upvoted 5 times

jackAttew_1 2 years, 11 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 5 times

Marski Highly Voted 2 years, 10 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

allinict Most Recent 2 weeks, 1 day 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 2 weeks, 4 days 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 1 times

RVivek 4 weeks ago

Selected Answer: B

To enable Traffic manager one of there three RBAC required 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 2 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 2 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 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

SeMo0o0o0o0o 3 months ago

Owner & Network Contributor can enable Traffic Analytics

upvoted 1 times

TheFivePips 4 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 8 months, 3 weeks ago

No is right

upvoted 1 times

LPaul 1 year, 2 months ago

Please read carefully "Traffic Manager " Contributor nothing to do with "Traffic Analytics" , is 2 different service .

upvoted 4 times

Souban07 1 year, 5 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 1 year, 10 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, 6 months ago

wrong, Reader Role is not correct. The rest is.

upvoted 3 times

nixer82 2 years, 1 month 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 1 year, 7 months 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

naxer82 2 years, 1 month 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 1 times

maheshm124 1 year, 10 months ago

#33 say you assign network contributor role -- so Yes

Here in #49 you assign traffic manager contributor role -- so NO
both roles are different

upvoted 3 times

bcristella 2 years, 1 month ago

Answer: No

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

You have to consider the 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:

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #50

Topic 2

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 **Most Voted**
- C. access packages in Azure AD entitlement management
- D. Azure roles

Correct Answer: B

Community vote distribution

B (93%)

A (7%)

Comments

HananS **Highly Voted** 2 years, 12 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 47 times

magichappens 2 years, 8 months 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 whether they need to administer all users or should only administer the users of their respective office.

upvoted 16 times

NaoVaz **Highly Voted** 2 years, 2 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 16 times

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

JananiToo 9 months, 3 weeks ago

Why some YouTube videos say azure AD roles?

upvoted 2 times

af68218 8 months, 2 weeks 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 2 times

Amir1909 9 months, 3 weeks ago

B is correct

upvoted 1 times

Rednevi 1 year, 2 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 7 times

grimrodd 1 year, 3 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, 2 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, 4 months ago

answer is correct

<https://youtu.be/XNqSQOYtcPQ>

upvoted 1 times

Chris76 1 year, 7 months 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 1 year, 8 months 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 1 year, 9 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 1 year, 9 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 nt actually specify.

upvoted 5 times

Chris76 1 year, 7 months ago

Finally somebody sane with attention to details

upvoted 2 times

zellck 1 year, 10 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 1 year, 10 months ago

Administrative units is correct

upvoted 1 times

EmnCours 2 years, 3 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 2 years, 9 months ago

It's very obvious, Administrative Unit is the answer

upvoted 2 times

edengoforit 2 years, 9 months ago

Answer is Administrative unit

If you go to porta.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

Snownoodles 2 years, 11 months ago

Why is A not correct?

Even with B(admin unit), you have to assign AAD role to administrators for an admin unit.

upvoted 5 times

Mozbius_ 2 years, 10 months ago

I think that B is the answer because it is what the question is implying a scenario for which "Administrative Units" are specifically tailored for...

"Deployment scenario

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#:~:text=An%20administrative%20unit%20is%20an%20Azure%20AD%20resource,any%20portion%20of%20your%20organization%20that%20you%20define.>

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #51

Topic 2

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

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

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 **Most Voted**

B. No

Correct Answer: A

Community vote distribution

A (60%)

B (40%)

Comments

MrMacro **Highly Voted** 2 years, 12 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-securig-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 66 times

2d153f5 3 weeks, 3 days ago

Contributor is needed.

upvoted 1 times

itniv2 2 years, 9 months ago

... 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 18 times

sca88 4 weeks, 1 day ago

The question talk about create Logic App. So Logic App Contributor Role it's enough

upvoted 1 times

klasbeatz 2 years, 2 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 1 year, 10 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, 1 month 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 15 times

LuLaCeK 1 month, 2 weeks ago

Tested as well, got the same error.

upvoted 2 times

sca88 Most Recent 4 weeks, 1 day 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 1 month, 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 1 month, 3 weeks ago

Selected Answer: A

A correct

Logic App Contributor & Contributor can create logical apps

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: A

A is correct

Logic App Contributor & Contributor can create logical apps

upvoted 1 times

asaulu 3 months, 4 weeks ago

Microsoft.Resources/deployments/* Create and manage a deployment ... Means Logic App Contributor can create a logic app
upvoted 1 times

Carmen_Ms 4 months, 1 week ago

Tested! The answer is A, you can create logic apps but only of the comsumption type. So the objective is fulfilled. All those who say the B, you have not tested it correctly.

upvoted 4 times

etrop 4 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 4 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 3 times

a6bd45e 4 months, 3 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

Makoporosh 5 months ago

No: While the Logic App Contributor role is useful for managing existing logic apps, it does not grant permissions to create new logic apps or other Azure resources. Therefore, to meet the requirement of allowing the Developers group to create Azure Logic Apps in the Dev resource group, you must assign them the Contributor role at the resource group level.

upvoted 1 times

apazman123 5 months ago

Selected Answer: B

Contributor and Logic App Contributor are different

upvoted 1 times

004b54b 5 months, 1 week ago

Selected Answer: B

Based on <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-contributor>, answer should be B. No

upvoted 1 times

HelixAbdu 5 months, 3 weeks ago

the Answer Is No.

I just tried it and got this error:

You cannot perform this action without all of the following permissions (Microsoft.Storage/storageAccounts/write, Microsoft.Web/ServerFarms/write, Microsoft.Web/Sites/write)

upvoted 3 times

MSExpertGER 5 months, 3 weeks ago

Selected Answer: B

B (NO) is correct. to create resources in a resource group, you need to be a Contibutor (Built-in Role). The Logic Apps

Contributor may change certain settings on an individual Logic App Instance, but not create a new Logic App resource!
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/integration#logic-app-contributor>
upvoted 1 times

Homedollars 6 months, 3 weeks ago

The answer is "Yes", assigning the Logic App Contributor role to the Developers group on the Dev resource group will meet the goal of providing the Developers group with the ability to create Azure Logic Apps in the Dev resource group. The Logic App Contributor role grants users the permissions necessary to create, update, and delete Logic Apps, but does not grant permissions to manage the resource group itself. This ensures that members of the Developers group can work within the Dev resource group to create Logic Apps without granting them broader permissions within the subscription. So, the solution provided meets the goal effectively.

upvoted 3 times

3c5adce 7 months ago

While the Logic App Standard Developer role provides more specific permissions tailored for developers working with Logic Apps, the Logic App Contributor role still grants the necessary permissions to create and manage logic apps within the specified resource group.

Therefore, both solutions meet the goal of providing the Developers group with the ability to create Azure Logic Apps in the Dev resource group.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #52

Topic 2

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) ①

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.

▼

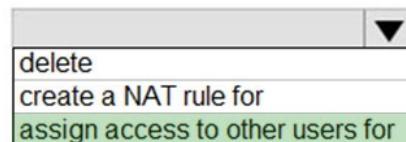
delete a virtual machine from
modify the load balancing rules in

deploy an Azure Kubernetes Service (AKS) cluster to

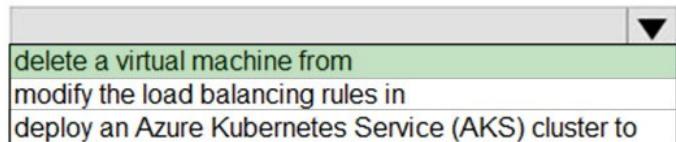
Correct Answer:

Answer Area

User1 can [answer choice] LB1.



User1 can [answer choice] the resource group.



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>

Comments

NaoVaz Highly Voted 2 years, 2 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 96 times

Rogit Highly Voted 1 year, 4 months ago

Was in test yesterday

upvoted 11 times

rteinformatica 1 year, 4 months ago

A lot of questions came out of here? Would they arrive to approve?

upvoted 1 times

behradcl Most Recent 3 months, 1 week ago

answer is absolutely correct

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

correct

upvoted 2 times

tashakori 8 months, 3 weeks ago

Given answer is right

upvoted 1 times

Amir1909 9 months, 3 weeks ago

Correct

upvoted 1 times

SkyZeroZx 11 months, 1 week ago

- 1) User1 can "assign access to other users for" LB1.

2) User1 can "delete a virtual machine from" the resource group

C) User can delete a virtual machine from the resource group.

The Role assignments say it all.

upvoted 1 times

nmm22 1 year, 2 months ago

i wish all questions were as simple as this

upvoted 5 times

zellck 1 year, 10 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, 1 month ago

Its Correct

upvoted 5 times

ECNS 2 years, 2 months ago

Answer is CORRECT

upvoted 5 times

EmnCours 2 years, 3 months ago

Answer is CORRECT

upvoted 4 times

vetrivelm 2 years, 7 months 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 2 years, 7 months ago

Correct

upvoted 2 times

Pasmo 2 years, 7 months ago

Correct Answer

upvoted 1 times

AzureDev777 2 years, 7 months ago

Answer is correct

upvoted 1 times

epomatti 2 years, 7 months ago

Answer provided is correct.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #53

Topic 2

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. **Most Voted**
- 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%)

C

Comments

MentalG Highly Voted 2 years, 7 months 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 50 times

NaoVaz Highly Voted 2 years, 2 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 1 week, 6 days ago

Selected Answer: B

Anything with 'Contributor' in the role cannot do anything with users.

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

Jedi_sg2000 6 months, 4 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 7 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

kijokskip 8 months, 4 weeks 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

Rednevi 1 year, 2 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, 3 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 4 times

Mehedi007 1 year, 4 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, 5 months ago

within provided solution , the Owner role can assign role for other users

B. Owner is answer

upvoted 1 times

Athul07 1 year, 6 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 1 year, 10 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 1 year, 10 months ago

Selected Answer: B

B is the answer.

upvoted 3 times

EmnCours 2 years, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 2 times

vetrivelm 2 years, 7 months ago

Answer B is correct. Owner Has full access to all resources including the right to delegate access to others.

upvoted 2 times

sjb666 2 years, 7 months ago

Selected Answer: B

Answer is B. Contributor can't grant access to others

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #54

Topic 2

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

Correct Answer:

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

Box 1: roletype -

You need to configure Azure RBAC policy to determine who can log in to the VM. Two Azure roles are used to authorize VM login:

Virtual Machine Administrator Login: Users with this role assigned can log in to an Azure virtual machine with administrator privileges.

Virtual Machine User Login: Users with this role assigned can log in to an Azure virtual machine with regular user privileges.

Note, example roletype:

```
"roleName": "Virtual Machine Administrator Login",
"roleType": "BuiltInRole",
"type": "Microsoft.Authorization/roleDefinitions"
```

Box 2: assignableScopes -

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

When you assign roles, you must specify a scope. Scope is the set of resources the access applies to. In Azure, you can specify a scope at four levels from broad to narrow: management group, subscription, resource group, and resource.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows>

<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/role-assignments-portal>

Comments

pkkalra Highly Voted 2 years, 3 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 219 times

duongduong_me 2 weeks, 3 days 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 10 months, 3 weeks 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 1 year, 7 months 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 31 times

ajdann 1 year, 3 months ago

Thank you, this helped me understand the difference

upvoted 2 times

sca88 Most Recent 4 weeks, 1 day 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 3 times

pstree 3 weeks, 5 days 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 4 times

sca88 1 week, 4 days ago

Thank you for the documentation link! So the correct Answer will be DataAction.

upvoted 2 times

Chuong0810 1 month, 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 1 month, 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 1 month, 2 weeks ago

all the AIs (ChatGPT, Google's whatever it's called) say actions

upvoted 1 times

Dankho 1 month, 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 1 month, 3 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 1 month, 3 weeks ago

Data Actions and assignableScopes
upvoted 3 times

komlaragnar 2 months 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

SeMo0o0o0o 3 months ago

WRONG

dataActions
assignableScopes
upvoted 2 times

behradcl 3 months, 1 week 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 1 month, 2 weeks ago

every single example is in the actions section not dataActions, are you high?

upvoted 1 times

divzrajshekhar123 4 months, 1 week ago

ANSWER IS dataactions and Assignable Scope

upvoted 2 times

ajay01avhad 4 months, 2 weeks ago

For the first requirement: actions

For the second requirement: assignableScopes

upvoted 2 times

23169fd 6 months ago

tested: Actions and Assignable Scope

"Microsoft.Compute/virtualMachines/login/action"

upvoted 4 times

Highgate 3 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 6 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 6 months, 1 week ago

Correct answer: Actions and Assignable Scope.
"Microsoft.Compute/virtualMachines/login/action"
upvoted 1 times

varinder82 6 months, 3 weeks ago

Final Answer : Data Action and AssignableScope
upvoted 2 times



Exam AZ-104 All Actual Questions

Question #55

Topic 2

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. **Most Voted**
- 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%)

Comments

NaoVaz **Highly Voted** 2 years, 2 months 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 21 times

Asta2001 1 year, 12 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 1 year ago

No, because it is now called "Microsoft Entra Domain Services".

upvoted 5 times

Athul07 Highly Voted 1 year, 6 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 18 times

Amir1909 Most Recent 8 months, 3 weeks ago

A is correct

upvoted 1 times

Mehedi007 1 year, 4 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

zellck 1 year, 10 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

zellck 1 year, 10 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, 10 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, 2 months ago

A is Correct

upvoted 3 times

libran 2 years, 3 months ago

Selected Answer: A

A is the right answer

upvoted 3 times

EmnCours 2 years, 3 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

RichardBill 2 years, 3 months ago

Correct

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #56

Topic 2

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. **Most Voted**

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 (83%)

Other (17%)

Comments

NaoVaz **Highly Voted** 2 years, 2 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 choose the User Access Administrator role instead of the Owner one.

upvoted 47 times

XristophD 2 years 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

privileges 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 1 year, 11 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 10 times

lykeman26 1 month, 3 weeks ago

It says for the planned and existing subscriptions. So it has to be the root tenant MG

upvoted 2 times

AnonFox 1 year, 7 months 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 4 months, 1 week 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

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: B

B is corerct

upvoted 1 times

GreenTick 5 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 7 months 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 9 months, 3 weeks ago

B is correct

upvoted 1 times

LetsGetThisCert 1 year, 1 month 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, 4 months ago

I think the key here is "existing subscriptions and the planned/future subscriptions"

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 so there's no point to it.

upvoted 4 times

Amateur2023 1 year, 3 months ago

yes; tks for your explain

upvoted 1 times

Teroristo 1 year, 4 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 choose the User Access Administrator role instead of the Owner one.

upvoted 1 times

[Removed] 1 year, 5 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, 6 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, 6 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, 6 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, 7 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 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 2 times

AnonFox 1 year, 9 months ago

Selected Answer: B

B is correct.

upvoted 3 times

er101q 1 year, 10 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 1 year, 10 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

zellck 1 year, 10 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/governance/management-groups/overview#root-management-group-for-each-directory>

Each directory is given a single top-level management group called the root management group. The root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level.

<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.

upvoted 1 times

zellck 1 year, 10 months ago

Assigning the User Access Administrator role to the root management group for Group1 will provide the necessary permissions for Group1 to manage role assignments for all existing and planned subscriptions, while also adhering to the principle of least privilege. This option also minimizes administrative effort as it only requires a single assignment.

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #57

Topic 2

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

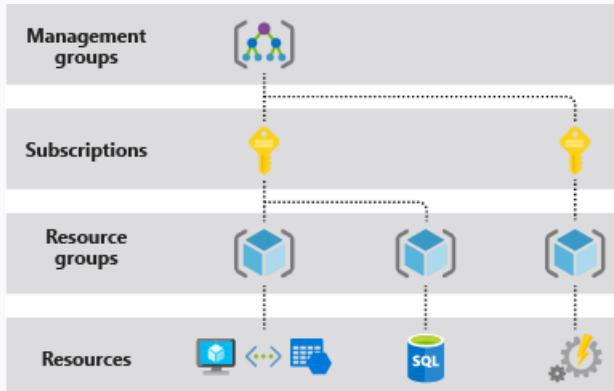
You can exclude Policy1 from:

- 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

Box 1: Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

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.

Note: Azure provides four levels of scope: management groups, subscriptions, resource groups, and resources. The following image shows an example of these layers.



Box 2: ManagementGroup1, Subscription1, RG1, and VM1

You can exclude a subscope from the assignment.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>

Comments

Ntinsky Highly Voted 2 years, 2 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.

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

- check assignments

In my opinion the provided answer is correct

upvoted 23 times

RichardBill 2 years, 3 months ago

So I checked again and the portal doesn't let you do it! That's what I based my assumption! But via Azure CLI it says that a resource is a valid 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 36 times

meeko86 2 years 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 4 times

Grande 2 years, 3 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, 3 months ago

Tried in portal as well. You cannot select resources as scope.

upvoted 4 times

buzzerboy 1 year, 11 months ago

I couldn't assign a policy at Tenant Root Management Group. There is no blade for policy.

upvoted 2 times

fittech Most Recent 2 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 2 times

SeMo0o0o0o 2 months, 4 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 1 times

SeMo0o0o0o 3 months, 1 week 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

SeMo0o0o0o 2 months, 4 weeks ago

sorry i misserad it,

You can assign Policy1 to:

Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only

Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only

You can exclude Policy1 from:
ManagementGroup1, Subscription1, RG1, and VM1 only
upvoted 1 times

Mshaty 2 months, 4 weeks ago

if you can exclude it doesn't that mean you can assign the policy to the resource ?you cant exclude something that cannot be part of the policy

upvoted 1 times

SeMo0o0o0o 2 months, 4 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 mentioned here, so we have to answer this in general.

upvoted 1 times

pasangawa 3 months, 1 week ago

tested on lab, you can assign policy on vm

upvoted 1 times

pet3r 4 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 5 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 5 months, 4 weeks ago

given answer is correct.

upvoted 2 times

76d5e04 6 months ago

Feeling tired of reading discussions. examtopics please quality seems ?

upvoted 2 times

76d5e04 6 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 4 months, 1 week 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 6 months, 3 weeks ago

the key in question is only

upvoted 1 times

3c5adce 7 months 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

MCLC2021 7 months, 1 week ago

- 1/ You can assing Policy1 to: Tenant Root Group, Mangement Group 1, Subscription 1, RG1,VM1
2/ You can exclude Policy1 to: Mangement Group 1, Subscription 1, RG1, VM1

"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." <https://learn.microsoft.com/en-us/azure/governance/policy/overview>

"Subscopes can be excluded, if necessary. "<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview#understand-scope>

upvoted 1 times

Dankho 2 months, 2 weeks ago

Link doesn't include tenant level.

upvoted 1 times

op22233 7 months, 2 weeks ago

The given answers are correct. Policy can be applied to all, Remember the kind of policy you can apply to prevent a particular set of types of instance while creating your VM., then the Only you can exclude all except the Tenant root Group from a policy.

upvoted 2 times

WeepingMaplte 7 months, 4 weeks ago

Answer should be:

- 1) Tenant Root Group, MG1, Sub1 and RG1 Only
- 2) MG1, Sub1, RG1 and VM1 only

upvoted 2 times

Amir1909 9 months, 3 weeks ago

Assign policy1: 4te Antwort

Exclude policy1: 4te Antwort

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #58

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (92%)

A (8%)

Comments

aaa112 **Highly Voted** 3 years, 11 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 96 times

miki 3 years, 9 months ago

mlantonis 3 years, 9 months ago

Thank you for clarifying

upvoted 2 times

r3tr0penguin 3 years, 6 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, 6 months ago

Yes because user2 wont have any role or connection with the new tenant unless added by user1 specifically.

upvoted 29 times

AzureG0d 2 years, 1 month 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, 1 month 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, 6 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 82 times

behradcll 3 months ago

OMG read question carefully, answer is NO

upvoted 1 times

Spam101198 1 year, 9 months ago

Question is asking about User 2 not user 1 , hence answer is NO

upvoted 16 times

EricMaes 3 years, 2 months ago

Didn't he become owner?

upvoted 3 times

A_GEE 2 years, 6 months ago

Yes. User1 becomes the owner and the first user in that Tenant
upvoted 4 times

FlaShhh 1 year ago

The Azure God mlantonis is wrong for once, is the world ending?
upvoted 11 times

rodrod 1 month, 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

myarali Most Recent 2 months, 1 week 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 7 times

shadad 2 months, 1 week 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 1 year, 9 months ago

How was your experience bro ?
upvoted 2 times

Omer87 2 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

it's B

upvoted 1 times

SeMo0o0o0o 3 months ago

only User1
upvoted 1 times

mojo86 4 months 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 4 months, 2 weeks 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 4 months, 2 weeks 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

OpOmOp 5 months 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

OpOmOp 5 months ago

Microsoft Entra ID (formerly Azure Active Directory)

upvoted 1 times

LearnerFL 5 months, 1 week 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 5 months, 2 weeks ago

yes and no, according to the least privilege you need a User Administrator hence (B)

upvoted 1 times

aflavien 5 months, 4 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 7 months 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 7 months, 1 week 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

behradcll 3 months ago

Read the question carefully for God sake

upvoted 1 times

tashakori 8 months, 4 weeks ago

No is right

upvoted 2 times

gil906 9 months, 1 week ago

Selected Answer: A

Answer is Yes, User2, as a Global Administrator in the Azure Active Directory, has the necessary permissions to create new user accounts in any associated directory, including external.contoso.onmicrosoft.com.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #59

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (92%)

A (8%)

Comments

Itkiller **Highly Voted** 2 years, 6 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>

account-in-the-new-tenant

upvoted 30 times

pranavhalgekar Highly Voted 2 years, 6 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

SeMo0o0o0o Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

SeMo0o0o0o 3 months ago

only User1

upvoted 1 times

MCLC2021 7 months, 1 week 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, 5 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 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 1 year, 9 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 1 year, 9 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 1 year, 9 months ago

There are several versions of this question. The following are the valid and invalid solutions that may be presented.

Valid Solution: Meets the Goal

Solution: You instruct User1 to create the user accounts.

Invalia 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 1 year, 10 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

zellick 1 year, 10 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, 2 months ago

This proves that answer to question 58 is No

upvoted 6 times

NaoVaz 2 years, 2 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, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

EmnCours 2 years, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

Fatrat 2 years, 3 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, 5 months ago

The answer is B

upvoted 1 times

Lazylinux 2 years, 5 months ago

B for sure

What be forgotten is that

Azure AD roles are used to manage access to Azure AD resources, whereas Azure roles are used to manage access to Azure resources.

The scope of Azure AD roles is at the tenant level, whereas the scope of Azure roles can be specified at multiple levels including management group, subscription, resource group, resource.

and hence Subscription owner has not access to AZ AD where as Azure Global Admin Can be granted owner of Azure subscription and not other way wrong

upvoted 5 times



Exam AZ-104 All Actual Questions

Question #60

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (83%)

A (17%)

Comments

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

The answer is No!

I tested this.

1. I created a new Tenant contosogmpp.
2. Added 2 users, User1 and User 2 in this tenant and gave them global privileges
3. I logqed through User1 and created a new tenant called externalcontosqmpp

4. Now when I logged in through User2 and try to switch tenants, the new tenant externalcontossgmpp is not available at all for User2. Hence User1 needs to invite User2 first

upvoted 61 times

ELearn 4 months, 4 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, 3 months ago

Selected Answer: B

it is another tentant

upvoted 47 times

allinict Most Recent 2 weeks, 1 day 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 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corerct

upvoted 1 times

SeMo0o0o0o 3 months ago

only User1

upvoted 1 times

hercule 5 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 5 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 7 months, 1 week 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

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 6 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 8 months, 4 weeks ago

No is right

upvoted 1 times

rreghioua 11 months, 1 week ago

Selected Answer: A

upvoted 1 times

VV11_SS22 1 year, 4 months ago

Correct answer is B

upvoted 1 times

NejmeddineBch 1 year, 4 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, 5 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, 5 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 1 year, 8 months 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 1 year, 9 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 1 year, 9 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 1 year, 9 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: 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

MotivePro 1 year, 8 months ago

what is the difference between user 1 and user2? they are both Global Admin..

upvoted 1 times

fatemani17 1 year, 4 months ago

user 1 made the tenant.

upvoted 1 times

myarali 1 year, 10 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



Exam AZ-104 All Actual Questions

Question #61

Topic 2

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.

Most Voted

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%)

Comments

NaoVaz **Highly Voted** 2 years, 2 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 27 times

Mazinger **Highly Voted** 1 year, 9 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 9 times

SeMoOoOo0o Most Recent 3 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

AlbertKwan 6 months ago

Selected Answer: A

Finally, the community 100% agreed on a Correct answer.

upvoted 3 times

3c5adce 7 months ago

ChatGPT4 says A

upvoted 1 times

MCLC2021 7 months, 1 week 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 8 months, 1 week 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 3 times

Amir1909 9 months, 3 weeks ago

A is correct

upvoted 1 times

Saurabh_Bhargav 10 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 10 months ago

C. Option

upvoted 1 times

NU88 11 months, 2 weeks ago

Is Azure Custom Role a property of a subscription? or it sits above all subscriptions?

upvoted 1 times

AK4U_111 1 year, 9 months ago

Answer is correct

upvoted 1 times

zellck 1 year, 10 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

zelleck 1 year, 10 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] 1 year, 11 months ago

on the test

upvoted 3 times

sourabhg 2 years, 1 month ago

The correct answer is A.

upvoted 1 times

kerimnl 2 years, 3 months ago

Selected Answer: A

Correct Answer is A for sure

upvoted 2 times

libran 2 years, 3 months ago

Selected Answer: A

Correct Answer: A

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #62

Topic 2

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 X

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) (i)

Role	Scope	Group assignment Condition
Reader	Resource group (inherited)	-- None
Storage Blob Data Contributor	This resource	-- Add

Deny assignments (0) (i)

Classic administrators (0) (i)

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. Most Voted
- C. Modify the firewall of storageacct1234.
- D. View blob data in storageacct1234. Most Voted
- E. View file shares in storageacct1234.

Correct Answer: BD

Community vote distribution

BD (99%)

0

Comments

kerimnl Highly Voted 2 years, 3 months ago

Selected Answer: BD

Correct Answer is:BD

upvoted 88 times

pmsiva 2 years, 1 month 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, 3 months ago

Selected Answer: BD

correct answers: BD

upvoted 29 times

cvalladares123 1 year, 5 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, 5 months ago

Azure file shares are deployed into storage accounts so I think it is BDE.
upvoted 6 times

Ben756 1 year, 2 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 3 months 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 1 month, 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

Dankho Most Recent 2 months, 2 weeks ago

I concur it's B and D. After some research I am good with this explanation.

I concur, its 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: BD

WRONG

B & D are correct

upvoted 1 times

Devs84 3 months, 2 weeks ago

Selected Answer: BD

It has to be B and D

upvoted 1 times

CheMetto 4 months, 2 weeks 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 5 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 6 months, 3 weeks ago

Selected Answer: BD

read cannot read file share, because it have not any dataAction

upvoted 1 times

3c5adce 7 months ago

ChatGPT4 says B&D

upvoted 1 times

Vladds 7 months ago

Selected Answer: BD

It has to be B & D. The Reader role is scoped to resource group anyway

upvoted 2 times

Chris17 7 months ago

Selected Answer: BD

correct answers: BD

upvoted 1 times

MCLC2021 7 months, 1 week 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 8 months, 2 weeks ago

This question was in exam 22/03/2024. My response BD
upvoted 4 times

MC420 8 months, 1 week ago

Was it correct?
upvoted 1 times

Amir1909 8 months, 3 weeks ago

B, D and E
upvoted 1 times

1828b9d 9 months, 1 week ago

This question was in exam 01/03/2024
upvoted 3 times

MC420 8 months, 1 week ago

What's the answer?
upvoted 1 times

LovelyGroovey 9 months, 2 weeks 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

LovelyGroovey 9 months, 2 weeks ago

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 1 times



Exam AZ-104 All Actual Questions

Question #63

Topic 2

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" Most Voted
- C. Event | where EventType is "error"
- D. Get-Event Event | where \${_.EventType == "error"}

Correct Answer: B

Community vote distribution

B (100%)

Comments

TheB Highly Voted 1 year, 11 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 8 months, 2 weeks ago

Shouldn't the last one have double 'equal to'?

upvoted 4 times

MCLC2021 Highly Voted 7 months, 1 week 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 combine multiple commands

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 8 times

Mark74 Most Recent 4 days, 14 hours ago

Selected Answer: B

B is correct answer

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

jecampos2 9 months, 3 weeks ago

Selected Answer: B

Correct answer is B

upvoted 1 times

Studyengineering 1 year ago

Will be doing exam next week. If this question isn't in my exam i sue Examtopics :P

upvoted 5 times

pinyonet 1 year, 2 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, 3 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, 6 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

Afcan 1 year, 11 months ago

Event | search "error"

upvoted 2 times

ccemyilmazz 1 year, 11 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 1 year, 11 months ago

BTW, I just saw that "C" is NOT OK, My mistake

upvoted 2 times

khaled_razouk 1 year, 11 months ago

Selected Answer: B

B. Event | search "error"

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #64

Topic 2

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 **Most Voted**
- D. Configure user-level credentials for FTPS

Correct Answer: C

Community vote distribution

C (98%)

A

Comments

Mazinger **Highly Voted** 1 year, 9 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 45 times

lebeyic620 8 months, 2 weeks 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 1 year, 11 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

Mark74 Most Recent 4 days, 14 hours ago

Selected Answer: C

C is correct

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: C

it's C

upvoted 1 times

mojo86 3 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 4 months, 2 weeks 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 5 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 3 times

edurakhan 6 months ago

on exam today 6/6/2024

upvoted 2 times

3c5adce 7 months 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 7 months, 1 week ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/web-and-mobile#website-contributor>

upvoted 1 times

upvoted 2 times

MCLC2021 7 months, 1 week 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 9 months 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

Seppl 9 months ago

good to hear, did you learn with the free version or did you buy all questions?

upvoted 2 times

LinuxLewis 9 months, 1 week 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 8 months, 2 weeks 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 9 months, 2 weeks ago

I believe B is correct.

<https://learn.microsoft.com/en-us/azure/app-service/deploy-ftp?tabs=portal>

upvoted 1 times

Amir1909 9 months, 2 weeks ago

C is correct

upvoted 1 times

stanislaus450 9 months, 4 weeks 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 10 months, 2 weeks ago

100% C is correct

upvoted 1 times

Wojer 10 months, 3 weeks ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/app-service/deploy-configure-credentials?tabs=cli>
from what I see you need to be a contributor anyway for app-level (FTPS) and question is saying least possible access, so contributor anyway, this is how I understand

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #65

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (76%)

A (24%)

Comments

Georgego **Highly Voted** 1 year, 10 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://docs.microsoft.com/en-us/active-directory/fundamentals/identity-data-bulk-upload#bulk-upload-prerequisites>

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#prerequisites>
upvoted 65 times

GreenTick 2 weeks, 1 day 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 1 times

MeysamBayani 1 year, 10 months ago

I think you can add Redirection url [inviteRedirectURL] for all user same <https://myapplications.microsoft.com> so it is possible we use Bulk

upvoted 6 times

rodrod 1 month, 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, 2 months ago

It is correct, redirection URL is not based on the end user, organization can decide

Answer : A

upvoted 3 times

shadad 1 year, 9 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, 2 months ago

B, is correct. Refer to the question, be comprehensive, too much technicality guys.

upvoted 3 times

Muffay Highly Voted 1 year, 11 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 16 times

Mugamed 1 year, 10 months ago

But it doesn't 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 isn't the case.

upvoted 8 times

Highgate 3 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 1 year, 10 months ago

Incorrect

upvoted 2 times

Announcement Most Recent 3 weeks, 1 day 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 1 month 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 1 month, 1 week 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 1 month, 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 2 months, 1 week ago

bulk invite needs names email and redirection url which is missing so the answer is NO

upvoted 1 times

SeMo0o0o0o 3 months, 1 week 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 1 times

demirsamuel 3 months, 1 week ago

it is definitely B -> No.

<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite>

upvoted 1 times

1a8ca01 3 months, 3 weeks ago

Today, there is also a Bulk invite users option in Entra ID.

<https://learn.microsoft.com/de-de/entra/external-id/tutorial-bulk-invite>

upvoted 1 times

1964L84Fulie 4 months, 1 week ago

The Answer is Yes. Replace Azure Active Directory with Microsoft Entra ID and you will find the Bulk template only needs the User Name and Service Principal (email). Question needs to be updated to contain the correct terms and answers.

upvoted 3 times

Elaheh_Ghaffari12533 5 months, 2 weeks ago

the answer is :yes

tested in azure portal according to this link :

<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite>

upvoted 3 times

rodrod 1 month, 1 week ago

your link confirms it's a NO:

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.

upvoted 1 times

maki999 6 months, 1 week ago

Selected Answer: A

Using the Bulk invite users operation in Azure Active Directory allows you to import a CSV file to create guest user accounts for multiple external users. This operation is specifically designed to handle scenarios where you need to invite a large number of external users (like your 500 users) as guest users in your Azure AD tenant.

upvoted 2 times

Chris17 7 months ago

Selected Answer: B

The answer is B.

From Microsoft doc. about bulk say email address and redirection url is required.

<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite#prerequisites>

upvoted 1 times

36eeabb 7 months ago

Selected Answer: B

If you don't specify email or Redirection URL: you get error: "The csv file you uploaded is not valid".

upvoted 1 times

MCLC2021 7 months, 1 week ago

Selected Answer: B

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..

<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite>

upvoted 1 times

Cfernandes 7 months, 2 weeks ago

To create guest user accounts in bulk in Azure AD, you can follow the proper procedure.

-Go to the Azure portal and go to Azure Active Directory.

-Select Users and then click Mass Invite Users.

-On the Bulk Invite User page, you can download a CSV (comma separated values) file that contains the properties of the users

you want to create.

- Open the CSV file and add a line for each external user you want to invite.
- Fill in the required information such as name, email address and other relevant properties.
- Upload the CSV file back to the Azure portal to create the guest users.

This allows you to create multiple guest user accounts at once, saving time and following the principle of least privilege.

Therefore, the solution of using the bulk invite users operation in Azure AD meets your objective.

Answer: A

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #66

Topic 2

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

Correct Answer:

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

Comments

TorresW Highly Voted 1 year, 11 months ago

<https://www.examtopics.com/discussions/microsoft/view/57784-exam-az-500-topic-2-question-58-discussion/>
 i found similar questions in other page

upvoted 26 times

jimmyym1 1 year, 11 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 152 times

shandorcoachman 1 year, 9 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 1 year, 9 months ago

Correcting myself, this is a subscription role.

upvoted 6 times

ChrisEkorhi 1 year, 6 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 test yourself using Azure free account.

upvoted 7 times

Paul_white 1 year, 9 months ago

This is the best answer here!!!

<https://www.examtopics.com/discussions/microsoft/view/57784-exam-az-500-topic-2-question-58-discussion/>
 upvoted 4 times

Panapi 1 year, 9 months ago

Answer is correct Valid! This question was on the exam 22/02/2023. Scored 920. Thanks guys!

upvoted 22 times

Sandip671 1 year, 1 month ago

Hiii my exam are in 10 days plz help me to make my concepts clear

upvoted 1 times

neelito 1 year, 1 month ago

neonstu 1 year, 1 month ago

Sandip671 how your exam? Did you pass it?

upvoted 3 times

ki01 11 months, 3 weeks 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

ElDakhli **Highly Voted** 1 year, 11 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 26 times

Georgego 1 year, 10 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** 1 month, 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 2 months, 1 week ago

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/custom-create>

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

WRONG

Role3: Role1 and built-in Azure subscription roles only

Role4: Role2 only

upvoted 1 times

certainly 3 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 neccessary cloning BOTH.

So correct anwser should

Role3: Role1 only

Role4: Role2 only

upvoted 1 times

certainly 2 months, 2 weeks ago

nvm. i got it now. correct answer

Role3: Role1 and Azure subscription Roles only.

Role4: Role2 only

upvoted 1 times

CheMetto 4 months, 2 weeks 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 4 months, 2 weeks 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 4 months, 2 weeks ago

i was wrong, it was a bug/issue of my tenant. i could do that on another one

upvoted 1 times

ajay01avhad 4 months, 2 weeks 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 6 months, 4 weeks ago

Final Answer:

Role3: Role1 and built-in Azure subscription roles only

Role4: Role2 only

upvoted 3 times

3c5adce 7 months 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 9 months, 3 weeks ago

Role3: Role1 and built-in subscription roles only

Role4: Role2 only

upvoted 4 times

mihir25 1 year 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 Scenraio and it's true that role 3 = role 1 + azure ad role

role 4 = role 2

upvoted 1 times

pradeepbadisa 1 year, 2 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, 2 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, 2 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, 2 months ago

Role3: Role1 and built-in Azure subscription roles only

Role4: Role2 only

upvoted 2 times

oopspruu 1 year, 3 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



Exam AZ-104 All Actual Questions

Question #67

Topic 2

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 roles

Owner
Contributor
Reader and Data Access
Storage Account Contributor

Answer Area

User1:

User2:

Answer Area

Correct Answer: User1: Reader and Data Access

User2: Owner

Comments

Muffay Highly Voted 1 year, 11 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 90 times

mohsanarfandanish Highly Voted 1 year, 8 months ago

Cleared Exam 930 was appeared in exam 18/3/2023 ANS most upvoted

upvoted 19 times

SeMo0o0o0o Most Recent 3 months, 1 week 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 1 times

18c2076 8 months, 4 weeks 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 9 months, 3 weeks ago

Correct

upvoted 1 times

jeru81 10 months, 1 week 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 7 times

MSBITSM 10 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 10 months, 4 weeks ago

This question was in exam 15/01/24

upvoted 3 times

Ahkhan 1 year ago

I got this question today in my exam—11/14 2023.

upvoted 3 times

Azc_T 12 months ago

Did you use free access? Are these questions from free access enough to clear exam.

upvoted 1 times

Rednevi 1 year, 2 months ago

Remember:

Contributor can NOT assign roles

upvoted 2 times

Alandt 11 months, 1 week ago

Exactly, only owner if I'm correct?

upvoted 1 times

fe0b3b4 11 months, 1 week 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 11 months ago

Good point!

upvoted 1 times

Rams786 1 year, 2 months ago

This question was on my exam on 22 Sep 2023. scored 900 i answered most Voted

upvoted 3 times

Azc_T 12 months ago

Did you use free access? Are these questions from free access enough to clear exam

upvoted 1 times

Indy429 11 months, 3 weeks ago

No you should get Contributor access to be able to go through everything, especially the case studies

upvoted 1 times

3c5adce 7 months ago

How do you access the case studies?

upvoted 1 times

rodrod 1 month, 1 week ago

he just explained...

upvoted 1 times

skavichal 1 year, 6 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, 6 months ago

User1: Reader

User2: Storage Account Contributor

upvoted 1 times

18c2076 8 months, 4 weeks 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, 6 months ago

User1: Storage Account Contributor

User2: Owner

upvoted 1 times

18c2076 8 months, 4 weeks 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 1 year, 10 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 1 year, 10 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 more 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 8 months, 4 weeks 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

Ikjsatlwjwwge 1 year, 10 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

Henryjb3 1 year, 11 months ago

Would the second answer be Storage Account Contributor, since it is the least privilege?

upvoted 3 times

Nickouh 1 year, 11 months ago

I think so as its least privilege

upvoted 1 times

VWSAM025 1 year, 10 months ago

Storage account contributor cannot assign roles

upvoted 3 times

KennethLZK 1 year, 10 months ago

The appropriate role should be "User Acess Administrator" but it is not an option. Therefore, the next "least privilege" role would be "Owner".

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.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 3 times

Ashfaque_9x 1 year, 11 months ago

User 1: "Reader and Data Access"

User 2: "Owner"

upvoted 4 times



Exam AZ-104 All Actual Questions

Question #68

Topic 2

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 **Most Voted**
- C. an IP address range

Correct Answer: B

Community vote distribution

B (100%)

Comments

lszy **Highly Voted** 1 year, 11 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 74 times

Muffay **Highly Voted** 1 year, 11 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>

<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

rodrod Most Recent 1 month, 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 3 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

3c5adce 7 months 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 8 months, 3 weeks ago

B is correct

upvoted 1 times

tripleaholic 1 year ago

similar as question 32 on <https://www.examtopics.com/exams/microsoft/az-104/view/51/>

upvoted 1 times

Rams786 1 year, 2 months ago

This question was on my exam on 22 Sep 2023. scored 900 i answered B

upvoted 5 times

rodrod 1 month, 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, 2 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, 2 months ago

Selected Answer: B

B most voted.

upvoted 1 times

Aquintero 1 year, 4 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, 4 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 1 year, 10 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

zellck 1 year, 10 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

zellck 1 year, 10 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

zellck 1 year, 10 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 1 year, 11 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

khaled_razouk 1 year, 11 months ago

Selected Answer: B

To ensure that the virtual machines can access Vault1 while minimizing administrative effort and using the principle of least privilege, you should configure a service tag as the destination of the outbound security rule for NSG1.

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #69

Topic 2

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 **Most Voted**
- C. User1, User2, and User4 only
- D. User1, User2, User3, and User4

Correct Answer: B

Community vote distribution

B (92%)

Other (8%)

Comments

sandorh **Highly Voted** 1 year, 11 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 90 times

suresh0512 1 year, 11 months ago

What about the user4, he is set to none and gets assigned whatever the new role is assigned?

upvoted 3 times

Hull 1 year, 11 months ago

"You assign the Azure Active Directory Premium Plan 2 license to Group1 and User4."

User 4 is assigned the license directly

upvoted 17 times

helixsam Highly Voted 1 year, 11 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 21 times

Dankho 2 months, 1 week 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 1 times

GohanF2 1 year, 8 months ago

Thank you ! I didn't know about the nested groups licenses inheritance

upvoted 3 times

Sholasleek Most Recent 3 weeks, 2 days 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

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corerct

upvoted 1 times

testtaker09 5 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 1 times

testtaker09 5 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 1 times

3c5adce 7 months 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 9 months, 3 weeks ago

B is correct

upvoted 1 times

Ahkhan 1 year ago

I got this exact question on my exam today on 11/14/2023.

upvoted 2 times

iamchoy 1 year, 2 months ago

Selected Answer: B

This is correct

upvoted 1 times

AntaninaD 1 year, 3 months ago

Got this question on 09/09/23

upvoted 2 times

CarlosMarin 1 year, 3 months ago

This question was in my exam on 31/08/2023.

upvoted 3 times

ecliptor 1 year, 4 months ago

Estava no exame 28/07/23

upvoted 2 times

Mehedi007 1 year, 4 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 2 months, 1 week 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

NavigatiOn 1 year, 4 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, 5 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

xRiot007 1 year, 6 months ago

Answer: B. Reason: User 4 is assigned the licence directly. User 1 is the only user part of Group 1. Because licences do not propagate to nested groups, other users will not receive such licences even if their group is a member of Group 1.

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #70

Topic 2

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: package1
Description: Guest users
Catalog name: General

Resource roles

Resource	Type	Sub Type	Role
Group1	Group and Team	Security Group	Member

Requests

Users who can request access: All configured connected organizations
Require approval: No
Enabled: Yes

Requestor information

Questions

Question	Answer format	Multiple choice options	Required
----------	---------------	-------------------------	----------

Attributes (Preview)

Attribute type	Attribute	Default display string	Answer format	Multi
Lifecycle				
Access package assignments expire		After 365 days		
Require access reviews		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. Yes No

After 365 days, fabrikam.com users will be removed from Group1. Yes No

After 395 days, fabrikam.com users will be removed from the contoso.com tenant. Yes No

Statements

Yes	No
-----	----

Litwareinc.com users can be assigned to package1. Yes No

Correct Answer: After 365 days, fabrikam.com users will be removed from Group1. Yes No

After 395 days, fabrikam.com users will be removed from the contoso.com tenant. Yes No

Comments

PlaceboC6 Highly Voted 1 year, 9 months ago

N - Because not Connected

Y - Because when it expires it is removed from the group. Proof to follow

X - Because none

y - Because..matn

<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 141 times

a6bd45e 4 months, 4 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

3c5adce 7 months ago

Confirmed

upvoted 1 times

AK4U_111 1 year, 9 months ago

After reading this article, i would say NYY is correct.

Thank you

upvoted 9 times

Indy429 11 months, 3 weeks ago

But this example states that the users will not immediately be removed after the expiration of their access package. This will happen after 30 days of expiration, which would be after 395 days, not 365 days. In this case if you base it off the example, the answers should be

N

N

Y

Comprehensive reading is just as important as technical knowledge guys.

upvoted 19 times

rnd3131 10 months, 4 weeks ago

the group 1 will be removed directly after 365 day, the EXT USER will be removed from the DIRECTORY (tenant) after 395 days.

as described in the article of PlaceboC6:

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.

upvoted 6 times

Ruby1133299 Highly Voted 1 year, 11 months ago

N not a connected organisation

N expired not remove

Y 365 + 30 = 395 removed

upvoted 99 times

RougePotatoe 1 year, 10 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 1 year, 10 months ago

I mis-read the question. I still wish people would cite their sources though.

upvoted 6 times

Indy429 11 months, 3 weeks 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 1 month, 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 1 month, 2 weeks ago

sorry N Y Y

upvoted 1 times

behradclid 3 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 1 times

SeMo0o0o0o 3 months, 1 week ago

WRONG

No

No

Yes

upvoted 1 times

varinder82 6 months, 4 weeks ago

Final Answer:

N not a connected organisation

N expired not remove

Y $365 + 30 = 395$ removed

upvoted 4 times

3c5adce 7 months ago

ChatGPT4 says No no no

upvoted 1 times

2fd1029 3 months, 2 weeks ago

We don't care what ChatGPT says. ChatGPT gets questions wrong all the time.

upvoted 4 times

SkyZeroZx 11 months, 1 week 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 14 times

Jedi_sg2000 5 months, 2 weeks ago

that make sense!

upvoted 1 times

hebbo777 1 year 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>

V - $365 + 30 = 395$ deleted

1 - 365+30 = 395 deleted.

upvoted 3 times

katrvintraiz 1 year, 1 month ago

The answer

https://www.youtube.com/watch?v=J136cq9r0u8&list=PLIKA5U_Yqgof3H0YWhzvarFixW9QLTr4S&index=53

upvoted 8 times

ziggy1117 1 year, 1 month 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, 1 month ago

sorry should be N-Y-Y

upvoted 4 times

amsioso 1 year, 1 month 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 6 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, 1 month 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, 2 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, 1 month 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 2 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."

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, 2 months ago

NNY makes sense, but why is Y marked with red in 1 ?

upvoted 1 times

oopspruu 1 year, 3 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, 4 months ago

NNY

1- Not a connected organization

2. Expired no remove

3. $365 + 30 = 395$ = removed

upvoted 7 times



Exam AZ-104 All Actual Questions

Question #71

Topic 2

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?

- Assign User1 the Network Contributor role for VNet1.
- Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- Assign User1 the Owner role for VNet1. **Most Voted**
- Assign User1 the Network Contributor role for RG1.

Correct Answer: C

Community vote distribution

C (100%)

Comments

myarali **Highly Voted** 1 year, 10 months ago

Selected Answer: C

There is only two choices for that purpose;

- Assign User1 the Owner role for VNet1.
 - Assign User1 the User Access Administrator role for VNet1.
- upvoted 25 times

Mark74 **Most Recent** 4 days, 15 hours ago

Selected Answer: C

C seems correct for me

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: C

C is corerct

upvoted 2 times

3c5adce 7 months, 2 weeks 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 5 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 3 times

tashakori 8 months, 3 weeks ago

C is right

upvoted 2 times

Nick111111 1 year, 4 months ago

I did see this on the exam

upvoted 4 times

Notteb 1 year, 10 months ago

Selected Answer: C

C. seems correct

upvoted 2 times

Ni33 1 year, 10 months ago

C is correct. It is the only role in the give options have capability to assign permissions.

upvoted 2 times

zellck 1 year, 10 months ago

Same as Question 53.

<https://www.examtopics.com/discussions/microsoft/view/74021-exam-az-104-topic-2-question-53-discussion>

upvoted 3 times

zellck 1 year, 10 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 1 year, 10 months ago

C is correct only Owner can assign roles (even reader role).

upvoted 1 times

Mo22 1 year, 10 months ago

Selected Answer: C

Correct

upvoted 1 times

Georgego 1 year, 10 months ago

Selected Answer: C

Answer is correct.

upvoted 1 times

Exam AZ-104 All Actual Questions

Question #72

Topic 2

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

Search (Ctrl+ /)

Add Download role assignments Edit columns Refresh Remove

Overview Activity log Access control (IAM) Tags Resource visualizer Events Settings Deployments

Check access Role assignments Roles Deny assignments Classic administrator

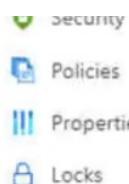
Number of role assignments for this subscription ①

2	2000
---	------

Search by name or email Type : All Role : All Scope : All

2 items (1 Users, 1 Groups)

Name	Type	Role	Scope	Condition
Owner				



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		
Correct Answer:	Statements	Yes
	You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	<input type="radio"/>
	You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	<input type="radio"/>
	You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for	<input checked="" type="radio"/>

Comments

HenriksDisciple Highly Voted 1 year, 10 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 109 times

JimmyYop 1 year, 9 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 12 times

3c5adce 7 months ago

Confirmed by ChatGPT4
upvoted 1 times

AndreaStack 1 year, 10 months ago

me too but... where you found yours instead?

upvoted 3 times

o0o0 1 year, 3 months ago

Just test and did not have your results.
1- Yes

2- No

3- No

upvoted 8 times

tableton 8 months, 1 week ago

My test had this results too

upvoted 1 times

hebbo777 1 year ago

agree, i tested first point is yes, 2&3 Office 365 not supporting membership

upvoted 2 times

LauLauLauw Highly Voted 1 year, 10 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 58 times

SanSoni 6 months, 4 weeks ago

I tested and confirm it

upvoted 1 times

eduardokm 1 year, 7 months 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 1 year, 10 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 1 year, 8 months ago

they are azure ad role enabled. nesting is not supported

upvoted 2 times

daws08322 1 year, 9 months ago

There is a difference with adding a group and assigning a role by adding a group.

upvoted 3 times

b411470 Most Recent 1 week, 6 days 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

Chuong0810 1 month 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

radrad 1 month, 1 week ago

rourou 1 month, 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 1 month, 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 1 times

jamesf 1 month, 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 3 times

SeMo0o0o0o 3 months, 1 week ago

CORRECT

upvoted 1 times

a_786_b 3 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.
- 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.
- 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 3 times

CheMetto 4 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 6 months, 1 week 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 8 months, 3 weeks ago

Given answer is right

upvoted 1 times

Amir1909 9 months, 3 weeks ago

No

No

Yes

upvoted 1 times

ITpower 10 months, 3 weeks ago

well first one is yes

second one is no cuz the group3 type is not security so it can not be used for the assigning roles in azure RBAC.

last one is yes if you want to modify the assigning role to the user3 as the owner and assign the group3 as the security type then of course in th RG1 you can assign user3 the owner role by assigning the owner role to group3 . i tested but here in this site there are many questions which are wrong so you have to test by yourself before proceeding to the answer.

upvoted 2 times

Ishraj 11 months ago

Yes - Nesting is indeed possible for Azure RBAC, not to be confused to Entra Id RBAC.

No. Microsoft 365 groups cannot be nested under a security group in Entra Id.

No Microsoft 365 groups cannot be added in Role assignment in Azure.

upvoted 4 times

gilbertlelancelo 10 months, 3 weeks ago

That's is the correct one!

upvoted 2 times

SkyZeroZx 11 months, 1 week ago

1. N - Adding as a member to a group won't inherit/share access privileges.

2. N - Adding as a member to a group won't inherit/share access privileges.

3. Y

upvoted 2 times

[Removed] 11 months, 3 weeks ago

I have tested this and I am not sure where you guys are getting Y N N.

When you assign Group1 to RG1 as Owner, the members of Group1 (in this case User1) will have Owner access. When you assign Group2 to Group1 and check access for User2, this user doesn't inherit the access from Group1.

When you try to assign User3 as the owner of RG1 by adding Group3 as a member of Group1 you simply can't, the option is greyed out and it tells you M365 groups are not supported.

If you assign Group3 the Owner role directly on RG1, User3 will then inherit the access. It is supported, do not mistake thinking M365 groups cannot be assigned access levels via IAM.

So the correct answer is N, N, Y. Do yourself a favor and ignore everyone saying anything else.

upvoted 13 times

etrop 4 months ago

Dude i have whole environments setup where I have nested groups everywhere and use them for RBAC, what did you test exactly? Are you sure you waited like at least 5mins for everything to sync. The nested group setup takes longer to take effect.

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #73

Topic 2

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. **Most Voted**

C. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.

D. Assign User1 the Contributor role for VNet1.

Correct Answer: B

Community vote distribution

B (100%)

Comments

Mark74 4 days, 15 hours ago

Selected Answer: B

B is correct

upvoted 1 times

phantom31 2 months, 3 weeks ago

Why filling up with repetitions just to increase question number?

upvoted 3 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

3c5adce 7 months, 2 weeks 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 6 months, 3 weeks ago

Contributor role does not allow you to assign roles

upvoted 5 times

GoldenDisciple2 1 year, 3 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, 4 months ago

AK4U - stop! LOL

upvoted 1 times

ASKBO 1 year, 5 months ago

Same with topic 2 question 5

upvoted 2 times

myarali 1 year, 9 months ago

Selected Answer: B

B is the answer.

upvoted 2 times

AK4U_111 1 year, 9 months ago

if they were all that easy, everyone would be certified :-)

upvoted 4 times

zellick 1 year, 10 months ago

Same as question 71.

<https://www.examtopics.com/discussions/microsoft/view/95675-exam-az-104-topic-2-question-71-discussion>

upvoted 3 times

zellick 1 year, 10 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 1 times

Nzudin 1 year, 10 months ago

YES THE ANSWER IS B

upvoted 1 times

examkiddos 1 year, 10 months ago

Selected Answer: B

B seems fine

upvoted 4 times



Exam AZ-104 All Actual Questions

Question #74

Topic 2

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 Most Voted
- C. a network security group (NSG)
- D. Azure Virtual WAN

Correct Answer: B

Community vote distribution

B (99%)

Comments

hevfe01 Highly Voted 1 year, 10 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."

<https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

LINK: <https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>
upvoted 37 times

shadad Highly Voted 1 year, 9 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 25 times

Joyerific 6 months ago

so if you already passed, why are you on here studying the practice questions?
upvoted 6 times

nailedIT 4 months, 1 week ago

Bots everywhere :D
Always the same sentence structure
upvoted 4 times

Mark74 Most Recent 4 days, 15 hours ago

Selected Answer: B

B is correct
upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corerct
upvoted 1 times

Amir1909 8 months, 3 weeks ago

B is correct
upvoted 2 times

iamchoy 1 year, 2 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, 3 months ago

This question was in my exam on 31/08/2023.
upvoted 2 times

kioks23 1 year, 3 months ago

I don't believe you. You are spamming every question with this reply
upvoted 14 times

behradcid 3 months ago

maybe he didnt pass the exam and he's here for practice again, come on don't judge people
upvoted 1 times

Mahedinn7 1 year, 4 months ago

MeneGivoV 1 year, 4 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, 4 months ago

Estava no exame hoje

upvoted 2 times

allyQ 1 year, 9 months ago

B: Take the VPN / VPN Gateway resources out of the question and the answer would be the same.

upvoted 1 times

Takate 1 year, 9 months ago

VPN is not part of Az-104 exam right ?

upvoted 1 times

allyQ 1 year, 9 months ago

It is, but I dont think its a VPN question.

upvoted 2 times

insanewriters 1 year, 9 months ago

It is.

upvoted 2 times

UmbongoDrink 1 year, 10 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 1 year, 10 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 1 year, 10 months ago

is it new question?

upvoted 3 times

shadad 1 year, 9 months ago

Yes it is and the answer is B Private endpoints

upvoted 1 times

examkiddos 1 year, 10 months ago

Selected Answer: D

Optimized routing using the Microsoft global network

<https://azure.microsoft.com/en-us/products/virtual-wan>

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #75

Topic 2

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
User1 can create a storage account in RG1.

Yes	No
<input checked="" type="checkbox"/>	<input type="radio"/>

Correct Answer:

User1 can modify the DNS settings of networkinterface1.

User1 can create an inbound security rule to filter inbound traffic to networkinterface1.

**Comments**

skydivex Highly Voted 1 year, 10 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 93 times

3c5adce 7 months ago

Confirmed by ChatGPT4

upvoted 3 times

Chris76 1 year, 7 months 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 24 times

deroid 1 year, 2 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 10 times

sardonicque 1 year, 2 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 10 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 2 times

umavaja 10 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

Chris76 1 year, 7 months ago

Ok I have tested this as its controversial as fk. You can indeed create new storage accounts with the SA Contribute role.

Confusion came after the identical experiment with the Logic App Contributor role. As for that one you cannot create logic apps due to lack of a write permission. Despite the docs saying Microsoft.Logic/*

upvoted 14 times

Toast1536 1 year, 4 months ago

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#classic-storage-account-contributor>

Classic Storage Account Contributor

Lets you manage classic storage accounts, but not access to them.

Actions Description

Microsoft.Authorization/*/read Read roles and role assignments

Microsoft.ClassicStorage/storageAccounts/* Create and manage storage accounts

Microsoft.Insights/alertRules/* Create and manage a classic metric alert

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.Support/* Create and update a support ticket

upvoted 1 times

RickySmith 1 year, 3 months ago

But the assignment is for Storage Account Contributor, not Classic Storage Account Contributor.

upvoted 2 times

RickySmith 1 year, 3 months ago

Correction. Both can create storage accounts.

upvoted 1 times

zellck Highly Voted 1 year, 10 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 22 times

Stunomatic Most Recent 1 month, 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

SeMo0o0o0o 2 months, 1 week ago

CORRECT

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

CORRECT

upvoted 1 times

tcoelho28 4 months ago

Correct Answers. No, No, Yes

NO - Storage Account Contribute 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 4 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 5 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 6 months, 4 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 1 times

Wassel_Laouini 7 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 7 months, 3 weeks 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 2 times

Amir1909 8 months, 3 weeks ago

Given answer is right

upvoted 1 times

bacana 9 months, 1 week ago

User1 has role assignments for NSG1 not for RG. He can't create storage account.

upvoted 1 times

18c2076 8 months, 4 weeks ago

His Storage Account Contributor role is inherited down from the RG. Read again. Try again. You failed.

upvoted 2 times

BluAlien 8 months ago

.. and where is specified that NSG1 is in RG1 ? Nowhere, noway NNY

upvoted 1 times

Amir1909 9 months, 3 weeks ago

Yes

No

Yes

upvoted 1 times

Atom270 10 months, 2 weeks ago

Yes no yes

upvoted 2 times

devops_devops 10 months, 4 weeks ago

This question was in exam 15/01/24

upvoted 2 times

SkyZeroZx 11 months, 1 week 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 3 times



Exam AZ-104 All Actual Questions

Question #76

Topic 2

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. **Most Voted**

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%)

Comments

yettie79 **Highly Voted** 1 year, 8 months 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

gogel **Highly Voted** 1 year ago

Shouldn't this be "User" Access Administrator?

upvoted 12 times

Mark74 Most Recent 4 days, 14 hours ago

Selected Answer: B

B is correct

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corecrt

upvoted 1 times

tfdestroy 11 months, 3 weeks 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, 3 months ago

Selected Answer: B

I would go for the B

upvoted 1 times

Athul07 1 year, 6 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 12 months ago

Sorry, this is wrong. The correct answer is B - Access Administrator role.

upvoted 1 times

al_john 11 months, 1 week ago

The "Contributor" not permit access permission !

upvoted 1 times

xRiot007 1 year, 6 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 1 year, 8 months ago

Selected Answer: B

Selected Answer: B

upvoted 2 times

myarali 1 year, 9 months ago

Selected Answer: B

You need User Administrator Role for assigning the Reader role to User1 for VNet1

upvoted 2 times

WreckIT 1 year, 9 months ago

Selected Answer: B

B. Assign User1 the Access Administrator role for VNet1.

upvoted 4 times



Exam AZ-104 All Actual Questions

Question #77

Topic 2

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

Statements

The Group1 members can view the configurations of the Azure functions.

Yes

No

Correct Answer:

User1 can assign the Owner role for RG1.



User1 can create a new resource group and deploy a virtual machine to the new group.



Comments

Shadowner Highly Voted 1 year, 9 months 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 69 times

Slimus 1 year, 6 months ago

3rd - Yes. it's says "You assign User the Virtual Machine Contributor role for Sub1 and Sub2."

upvoted 4 times

kam1122 1 month, 1 week ago

No, user cannot create RG

upvoted 1 times

090200f 6 months, 1 week ago

neither and nor.. so not able to create new resources

upvoted 1 times

Simplon 8 months, 2 weeks ago

No, User has only the Virtual Machine Contributor role for Sub1 and Sub2 but not to create a new RG before.

upvoted 4 times

Chris76 1 year, 7 months ago

Group1 is not said to be under MG1. And not associated with any subscriptions. So why you think first answer is Y ?

upvoted 4 times

AN79 1 year, 7 months ago

It clearly states Group1 is assigned Reader role at the MG1 Scope

upvoted 13 times

Indy429 11 months, 3 weeks ago

I agree

upvoted 2 times

garmatey Highly Voted 1 year, 8 months 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, 1 month 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 1 times

upvoted 1 times

ajdann 1 year, 3 months ago

That is exactly the point of User Access Administrator

upvoted 1 times

skeleto11 1 year, 5 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, 2 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

Chuong0810 Most Recent 1 month 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

SeMo0o0o0o 3 months, 1 week ago

CORRECT

upvoted 1 times

etrop 4 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 configuration 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 1 times

3c5adce 7 months ago

ChatGPT4 says all yes

upvoted 1 times

Mentalfloss 4 months, 2 weeks ago

ChatGPT appears to be wrong quite often.

upvoted 4 times

3c5adce 7 months 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 5 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 2 times

Wassel_Laouini 7 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 8 months, 3 weeks ago

Given answer is right

upvoted 1 times

18c2076 8 months, 4 weeks 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 4 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 9 months, 1 week ago

This question was in exam 01/03/2024

upvoted 3 times

Amir1909 9 months, 3 weeks ago

Correct

Yes

Yes

No

upvoted 1 times

User65567473 10 months ago

Was on exam 11/2 /2024

upvoted 4 times

MGJG 1 year, 3 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, 3 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, 3 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

blackwhites 1 year, 6 months ago

Answer YYN

"The Group1 members can view the configurations of the Azure functions." - True. As Group1 members have Reader access at

the management group level, they can view all resources in the management group, including the Azure functions in RG1.

"User1 can assign the Owner role for RG1." - True. As a User Access Administrator for MG1, User1 can manage access to all resources in the management group. This includes assigning any role, including the Owner role, to any resource within MG1, which includes RG1.

"User1 can create a new resource group and deploy a virtual machine to the new group." - False. The Virtual Machine Contributor role allows User1 to manage virtual machines, but it does not provide permissions to create new resource groups. Additionally, User Access Administrator and Reader roles do not grant permission to create resources or resource groups. To perform this task, User1 would need to be assigned a role with resource creation permissions, such as the Contributor role.

upvoted 8 times

TestKingTW 1 year, 6 months ago

the answer is YYY.

the last one is because user has Virtual Machine Contributor role, which is sufficient to create VM and resource group.
It has "Microsoft.Resources/deployments/**"permission, see the docs:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

upvoted 2 times

Yodao 1 year, 6 months ago

Yup you are right, whole thing changes with that line of virtual contributor role.

upvoted 1 times

Mahbus 1 year, 6 months ago

Virtual Machine Contributor role can't create Resource Groups.

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 2 times

aws_arn_name 1 year, 6 months ago

i think here is the action can create resource group "Microsoft.Resources/subscriptions/resourcegroups/deployments/**" . Action "Microsoft.Resources/deployments/**" only state "Create and manage a deployment"

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #78

Topic 2

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. **Most Voted**
- 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: A

Community vote distribution

A (52%)

D (48%)

Comments

macrawat Highly Voted 1 year, 8 months 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 111 times

yettie79 1 year, 8 months 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 1 year, 7 months ago

Correct. Did the same. Very tricky. But this is the right answer.

upvoted 2 times

garmatey 1 year, 6 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 11 months, 3 weeks 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 1 year, 8 months 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

qrlkaidhn 1 year, 5 months ago

so, it says the fist step is "authentication for the storage account." that means 3 is correct.

upvoted 1 times

mfalkjunk Highly Voted 1 year, 8 months 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, 7 months ago

kkkkkkkkkkkkkkkk

upvoted 2 times

maxsteele 1 year, 2 months ago

lol you cant trust ChatGPT to be truthful.

upvoted 18 times

Mark74 Most Recent 4 days, 14 hours ago

Selected Answer: A

A for me is correct

upvoted 1 times

JPA210 1 month ago

Selected Answer: A

Definetly A is the correct answer. That is the first step

Demney A is the correct answer. That is the first step.

upvoted 1 times

Yooooom 1 month, 3 weeks ago

Selected Answer: A

The answer is A

upvoted 1 times

jamesf 1 month, 3 weeks ago

Selected Answer: A

Should be A enable identity-based authentication 1st,
then only go to D, IAM

upvoted 1 times

jamesf 1 month, 3 weeks ago

I prefer A then D

upvoted 1 times

minura 2 months, 1 week ago

Selected Answer: A

To assign User1 the Storage File Data SMB Share Contributor role for share1 (a file share in storage1), you first need to enable identity-based data access for file shares in storage1. This is required so that you can use Azure AD-based authentication for accessing the file shares.

Once identity-based access is enabled, Azure Active Directory (Azure AD) users like User1 can be assigned roles such as Storage File Data SMB Share Contributor to control access to Azure file shares.

You will eventually need to assign the role to User1 using IAM, but first, you must enable identity-based access to the file shares.

upvoted 2 times

117b84e 2 months, 2 weeks ago

chatgpt

To assign User1 the Storage File Data SMB Share Contributor role for share1, the first step is to ensure that Azure Active Directory (AD)-based authentication is enabled for the file shares. This allows Azure AD users to be authenticated when accessing the file shares using SMB.

In this scenario, the correct action to perform first is:

A. Enable identity-based data access for the file shares in storage1.

Explanation:

Azure Files supports Azure AD-based access control for file shares using SMB. However, before you can assign roles like Storage File Data SMB Share Contributor, you need to enable identity-based access for the file shares within the storage account (storage1 in this case).

Once identity-based access is enabled, you can then assign roles such as Storage File Data SMB Share Contributor to Azure AD users like User1, granting them the necessary permissions on share1.

upvoted 1 times

b35c3ef 3 months ago

I think I'm going to go with A based on the following information I found when I search the differences between identity-based access and access control IAM:

Identity and Access Management (IAM)

IAM is a cybersecurity discipline that manages how users access digital resources and what they can do with them. IAM systems verify users' identities and ensure that they have the correct permissions to do their jobs. IAM can also integrate with AI-based cybersecurity tools to analyze data for potential cyber attacks.

Access control

Access control is a data security process that manages who has access to corporate data and resources. Access control uses policies to verify users' identities and grant them the appropriate level of access. Access control is important for applications that have different levels of authorization for different users.

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: A

it's A as the first step

D comes next

upvoted 1 times

Thisisacat 4 months, 2 weeks ago

It should be D.

In the lab, I created following :

1. A user
2. A new storage account
3. A new file share.

Then, I went to file share > IAM > Add role assignment > Members > (newly created user) > Role > (search for given role) > select > review+assign > done.

No error, nothing.

upvoted 2 times

ajay01avhad 4 months, 2 weeks ago

A. Enable identity-based data access for the file shares in storage1

upvoted 1 times

Y2 4 months, 3 weeks ago

Selected Answer: D

Tested - Was able to assign the role in Access Control (IAM) without enabling identity-based authentication.

upvoted 6 times

Makoporosh 5 months ago

A is correct key words are what should you do first, A is done first before D.

upvoted 1 times

Dicer 5 months, 3 weeks ago

Selected Answer: D

Answer is D.

Stop saying A.

It is very clear in Microsoft Documentation (<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>)

Step 2: Open the Add role assignment page (Answer D)

Step 3: Select the appropriate role (Answer A)

upvoted 4 times

LearnerFL 6 months ago

Selected Answer: D

To assign the SMB Share Contributor role to user1 for Share1, you can follow these steps:

1. Go to the Azure portal: Log in to your Azure portal.
2. Navigate to the storage account: Browse to the storage account (storage1) that contains the file share (Share1) you created previously.
3. Select Access Control (IAM): This is where you can manage access to your resources.
4. Add a role assignment: Select '+ Add', then select 'Add role assignment' from the drop-down menu.
5. Select the role and assign it to the user: In the 'Add role assignment' blade, select the 'Storage File Data SMB Share Contributor' role from the Role list. Then, in the 'Select members' field, search for and select user1.
6. Review and assign: Review the role assignment details and then click 'Assign'.

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #79

Topic 2

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. **Most Voted**
- 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 (96%)

A

Comments

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

many time repeated question

upvoted 22 times

Shadowner **Highly Voted** 1 year, 9 months ago

Selected Answer: B

B is indeed correct.

Only User Access Administrator role and Owner role can assign permissions.

upvoted 9 times

Mark74 Most Recent 4 days, 14 hours ago

Selected Answer: B

B for me is correct

upvoted 1 times

minura 2 months, 1 week ago

Selected Answer: B

you need to assign the User Access Administrator role.

upvoted 1 times

SeMo0o0o0o 3 months, 1 week ago

Selected Answer: B

B is corerct

upvoted 1 times

No_Restaurant9617 4 months 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 4 months 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 9 months, 2 weeks ago

This question comes up a good bit on the site lol.

upvoted 3 times

Hi_09 10 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

BluAlien 10 months, 2 weeks 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 12 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 12 months ago

<https://ior.ad/8IDA?iframeHash=viewsteps>

upvoted 1 times

Studyengineeringe 1 year ago

Selected Answer: B

Repetitive question. This one must be simply on my exam next week :D

Repetitive question. This one must be simply on my exam next week.

upvoted 3 times

GoldenDisciple2 1 year, 3 months ago

I hope that the AZ-104 is just different variations of this question 60 times.

upvoted 7 times

oopspruu 1 year, 3 months ago

This question has appeared too many times. It better be on the exam now lol

upvoted 3 times

GoldenDisciple2 1 year, 3 months ago

I know right. lol I hope it's on the exam at least 10 times.

upvoted 1 times

TonySuccess 1 year, 5 months ago

I used to be a question, but now I am the answer

upvoted 6 times

GoldenDisciple2 1 year, 3 months ago

LMAO hilarious

upvoted 2 times

IT_Guy23 1 year, 8 months ago

This same question appears many times

upvoted 1 times

obaali1990 1 year, 8 months ago

Maybe you will meet it in the exams

upvoted 1 times

WreckIT 1 year, 9 months ago

Selected Answer: B

B. Assign User1 the User Access Administrator role for VNet1.

upvoted 5 times



Exam AZ-104 All Actual Questions

Question #80

Topic 2

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

Off

On

Azure Active Directory Premium P2

Off

On

Microsoft Azure Multi-Factor Authentication

Off On

Microsoft Defender for Cloud Apps Discovery

Off On

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

Correct Answer:	Statements	Yes	No
	You can assign User1 the Microsoft Defender for Cloud Apps Discovery license.	<input type="radio"/>	<input checked="" type="checkbox"/>
	You can remove the Azure Active Directory Premium P2 license from User1.	<input checked="" type="checkbox"/>	<input type="radio"/>
	User2 is assigned the Azure Active Directory Premium P2.	<input checked="" type="checkbox"/>	<input type="radio"/>

Comments

ExamHelp22 Highly Voted 1 year, 7 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 117 times

RickySmith 1 year, 4 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 Dev license by a group. After it was assigned for a while, I went in and assigned the user the same license directly and then switched 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 correct answers should be as below.

- 1) Y. Additional licenses can be assigned on top of a group assignment with a cumulative result.
- 2) N. The licenses are 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 10 times

nmshrw 11 months, 2 weeks ago

question clearly states license is 'NOT' ASSIGNED DIRECTLY VIA GROUP BASED LICENSING'

upvoted 2 times

Soudenh 1 month, 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 4 months, 2 weeks ago

Answer is NNN, tested in LAB

upvoted 9 times

Slimus 1 year, 6 months ago

1st is also NO. Microsoft Defender for Cloud Apps Discovery license is OFF.

upvoted 15 times

Mshaty 2 months, 1 week ago

the question is asking if you can assign (if you can turn it on) from my understanding so Yes you can

upvoted 1 times

aaqibkhan123 22 hours, 37 minutes ago

The exhibit shows the current configuration, why are you assuming that it could be turned on? You need to follow the instructions rather than blind assumptions.

upvoted 1 times

ggogel 1 year ago

But you CAN assign it to individual users even if its turned off at the group level. Read the question properly!

upvoted 5 times

suddin1 6 months, 2 weeks ago

ChatGPT says you can't if it is turned off at group level

upvoted 2 times

bp_a_user 1 year, 6 months ago

Isn't it possible to assign the license to an individual user?

upvoted 2 times

KingBarney 1 year, 1 month ago

If you're referring to User 2, it's not asking if User 2 CAN be assigned the license, but if User 2 IS assigned the license. Only Group 1 was assigned the license, members of Group 2 wouldn't get assigned the licenses because nested groups don't inherit licenses.

upvoted 1 times

Exilic Highly Voted 1 year, 6 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

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 55 times

Yodao 1 year, 6 months ago

You are correct because defender is already off for assignment .

upvoted 3 times

xian05 1 year, 3 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, 2 months ago

you cant trust AI sources. They are not reliable sources of factual information

upvoted 10 times

00o0 1 year, 3 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 2 times

hebbo777 1 year ago

question given you a scenario to work on it not can and doing your out of the box workaround!

upvoted 2 times

gogel 1 year 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 9 times

sca88 Most Recent 3 weeks, 4 days 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 explaination, 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 2 times

Chuong0810 1 month 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 1 times

jamesf 1 month, 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

SeMo0o0o0o 3 months, 1 week ago

WRONG

No

No

No

upvoted 1 times

CheMetto 4 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 5 months ago

NNN is the answer!

upvoted 1 times

Jedi_sg2000 5 months ago

1 - the option is greyed out.. you are unable to do it

upvoted 1 times

varinder82 6 months, 2 weeks ago

Final Answer : YNN

upvoted 1 times

Joseeph 6 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 1 times

ssky 7 months, 1 week 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 7 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 7 months, 1 week ago

what is the correct answer?

upvoted 1 times

Amir1909 8 months, 3 weeks ago

Yes

No

No

upvoted 1 times

bhagyashree11 9 months, 2 weeks ago

This is very frustrating, why examtopics didnt added correct answers. For every question there is conflict answers in comment

upvoted 9 times

GlixRox 6 months ago

because the answers are *free*

upvoted 1 times

Amir1909 9 months, 3 weeks ago

Yes

No

No

upvoted 1 times

ITpower 10 months, 3 weeks ago

three of them NOOOO i tested already

upvoted 6 times

TripleFires 10 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/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.
- When a user inherits a license from a group, you can't directly remove or modify that license in the user's properties. You can change the license assignment only in the group and the changes are then propagated to all group members.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #81

Topic 2

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

JobTitle:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Correct Answer:

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

Comments

JeremyChainsaw Highly Voted 1 year, 4 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 53 times

maxsteele 1 year, 2 months ago

so the correct answer is:

1 and 3
and
1,2, and 3
is that correct?

upvoted 20 times

LPaul Highly Voted 1 year, 1 month 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 21 times

RanPo 3 months ago

the best explanation so far

upvoted 1 times

op22233 7 months, 2 weeks ago

Thank you for the understanding you brought.

upvoted 2 times

SeMo0o0o0o Most Recent 3 months ago

CORRECT

upvoted 1 times

deathazul 9 months, 2 weeks 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 11 months, 2 weeks 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 8 months ago

10k/year raise
upvoted 2 times

18c2076 8 months, 4 weeks ago

the answer here is almost always due to company only benefit.
upvoted 1 times

SQL_Student 11 months, 2 weeks 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, 2 months ago

Nice question
upvoted 2 times

Mehedi007 1 year, 4 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 9 times

antropaws 1 year, 4 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, 4 months ago

Disregard.
upvoted 2 times

shiraghami 1 year, 3 months ago

But User 1 and User 3 don't have On-Premises sync enabled
upvoted 4 times

cvalladares123 1 year, 4 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, 5 months ago

Found this Q in the exam, 3/7/23
upvoted 7 times

efayed 1 year, 5 months ago

<https://www.examtopics.com/discussions/microsoft/view/38424-exam-az-104-topic-2-question-32-discussion/>
upvoted 10 times

fessebook 1 year, 4 months ago

Not exactly the same question.
upvoted 2 times

alexvv89 1 year, 3 months ago

I believe it's pretty much the same questions.
JobTitle: User1 and User3
UsageLocation: all Users
upvoted 2 times

Codelawdepp 1 year, 3 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, 5 months ago

JobTitle can't be changed in AD in hybrid setup
upvoted 4 times

antropaws 1 year, 4 months ago

Where does it say so?
upvoted 1 times

rteinformatica 1 year, 4 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, 3 months ago

The question states: For which users can you modify the attributes from Azure AD?
Not from AD, but AAD.
upvoted 1 times



Exam AZ-104 All Actual Questions

Question #82

Topic 2

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

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

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

通过百度网盘分享的文件：AZ104

链接: https://pan.baidu.com/s/1i5xd_pbKx4xzkeT9gRaFbA?pwd=8888

B. No **Most Voted**

提取码:8888

复制这段内容打开「百度网盘APP 即可获取」

Correct Answer: B

Community vote distribution

B (96%)

A

Comments

iamchoy **Highly Voted** 1 year, 2 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 related command in the Microsoft Graph module.

module or a related command in the Microsoft Graph module.

Given the provided solution, the answer is:

B. No

upvoted 19 times

Rams786 Highly Voted 1 year, 2 months ago

This question was on my exam on 22 Sep 2023. scored 900 i answered B

upvoted 5 times

SeMo0o0o0o Most Recent 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

Amir1909 9 months, 3 weeks ago

No is correct

upvoted 2 times

vsvaid 10 months, 2 weeks 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

vsvaid 10 months, 2 weeks ago

Sorry wrong question, please ignore the above

upvoted 1 times

VV11_SS22 1 year, 4 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, 4 months ago

Do we have a similar question and the answer is no due to missing RedirectURL in the CSV?

upvoted 3 times

fdead 1 year, 4 months ago

yeah, that was to be created from AZ portal

upvoted 2 times

MHguy 1 year, 4 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, 3 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

Guest posts, see [View post](#) and [Leave a comment](#).

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/new-mguser?view=graph-powershell-1.0>
upvoted 1 times

Pakawat 1 year, 5 months ago

Found this Q in the exam, 3/7/23
upvoted 3 times

tech07 1 year, 5 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, 5 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, 5 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, 5 months ago

Are you saying the correct answer is Option B?
upvoted 3 times



Exam AZ-104 All Actual Questions

Question #83

Topic 2

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

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

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 **Most Voted**

B. No

Correct Answer: A

Community vote distribution

A (86%)

B (14%)

Comments

iamchoy **Highly Voted** 1 year, 2 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.

they will 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 27 times

Shark006 1 year, 1 month 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 14 times

Batiste2023 1 year, 1 month 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 10 months, 1 week 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, 5 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/module/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0#users>

upvoted 5 times

SeMo0o0o0o Most Recent 3 months ago

Selected Answer: A

it's A

upvoted 2 times

60ties 5 months 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 6 months, 2 weeks 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 7 months 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 8 months, 3 weeks ago

Yes is correct

upvoted 1 times

MatAlves 9 months, 2 weeks 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 10 months, 1 week ago

The CSV is missing a Redirect URL and the New-MgInvitation command requires it. Correct answer is No.

upvoted 1 times

vsvaid 10 months, 2 weeks 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 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 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

cig003 1 year ago

Selected Answer: A

Yes with New-MgInvitation 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 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 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, 1 month ago

Selected Answer: B

needs redirection URL

upvoted 3 times

amsioso 1 year, 1 month 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-MgInvitation 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, 1 month ago

Seem like Yes

[#users](https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0)

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, 2 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-MgInvitation, 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, 2 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, 2 months ago

Selected Answer: B

La respuesta correcta es la B.

In this quickstart, you'll use the New-MgInvitation 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

Korny11 1 year, 2 months ago

I would go for B. The cmdlet is correct but the required parameter "-InviteRedirectUrl" is missing in the CSV as mentioned here
<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0&preserve-view=true#-inviteredeemurl>

upvoted 4 times



Exam AZ-104 All Actual Questions

Question #84

Topic 2

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?

- Assign User1 the Contributor role for VNet1.
- Assign User1 the Network Contributor role for VNet1.
- Assign User1 the User Access Administrator role for VNet1. **Most Voted**
- 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%)

Comments

vsvald **Highly Voted** 10 months, 2 weeks ago

Selected Answer: C

This question has already appeared multiple times
upvoted 8 times

SeMo0o0o0o **Most Recent** 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

No_Restaurant9617 4 months 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 1 times

ELearn 4 months, 3 weeks ago

Selected Answer: C

C. Assign User1 the User Access Administrator role for VNet1.

upvoted 1 times

TedM2 1 year, 1 month 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, 2 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

Mudassar_Ift 1 year, 2 months ago

Selected Answer: C

correcta

upvoted 1 times

Vokuhila 1 year, 3 months ago

Selected Answer: C

Assigning roles to users is at least User Access Administrator

upvoted 1 times

Antaninad 1 year, 3 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>

<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



Exam AZ-104 All Actual Questions

Question #85

Topic 2

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?

- Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- Assign User1 the Network Contributor role for VNet1.
- Assign User1 the User Access Administrator role for VNet1. Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Comments

SeMo0o0o0o 3 months ago

Selected Answer: D

D is correct
upvoted 1 times

3c5adce 7 months, 2 weeks 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

vsvaid 10 months, 2 weeks ago

Selected Answer: D

Owner and User Access Administrator can assign roles

upvoted 4 times

TedM2 1 year, 1 month 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 3 times

iamchoy 1 year, 2 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, 3 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



Exam AZ-104 All Actual Questions

Question #86

Topic 2

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)



Comments

Vokuhila Highly Voted 1 year, 3 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 32 times

Sameer9371 1 year, 3 months ago

you are absolutely right

upvoted 3 times

hank00r 11 months, 1 week 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 20 times

ggogel 10 months, 2 weeks 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-configure-azure-active-directory>

upvoted 7 times

SDewan 10 months, 1 week ago

No, if you are targeting copy to the whole "file share" then SAS is the only option. Entra ID can be used , if you are copying a file or files to a specific folder inside file share. So, SAS only is correct for 2nd question

upvoted 2 times

tableton 8 months, 1 week 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 6 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 5 times

[Removed] Highly Voted 12 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 10 months, 3 weeks ago

Sorry, but with the official doc :<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-configure-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 4 months, 2 weeks ago

I think for both the answer is 3rd option

upvoted 2 times

sca88 Most Recent 3 weeks, 4 days 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 1 month ago

this kind of questions are tricky, because it is not explicit if it is going to copy only some files 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 1 month, 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-configure-azure-active-directory>

upvoted 4 times

155e6a0 2 months, 1 week 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-configure-azure-active-directory>

upvoted 3 times

SeMo0o0o0o 3 months ago

CORRECT

upvoted 1 times

OpOmOp 5 months ago

It can be authorized with credentials for FileShare as well

It can be authorized with credentials for the share 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 6 months, 4 weeks ago

Final Answer:

First: Azure AD & SAS

Second: SAS

upvoted 2 times

3c5adce 7 months 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 7 months ago

Changing my answer

Blob storage: Azure AD and shared access signatures (SAS)

File storage: Azure AD only

upvoted 2 times

ssky 7 months, 1 week 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 9 months, 1 week ago

Correct

upvoted 1 times

Ziolupo 9 months, 3 weeks ago

Entra ID is now available to authorize Azcopy on Azure file share.

upvoted 5 times

allyou 9 months, 3 weeks ago

<https://learn.microsoft.com/fr-fr/azure/storage/common/storage-ref-azcopy-copy>

upvoted 2 times

allyou 9 months, 3 weeks ago

<https://learn.microsoft.com/en-us/training/modules/configure-storage-tools/4-use-azcopy>

upvoted 1 times

edurakhan 10 months ago

This link:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-configure-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

RockyChak 10 months ago

Authorize access to blobs and files with AzCopy and Microsoft Entra ID

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-authorize-azure-active-directory>

Both Blob and File storage can be authenticated with Entra ID and SAS

upvoted 3 times

ggogel 1 year ago

Funny how even Microsoft is confused by their naming. It is called "Azure Files" or specifically "File Shares" and not "File storage".

upvoted 5 times



Exam AZ-104 All Actual Questions

Question #87

Topic 2

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 Azure portal's "External User" overview blade for a user named "External User". The user principal name is listed as "external195_gmail.com#EXT#@sk230415outlook.onmicrosoft.com". The user type is listed as "Guest". The "Basic info" section includes fields for "User principal name", "Object ID", "Created date time", "User type", and "Identities". The "Identities" field contains the value "mail". The "Manage" sidebar on the left lists options like "Custom security attributes (preview)", "Assigned roles", "Administrative units", "Groups", "Applications", "Licenses", "Devices", "Azure role assignments", "Authentication methods", "Troubleshooting + Support", and "New support request". The "Overview" tab is selected. At the bottom, there are three cards: "Account status" (Enabled), "Sign-ins" (Last sign-in: ---, See all sign-ins), and "B2B collaboration" (Invitation state: Accepted, Reset redemption status).

Answer Area

The screenshot shows the Azure Active Directory External User blade. On the left, there's a sidebar with options like Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Manage, Troubleshooting + Support, and New support request. The main area has tabs for Overview, Monitoring, and Properties. Under Basic Info, it shows the user principal name (external195_gmail.com#EXT#@sk230415outlook.onmicrosoft.com), Object ID (2b353249-fa3d-4cbe-bd9d-fa6cd60fa1c), and Created date time (Apr 29, 2022, 11:58 AM). The identities section is highlighted with a red box. At the bottom, there's a My Feed section with Account status, Sign-ins, and B2B collaboration tiles.

Comments

Vestibal Highly Voted 1 year, 2 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 38 times

PhiloUK 5 months, 1 week ago

This is right, you can easily confirm this on azure portal.

upvoted 1 times

090200f 6 months, 1 week 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, 2 months ago

I totally agree. MS document clearly lists these steps.

upvoted 2 times

devops_devops Highly Voted 10 months, 4 weeks ago

This question was in exam 15/01/24

upvoted 9 times

jamesf Most Recent 1 month, 2 weeks ago

"Edit properties"

"B2B collaboration"

<https://learn.microsoft.com/en-us/entra/external-id/reset-redemption-status>

upvoted 1 times

lykeman26 1 month, 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 1 times

SeMo0o0o0o 3 months ago

CORRECT

Edit properties
Identities
B2B collaboration
upvoted 1 times

Felas 7 months, 3 weeks ago

Then, the correct answer would be:
"Edit properties".
"B2B collaboration"
?
upvoted 2 times

1828b9d 9 months, 1 week ago

This question was in exam 01/03/2024
upvoted 4 times

Amir1909 9 months, 3 weeks ago

Edit properties
B2B
upvoted 1 times

31c21da 11 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 11 months, 1 week ago

Click in "edit properties" and "Reset redemption Status"
upvoted 2 times

[Removed] 11 months, 3 weeks 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 resend the B2B invitation.
upvoted 2 times

[Removed] 11 months, 1 week ago

<https://learn.microsoft.com/en-us/entra/external-id/reset-redemption-status>
upvoted 1 times

alexandrud 1 year, 1 month ago

1. Edit Identities (new email address)
2. Resend invitation to the new email address.
upvoted 2 times

shiraghami 1 year, 2 months ago

"Which two settings should you configure from the Overview blade?"
Read carefully question very important, right?
upvoted 1 times

Vokuhila 1 year, 3 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, 3 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, 3 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/reset-redemption-status>
upvoted 4 times

maxsteele 1 year, 2 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 10 months, 2 weeks 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



Exam AZ-104 All Actual Questions

Question #88

Topic 2

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 Most Voted
- D. Reader and Data Access

Correct Answer: C

Community vote distribution

C (64%)

A (36%)

Comments

Rastova Highly Voted 12 months ago

Selected Answer: A

hello am under the water please help me
upvoted 40 times

Babustest Highly Voted 1 year, 2 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 24 times

ayufitri Most Recent 11 hours, 57 minutes 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 1 times

Omer87 2 months, 3 weeks ago

Selected Answer: C

Storage Blob Data Contributor

upvoted 2 times

SeMo0o0o0o 3 months ago

Selected Answer: C

C is correct

upvoted 3 times

alsmk2 4 months 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 4 months, 2 weeks 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 6 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 6 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 7 months 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 8 months, 2 weeks 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 9 months, 1 week 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 doesn't 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 9 months, 1 week ago

C is correct

upvoted 1 times

AAlmani 9 months, 3 weeks 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

SkyZeroZx 11 months, 1 week ago

Selected Answer: C

A : No has permissions 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 8 times

tripleaholic 1 year, 1 month 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 .

The Contributor in option D 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, 2 months ago

Correct answer is C due to delete-operation

upvoted 4 times



Exam AZ-104 All Actual Questions

Question #89

Topic 2

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?

- Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- Assign User1 the Contributor role for VNet1.
- Assign User1 the Owner role for VNet1. **Most Voted**
- Assign User1 the Network Contributor role for RG1.

Correct Answer: C

Community vote distribution

C (100%)

Comments

ki01 **Highly Voted** 12 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 15 times

shrsrm95 **Highly Voted** 1 year, 3 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

VitaliiKurishko Most Recent 1 month ago

I like this question, 10 more times and I will love it)

upvoted 1 times

kijokskip 8 months, 3 weeks ago

Why this question is so often?

upvoted 4 times

bgcarter 10 months, 2 weeks 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, 2 months ago

Option C

This question is repeated many times

upvoted 4 times

samehpalass 1 year, 3 months ago

c Owner or user access administrator to assign role to other users

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #90

Topic 2

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 **Most Voted**
- C. Group3 and Group4 only
- D. Group1, Group2, and Group3 only
- E. Group1, Group2, Group3, and Group4

Correct Answer: B

Community vote distribution

B (50%)

D (47%)

Other

Comments

SivaPannier **Highly Voted** 1 year, 3 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 41 times

[Removed] 1 year, 1 month 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, 1 month 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 6 months, 1 week 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 6 times

Jedi_sg2000 6 months, 4 weeks ago

u r rite!

upvoted 1 times

iamchoy **Highly Voted** 1 year, 2 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 37 times

Fryether1 4 months 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 5 times

2d153f5 3 weeks, 2 days ago

That's it.

upvoted 1 times

LovelyGroovey 9 months, 1 week ago

Thank you! Your explanation is so clear and I understand better now

upvoted 1 times

Armandez **Most Recent** 5 days 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 and Group3.

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 1 times

JPA210 1 month ago

Selected Answer: D

sorry guys according to Microsoft documentation :

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

jamesf 1 month, 2 weeks ago

Selected Answer: D

Should be D, Group 1, 2 & 3

"The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE."

upvoted 2 times

Shame1994 1 month, 3 weeks ago

You can absolutely assign these licensed to mail enabled security groups. They shifted this to admin portal and I am able to assign my e5 licenses to a mail enabled security group

upvoted 1 times

jamesf 1 month, 3 weeks ago

Selected Answer: D

I prefer for D as Security Enabled is the key

upvoted 1 times

Omer87 2 months, 3 weeks ago

Selected Answer: B

License can be applied for only security groups or security-enabled Microsoft 365 (Unified) groups.

<https://techcommunity.microsoft.com/t5/microsoft-365/why-can-t-i-assign-licenses-to-every-groups-created-using-ms-m-p/2776552>

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: B

B is correct

Type: Security + Microsoft 365

Security: Enabled

upvoted 1 times

mojo86 3 months, 3 weeks ago

Answer is B. Group 2(No) Because Azure AD does not support assigning licenses, including Azure AD Premium P2 licenses, to mail-enabled security groups. The group types that support licensing do not include mail-enabled security groups due to their hybrid nature and focus on email distribution. You cannot assign an Azure AD Premium P2 license to a Microsoft 365 Group with security disabled. Group 4 (No) Because the group must be a security principal (i.e., security-enabled) to support license assignment in Azure AD.

upvoted 1 times

Thisisacat 4 months, 2 weeks ago

A prime example why AI should not be trusted:

Gemini - Yes, you can assign licenses to mail-enabled security groups in Azure AD.

ChatGPT: No, you cannot assign licenses to mail-enabled security groups in Azure Active Directory (Azure AD).

upvoted 2 times

ajay01avhad 4 months, 2 weeks ago

Based on the detailed information from reliable sources:

To assign Azure Active Directory Premium P2 licenses, you can assign them to security groups and Microsoft 365 groups that have the securityEnabled property set to true. The groups eligible for license assignment include:

Group1: Security group, Enabled.

Group2: Mail-enabled security group, Enabled.

Group3: Microsoft 365 group, Enabled.

Group4: Microsoft 365 group, Disabled (Not eligible because it is disabled).

Given these criteria, you can assign licenses to Group1, Group2, and Group3.

Therefore, the correct answer is:

D. Group1, Group2, and Group3 only

upvoted 4 times

Tbag 4 months, 3 weeks ago

Types of Groups You Can Assign Licenses To
Security Groups:

Standard Security Groups: These are the most common types of groups used for managing access to resources. You can assign licenses to standard security groups.

Mail-Enabled Security Groups: These groups function as both security groups and distribution lists. They can also be assigned licenses.

Microsoft 365 Groups (formerly Office 365 Groups):

These groups include collaboration features such as shared mailboxes, calendars, and document libraries. You can assign licenses to Microsoft 365 Groups.

upvoted 1 times

manoj3039 6 months, 1 week ago

Selected Answer: B

<https://techcommunity.microsoft.com/t5/microsoft-365/why-can-t-i-assign-licenses-to-every-groups-created-using-ms/td-p/2776552>

"....License can be applied for only security groups or security enabled Microsoft 365 (Unified) groups....."

upvoted 2 times

23169fd 6 months, 1 week ago

Correct answer is D.

The key here is security enabled.

upvoted 1 times

SofiaLorean 6 months, 3 weeks ago

Selected Answer: B

Security groups: Yes

Microsoft 365 groups: Yes

Mail-enabled security groups: No

Distribution groups: No

If the groups mentioned include any mail-enabled security groups, those cannot be assigned the Azure AD Premium P2 licenses.

upvoted 2 times

3c5adce 7 months ago

Since Azure AD licenses typically require groups to have security enabled to manage memberships and assign licenses properly:

Group1, Group2, and Group3 are eligible for the license assignments because they are security-enabled groups.

Group4 cannot have licenses assigned directly since its security is disabled, meaning it does not manage security principals needed for direct license assignments.

Therefore, the correct choice, based on the requirement that groups must have security enabled to receive Azure AD license assignments, is:

D. Group1, Group2, and Group3 only

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #91

Topic 2

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

([] ▼ -eq "Marketing") [] ▼ (user.country [] ▼ "France")

[] ▼
device.managementType
device.organizationalUnit
user.department
user.usageLocation

[] ▼
and
or
typeof

[] ▼
-and
-eq
-in
-match

Answer Area

Correct Answer:

([] ▼ -eq "Marketing") [] ▼ (user.country [] ▼ "France")

[] ▼
device.managementType
device.organizationalUnit
user.department
user.usageLocation

[] ▼
and
or
typeof

[] ▼
-eq
-in
-match

Comments

AntaninaD Highly Voted 1 year, 3 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 28 times

Vokuhila Highly Voted 1 year, 3 months ago

(user.department -eq "Marketing") -and (user.country -eq "France")

upvoted 9 times

RanPo Most Recent 3 months ago

It was in my exam at 29.8.24

upvoted 1 times

SeMo0o0o0o 3 months ago

CORRECT

upvoted 1 times

3c5adce 7 months ago

(user.department -eq "Marketing") and (user.country -eq "France")

upvoted 1 times

1828b9d 9 months, 1 week ago

This question was in exam 01/03/2024

upvoted 2 times

bnicolas 9 months, 3 weeks ago

"-eq" AND "-match" would work.

upvoted 1 times

Amir1909 9 months, 3 weeks ago

Correct

upvoted 1 times

tfdestroy 11 months, 3 weeks 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, 1 month ago

The given answer is correct.

upvoted 2 times

pinyonet 1 year, 2 months ago

(user.department -eq "Marketing") -and (user.country -eq "France")

upvoted 2 times

rikininetysix 1 year, 3 months ago

The given answer is correct.

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #92

Topic 2

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.

Default user role permissions

Learn more

Users can register applications	<input checked="" type="radio"/> Yes
Restrict non-admin users from creating tenants	<input checked="" type="radio"/> No
Users can create security groups	<input checked="" type="radio"/> Yes

Guest user access

Learn more

Guest user access restrictions	<input type="radio"/> Guest users have the same access as members (most inclusive)
	<input checked="" type="radio"/> Guest users have limited access to properties and memberships of directory objects
	<input type="radio"/> 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	<input checked="" type="radio"/> No
---	-------------------------------------

LinkedIn account connections

Learn more

Allow users to connect their work or school account with	<input checked="" type="radio"/> Yes
--	--------------------------------------

LinkedIn

Selected group
 No

Show keep user signed in

Show keep user signed in Yes

Correct Answer:

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

Comments

AntaninaD Highly Voted 1 year, 3 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 Graph API, 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 25 times

josola 1 year, 1 month 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 11 months ago

No. the "Restrict Access to Azure AD" is set to "No".

No, the "User can register applications" option is set to No.

upvoted 5 times

SeMo0o0o0o Most Recent 3 months ago

CORRECT

upvoted 1 times

testtaker09 5 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 4 times

3c5adce 7 months 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 9 months, 3 weeks ago

Correct

upvoted 1 times

river1999991 1 year, 1 month ago

The given answer is correct.

upvoted 3 times

markb258 1 year, 2 months ago

why isn't it to restrict user to their own directory objects?

upvoted 3 times

alsmk2 4 months, 1 week ago

Because the question is for STANDARD users, and that option refers to GUEST users.

upvoted 1 times

Cfernandes 1 year, 2 months ago

Acho correto

upvoted 1 times

ajdann 1 year, 3 months ago

I believe its correct

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #93

Topic 2

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

Statements	Yes	No
Correct Answer:		
User1 can read blob2.	<input checked="" type="checkbox"/>	<input type="radio"/>
User1 can read blob3.	<input checked="" type="checkbox"/>	<input type="radio"/>
User2 can read blob1.	<input type="radio"/>	<input checked="" type="checkbox"/>

Comments

sugarbubbles Highly Voted 1 year, 3 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 128 times

Stunomatic 1 month, 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, 2 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 21 times

Batiste2023 1 year, 1 month 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, 2 months ago

I agree Joshua thanks

upvoted 2 times

QL112233 10 months, 2 weeks ago

Human language, reader role cannot read unless it's blob one, writer role cannot write unless it's blob 2

upvoted 6 times

HoT77777 Highly Voted 1 year, 3 months ago

Based on the documentation is NNY

upvoted 27 times

Ycheqri 1 year, 3 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.

Documentation:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-format>

upvoted 8 times

Ycheqri 1 year, 3 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, 2 months ago

There is OR condition

upvoted 6 times

Lapiduse 1 year, 3 months ago

This is not an answer

upvoted 2 times

GreenTick Most Recent 2 weeks, 1 day 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 1 times

sca88 3 weeks, 3 days ago

Should be NNY

upvoted 1 times

behradclid 3 months ago

ChatGPT says NNN which I believe based on explanation it provided

upvoted 1 times

SeMo0o0o0o 3 months ago

WRONG

No

No

Yes

upvoted 1 times

SeMo0o0o0o 2 months, 4 weeks ago

.....
upvoted 1 times

azmlan 4 months, 2 weeks 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 5 months ago

The answer is NNY

upvoted 1 times

OscarFRitz 5 months, 2 weeks ago

Tested:

NNY

upvoted 1 times

testtaker09 5 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 1 times

robsoneuclides 6 months, 2 weeks ago

NNY the image is wrong

upvoted 2 times

Miccc 6 months, 2 weeks ago

Answer is NNN

The condition has OR check, not AND

upvoted 4 times

3c5adce 7 months ago

Based on the documentation is NNY

upvoted 1 times

roobzn 7 months, 2 weeks ago

I thought the answer is YYN. Because isn't the "!" in front of the action standing for "NOT"? So isn't it saying: if the action is everything but NOT reading (in condition a) and NOT writing (in condition b)? Not trying to confuse people, just asking..

upvoted 2 times

LovelyGroovey 7 months, 3 weeks ago

I say Yes-Yes-No. Here is why I think it's Yes-Yes-No.

It says, "Sub1 contains two users named User1 and User2. Both users are assigned the Reader role at the Sub1 scope."

User1 and User2 got reader role. So, they both can read. However, conditions: Condition1 and Condition2.

If you look at ActionMaches in blue, Condition1 has blobs/read' and Condition2 has blob/write'

Normally Owner can read. But it does not say blob/read' on Condition2 which is linked to User2 (Owner) in this case. So, the User2 (Owner) can not read blob1 this time.

Let me know if my logic is wrong.

upvoted 4 times

mojo86 7 months, 3 weeks ago

Ans is YYY. User1 and User 2 have read role in sub1 scope.

In Azure Policy, scope takes precedence over condition. The policy scope determines which Azure resources the policy applies to. If a policy's scope is defined to apply to a specific resource group, subscription, or management group, then the policy will only affect resources within that scope, regardless of the conditions defined in the policy. Conditions are used to further refine the policy's application within the specified scope, but the scope itself is the primary factor in determining where the policy is enforced.

upvoted 4 times

Amir1909 9 months, 3 weeks ago

No

No

Yes

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #94

Topic 2

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

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

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 **Most Voted**

Correct Answer: B

Community vote distribution

B (92%)

A (8%)

Comments

rajneeshverma2020 **Highly Voted** 11 months, 2 weeks ago

This question is repeated multiple times, can admin remove duplicates
upvoted 7 times

Kalaiarasu **Most Recent** 2 months, 1 week ago

New-MgInvitation cmdlet for inviting external users ..
unvoted 1 times

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

ProfesorF 5 months ago

ive seen this question like 10 times wow

upvoted 1 times

AlbertKwan 6 months ago

Selected Answer: A

Voting for A to test if admin actually reads my comment here.

upvoted 1 times

Cfernandes 7 months, 1 week 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, 1 month 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, 2 months ago

Selected Answer: B

should do the invite cmdlet rather than the create one

upvoted 3 times

Babustest 1 year, 2 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 4 times



Exam AZ-104 All Actual Questions

Question #95

Topic 2

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": "https://schema.management.azure.com/schemas/2019-04-
3    "contentVersion": "1.0.0.0",
4    "parameters": {
5      "obj1": {
6        "type": "object",
7        "defaultValue": {
8          "propA": "one",
9          "propB": "two",
10         "propC": "three",
11         "propD": {
12           "propD-1": "sub",
13           "propD-2": "sub"
14         }
15       }
16     },
17     "par1": {
18       "type": "string",
19       "allowedValues": [
20         "centralus",
21         "eastus",
22         "westus" ],
23       "defaultValue": "eastus"
24     }
25   },
26   "variables": {
27     "var1": [
28       "westus",
29       "centraus"
30       "eastus"
31     ]
32   },
33   "resources": [
34     {
35       "type": "Microsoft.Resources/resourceGroups",
36       "apiVersion": "2018-05-01"
```

```
56     "apiVersion": "2018-05-01",
57     "location": "eastus",
58     "name": [concat('RGS', copyIndex())]
59   },
60   {
61     "type": "Microsoft.Resources/resourceGroups",
62     "apiVersion": "2018-05-01",
63     "location": [last(variables('var1'))],
64     "name": "[concat('ResGrp', '8')]"
65   },
66   {
67     "type": "Microsoft.Resources/resourceGroups",
68     "apiVersion": "2018-05-01",
69     "location": "[parameters('part1')]",
70     "name": "[concat('RGroup', length(parameters('obj1')))]"
71   }
72 ],
73 "outputs": {}
74 }
```

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 checked="" type="checkbox"/>	<input type="radio"/>
A resource group named RGroup5 is created.	<input type="radio"/>	<input checked="" type="checkbox"/>
All the resource groups are created in the East US Azure region.	<input checked="" type="checkbox"/>	<input type="radio"/>

Comments

trferreiraBR Highly Voted 1 year, 2 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 resource group named RGroup5;
3 - It's Y, because all resource groups were created in the East US Azure Region.
upvoted 89 times

Archangel0007 1 year, 1 month 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, 1 month 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 14 times

Highgate 3 months, 3 weeks ago

Excellent answer

upvoted 1 times

fomedad 1 year, 1 month ago

Why The Resource Group named with "[concat('RGS', copyIndex())]", creates RGS0 and RGS1?

upvoted 4 times

ubiquituz 12 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 7 times

ubiquituz 12 months ago

count: how many instance of the RG should exist...sorry my english isnt too good

upvoted 2 times

pharsat 1 year, 1 month ago

Count property

upvoted 4 times

nsss 1 year 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 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 11 months ago

microsoft willfully put it like that because the default value for location which is "EAST US" if a location is not specified or empty it will default to that or wrong specification

upvoted 1 times

c5ad307 10 months, 3 weeks ago

You can also assume that it is a transcription error. Just consider both possibilities when taking the exam and read carefully

upvoted 2 times

forkie Highly Voted 1 year, 2 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 resources 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, 1 month 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 11 months, 3 weeks 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

SeMo0o0o0o Most Recent 3 months ago

WRONG

No

No

Yes

upvoted 1 times

SeMo0o0o0o 2 months, 4 weeks ago

.....
upvoted 1 times

AlbertKwan 6 months ago

NNN - because in Line 35, the text "resrouceGroup" is wrong.

upvoted 4 times

varinder82 6 months, 4 weeks ago

Final Answer: 'Yes No No

upvoted 1 times

3c5adce 7 months ago

ChatGPT4 says Yes No No

upvoted 1 times

semse27 6 months, 1 week ago

mine says no no yes

upvoted 2 times

3c5adce 7 months ago

Went through comments - most popular answer is NNY

upvoted 1 times

devilish84 7 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 2 times

5faef8c 7 months, 2 weeks 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 8 months 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, deafaultvalue eastus

upvoted 1 times

prshntdxt7 8 months, 1 week 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 8 months, 2 weeks 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 1 times

Amir1909 8 months, 3 weeks ago

No

No

Yes

upvoted 1 times

adilkhan 10 months, 2 weeks ago

answer is N N Y

upvoted 2 times

SkyZeroZx 11 months, 1 week 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 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 ago

With that typo, the template would not execute.

upvoted 1 times

lsumby10 1 year ago

bro stop killing the excitement of learning.. you are literally creating a whole discussion just for a TYPO??

?????????????????????

upvoted 3 times

AlbertKwan 6 months ago

Obviously you are wishful that the compiler/interpreter has intelligence to correct typos...

upvoted 1 times

esetyanto 1 year, 1 month ago

N - spelling mistake on first resource group

N - RGroup4

N - spelling mistake on the param

upvoted 5 times



Exam AZ-104 All Actual Questions

Question #96

Topic 2

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 **Most Voted**
- C. a network security group (NSG)
- D. Azure Peering Service

Correct Answer: B

Community vote distribution

B (100%)

Comments

Batiste2023 **Highly Voted** 1 year, 1 month 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>

<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview>

upvoted 5 times

Batiste2023 1 year, 1 month 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 2 times

SeMo0o0o0o Most Recent 1 month ago

Selected Answer: B

B is correct

from VM1 to storage1 = private endpoints
between VNet1 and VNet2 = peering

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: B

B is corerct

upvoted 1 times

Pdutz 5 months ago

Correct, private endpoint

upvoted 1 times

testtaker09 5 months, 3 weeks ago

was in the exam today 17/06/2024

upvoted 4 times

090200f 6 months, 1 week ago

private endpoint

upvoted 2 times

Navigator 10 months, 3 weeks ago

B is perfect

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #97

Topic 2

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 **Most Voted**
- C. a network security group (NSG)
- D. Azure Firewall

Correct Answer: B

Community vote distribution

B (100%)

Comments

Sicknt 3 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 example a Storage Account) But Microsoft would know to route it in its Microsoft Backbone network

upvoted 4 times

ProfesorF 5 months ago

sometimes it is private endpoints

upvoted 1 times

Josh219 4 months, 1 week ago

so both are correct ?

Private endpoints and Service endpoints?

upvoted 1 times

asdfgqwer 9 months, 1 week ago

500 and 400 repeated

upvoted 2 times

tfdestroy 11 months, 2 weeks 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 11 months, 3 weeks ago

No doubts here

upvoted 1 times

Batiste2023 1 year, 1 month 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



Exam AZ-104 All Actual Questions

Question #98

Topic 2

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 **Most Voted**
- C. a network security group (NSG)
- D. Azure Peering Service

Correct Answer: B

Community vote distribution

B (100%)

Comments

01111010 **Highly Voted** 1 year ago

Selected Answer: B

B. service endpoints - assures traffic goes over MS bon(er)
upvoted 6 times

Ahkhan **Most Recent** 1 year ago

This question was on my exam today on 11/14/2023.

upvoted 2 times

PERCY23 1 year ago

And wat was your answer

upvoted 1 times

lebeyic620 8 months, 2 weeks ago

And did you pass?

upvoted 1 times

victorlie 5 months ago

It seems not, cause he's still here

upvoted 2 times

gbemxods 4 months ago

ACCOUNT IS A BOT

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #99

Topic 2

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 **Most Voted**
- D. VM1

Correct Answer: C

Community vote distribution

C (100%)

Comments

Gabsyfire **Highly Voted** 1 year, 1 month 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 40 times

Batiste2023 Highly Voted 1 year, 1 month ago

Selected Answer: C

Answer is correct.

A new question about a legacy topic. Co-Administrators were 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 14 times

2d153f5 Most Recent 3 weeks, 2 days ago

Co-admin is a role that no longer exists in Azure as of August 2024. This question is obsolete.

upvoted 2 times

sukaysukay 3 months ago

As of August 31st 2024, classic Azure Role has retired, which includes retirement of co-administrator role.

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

3c5adce 7 months 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 9 months, 3 weeks ago

C is correct

upvoted 1 times

Wojer 10 months, 3 weeks ago

from 15 February 2024 you will not be able to add new Co-Administrator

upvoted 3 times

Tilakarasu 11 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 ago

The correct answer is C: Sub1, however this is a legacy question, Co-Administrator and Service Administrator roles are used with classic resources: 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 3 times



Exam AZ-104 All Actual Questions

Question #100

Topic 2

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



Comments

techtest848 Highly Voted 11 months, 1 week 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 72 times

Giovachia2016 10 months, 3 weeks ago

Correct. Tested in Lab too.

upvoted 7 times

Alandt 11 months, 1 week ago

Please be clear in your answer. What is your answer now?

upvoted 2 times

rodrod 1 month, 1 week ago

He gave a very clear answer. It just can't be clearer... Read again

upvoted 1 times

Andreas_Czech 11 months, 1 week ago

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced#deleting-a-group-with-an-assigned-license>

upvoted 1 times

SkyZeroZx Highly Voted 11 months, 1 week 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 10 times

LinuxLewis Most Recent 4 weeks, 1 day 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 1 times

SeMo0o0o0o 3 months ago

WRONG

Users: User1, User2, User3, and User4
Groups: Group 2 and Group 4 only
upvoted 1 times

SeMo0o0o0o 2 months, 4 weeks ago

.....
upvoted 1 times

3c5adce 7 months 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 8 months, 2 weeks 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 9 months, 3 weeks ago

We can delete all users and Group 2 and 4
upvoted 2 times

yukkki 11 months, 2 weeks ago

these answers are correct.
upvoted 1 times



Exam AZ-104 All Actual Questions

Question #101

Topic 2

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 **Most Voted**
- 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%)

Comments

Yumperboy **Highly Voted** 11 months, 1 week 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 10 times

SeMo0o0o0o **Most Recent** 3 months ago

Selected Answer: B

B is correct
upvoted 1 times

testtaker09 5 months, 3 weeks ago

was in the exam today 17/06/2024
upvoted 2 times

edurakhan 6 months ago

Selected Answer: B

Definitely B
upvoted 1 times

Peachu200 9 months, 3 weeks ago

correct Amswer :B
upvoted 1 times

Mysystemad 11 months ago

B it's ok
upvoted 1 times

SkyZeroZx 11 months, 1 week 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



Exam AZ-104 All Actual Questions

Question #102

Topic 2

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="checkbox"/>	<input type="radio"/>
	User2 can create a new storage account in RG1.	<input type="radio"/>	<input checked="" type="checkbox"/>
	User3 can assign User1 the Owner role for RG3.	<input checked="" type="checkbox"/>	<input type="radio"/>

Comments

alsmk2 Highly Voted 3 months, 2 weeks ago

YNY

1. User 1 is a contributor of MG2, which contains 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 17 times

sabrinakloud Highly Voted 1 month, 1 week 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 5 times

2d153f5 3 weeks, 2 days ago

Great!

upvoted 1 times

allinict Most Recent 1 week, 6 days 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 1 times

c4ecedc 1 month, 1 week 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

Sifon_n 1 month, 1 week ago

Y, N, Y

upvoted 1 times

SeMo0o0o0o 3 months ago

CORRECT

upvoted 1 times

SeMo0o0o0o 2 months, 1 week ago

according to the scopes

upvoted 1 times

RanPo 3 months, 1 week ago

agreed

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #103

Topic 2

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 **Most Voted**
- C. Microsoft Entra Application Proxy
- D. Azure Virtual WAN

Correct Answer: B

Community vote distribution

B (100%)

Comments

webbrowser 2 months ago

The answer is B
upvoted 1 times

behradcll 3 months ago

Selected Answer: B

100% correct. I like this question :) Good luck with your exam!

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

RanPo 3 months, 1 week ago

these kind of question seen all the times, might need to shrink them

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #104

Topic 2

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. **Most Voted**
- 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. **Most Voted**

Correct Answer: CF

Community vote distribution

CF (92%)

DF (8%)

Comments

behradcl1 3 months ago

Selected Answer: CF

I would say CDF but there is no third answer so the best choices are CF.

upvoted 2 times

SeMo0o0o0o 3 months ago

Selected Answer: CF

C & F are correct

upvoted 3 times

ELearn 3 months, 1 week ago

Selected Answer: CF

vote: C&F

upvoted 4 times

ELearn 3 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 4 times

ELearn 3 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 2 times

siheom 3 months, 2 weeks ago

Selected Answer: CF

vote CF

upvoted 2 times

michael1msc 3 months, 2 weeks ago

Selected Answer: DF

As you don't have option to upload csv to Azure the only option is PowerShell + CSV.

upvoted 1 times

pasangawa 3 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 3 months, 2 weeks ago

ChatGPT: Correct answer CF

CHAPTER 1. CORRECT ANSWER: C,F.

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



Exam AZ-104 All Actual Questions

Question #105

Topic 2

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 Most Voted**
- E. a Recovery Services vault

Correct Answer: D

Community vote distribution

D (100%)

Comments

exa104az Highly Voted 3 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 9 times

behradcl1 Most Recent 3 months ago

Selected Answer: D

simple as cake

upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: D

D is correct

upvoted 1 times

6c05b3d 3 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 2 times

alsmk2 3 months, 2 weeks ago

Selected Answer: D

Correct

upvoted 3 times



Exam AZ-104 All Actual Questions

Question #106

Topic 2

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 Most Voted
- E. User1, Group1, and Group2

Correct Answer: D

Community vote distribution



Comments

hnk Highly Voted 2 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 11 times

d72bae5 3 weeks, 2 days ago

I agree, D is the answer. I tested and I agree with hnK

unvoted 1 times

pheztux 1 month, 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 2 times

feralberti 1 month, 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 1 week ago

<https://youtu.be/rA8TvhNcCvQ>

upvoted 1 times

Sunth65 1 week ago

<https://youtu.be/Lu1VT13GvyE>

upvoted 1 times

alsmk2 Highly Voted 3 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 7 times

Josh219 1 week ago

you have to stick to the information given in question and answer it.

Its Option C

upvoted 1 times

MSLearningStuff Most Recent 3 days, 6 hours ago

Selected Answer: A

The question asks for which identities you can *enable* SSPR, not which identities you can *assign* SSPR policies. I think it's poorly structured but given the use of the word "enable", A is the correct answer.

upvoted 1 times

minura 1 week, 2 days ago

Selected Answer: E

Correct Answer is E

"Microsoft Entra self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement."

Ref: <https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr>

upvoted 1 times

Sholasleek 3 weeks, 1 day ago

Correct answer is E, when deploying SSPR, even in the testing phase, you can test out with individual user accounts.
(E. user1, group1, group2) is the right answer.

upvoted 1 times

Chuong0810 1 month ago

Selected Answer: A

Self-Service Password Reset (SSPR) is a feature designed for individual users to reset their own passwords. It's primarily intended for user accounts, not groups.

While groups can be used for various administrative tasks, they don't have individual passwords that can be reset. Therefore, you can only enable SSPR for User1 in this scenario.

upvoted 3 times

JPA210 1 month ago

Selected Answer: D

Please read here carefully and you can see that you can only use groups, not users.

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#enable-self-service-password-reset>

upvoted 2 times

sabrinakloud 1 month, 1 week ago

Selected Answer: C

sspr not supported for Microsoft 365

upvoted 2 times

Bolthen 1 month, 2 weeks ago

Selected Answer: D

Tested in personal tenant. Answer is D. You can assign either M365 and Security Groups to the scope of SSPR when set to "Selected". Check subpoint 4:

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#enable-self-service-password-reset>

upvoted 3 times

AgnieszkaM 3 days, 10 hours ago

te same place but point 5: To enable SSPR for the select users, select Save.

upvoted 1 times

jamesf 1 month, 3 weeks ago

Selected Answer: 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 2 times

freeacrite 1 month, 4 weeks ago

Selected Answer: B

Can only be enabled for security groups.

upvoted 1 times

Pisces225 2 months ago

Selected Answer: D

You cannot assign SSPR to an individual user. The people saying you can are either simply wrong or intentionally putting bogus info into these comments to make the discussion less helpful.

upvoted 4 times

kejo2 2 months, 1 week ago

Just tried this in my Lab today 2-oct-2024. You can only assign SSPR to Security and Microsoft 365 groups but not to Users account. The answer should be D. Before commenting, please always try it out on your lab.

upvoted 3 times

sahilarora1 2 months, 1 week ago

Selected Answer: E

checked with ChatGPT and Gemini

upvoted 1 times

examprepboy 2 months, 2 weeks ago

the correct answer is D

you CANNOT assign SSPR to a user. it is a feature which is either enabled for ALL or a group

upvoted 5 times

thekrushka 3 months ago

Selected Answer: E

I don't know what I'm missing, but I've created clean new 365 group with default settings and I was able to assign SSPR with no

problem

upvoted 1 times

rober13 3 months ago

SSPR is designed for individual user accounts and security groups within Azure Active Directory (Azure AD). I think it is C

upvoted 1 times

examprepboy 2 months, 2 weeks ago

you cannot assign SSPR policy to users it has to be a group

upvoted 2 times

SeMo0o0o0o 3 months ago

Selected Answer: C

C is corerct

since it's not mentioned that Microsoft 365 has security-enabled.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #107

Topic 2

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

Create a group naming policy.

Correct Answer:

Set Add prefix to Attribute

Set Add prefix to **Attribute**.

Set Select type to **Department**.

Comments

ELearn Highly Voted 3 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 7 times

eduardovzermeno Most Recent 2 months ago

<https://learn.microsoft.com/es-mx/entra/identity/users/groups-naming-policy>

upvoted 2 times

SeMo0o0o0o 3 months ago

CORRECT

upvoted 1 times

Jacky_1 3 months, 2 weeks ago

Answer is correct. Tested it in my tenant.

upvoted 4 times

Shakka 3 months, 2 weeks ago

Tested in Azure, Given Answer is correct

upvoted 1 times

Alawi1990 3 months, 2 weeks ago

Create a group naming policy.

Set Add prefix to Attribute.

Set Add suffix to String.

upvoted 4 times

alsmk2 3 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 4 times



Exam AZ-104 All Actual Questions

Question #108

Topic 2

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

Comments

ELearn Highly Voted 3 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 13 times

Armandez 4 days, 21 hours 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 1 times

IPERSONIC Most Recent 1 month, 1 week 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 3 times

gt1405 3 months ago

Box1 : User1, User2, User3, and User4

Box2 : Group1 only

upvoted 4 times

gt1405 3 months ago

Box1 : User1, User2, User3, and User4

Box2 : Group1 and Group3 only

upvoted 2 times

SeMo0o0o0o 3 months ago

CORRECT

upvoted 2 times



Exam AZ-104 All Actual Questions

Question #109

Topic 2

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

Create a:

Managed identity

Correct Answer:

Private endpoint
Service principal
User account

Use the secret from:

Vault1 only
Vault1 and Vault2 only
Vault1 and Vault3 only
Vault1, Vault2, or Vault3

Comments

SeMo0o0o0o Highly Voted 3 months ago

WRONG

Create a: Managed Identity

Use the secret from: Vault1, Vault2, or Vault3

upvoted 14 times

happpieee 1 month 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 Most Recent 1 month 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 3 times

Stunomatic 1 month, 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 1 month, 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 5 times

0378d43 1 month, 3 weeks ago

Managed Identity and VAULT1 and 3 due to the location of the APP.

upvoted 2 times

akinz 1 month, 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 3 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 4 times

pasangawa 3 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 3 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 the 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 possibilities/options)

upvoted 3 times

Dankho 2 months ago

agreed, the question doesn't specify so I think all 3 vaults are possible.

upvoted 2 times

ELearn 3 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 3 months, 2 weeks ago

*Correction: Vault2 is in different region

upvoted 2 times

majejim435 3 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 3 months, 2 weeks ago

*Correction: Vault2 is in different region

upvoted 1 times

6c05b3d 3 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

upvoted 1 times

HardeWerker433 3 months, 2 weeks ago

is this brokey?

upvoted 1 times

Jacky_1 3 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



Exam AZ-104 All Actual Questions

Question #110

Topic 2

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. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

KAM2023 Highly Voted 3 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 11 times

Shakka Highly Voted 3 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

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 7 times

minura Most Recent 1 week, 2 days 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 1 times

SeMo0o0o0o 3 months ago

Selected Answer: D

D is corerct

upvoted 1 times

DJHASH786 3 months, 2 weeks ago

D is correct answer.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #111

Topic 2

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 Most Voted
- E. Storage Blob Data Owner Most Voted
- F. Storage Blob Delegator

Correct Answer: DE

Community vote distribution

DE (92%)

BD (8%)

Comments

alsmk2 Highly Voted 3 months, 2 weeks ago

Selected Answer: DE

Incorrect. Answer should be DE.

upvoted 8 times

Shakka 3 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 2 times

SeMo0o0o0o Most Recent 3 months ago

Selected Answer: DE

WRONG

D & E are correct

upvoted 1 times

6c05b3d 3 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

arunyadav09 3 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



Exam AZ-104 All Actual Questions

Question #112

Topic 2

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 a 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	<i>None</i>
Admin2	Attribute Definition Administrator	<i>None</i>
Admin3	Attribute Assignment Administrator	<i>None</i>
User1	<i>None</i>	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:
 - Three stored access policies named Stored1, Stored2, and Stored3
 - 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.

Admin2 can assign Attribute1 to User1.

Admin3 can assign Attribute1 to Group2.

Answer Area

Statements	Yes	No
------------	-----	----

Correct Answer: Admin1 can assign Attribute1 to Group1.

Admin2 can assign Attribute1 to User1.

Admin3 can assign Attribute1 to Group2.

Comments

dilopezat 2 weeks 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 3 weeks, 2 days 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 3 times

kam1122 2 weeks, 3 days ago

Correct, only Attribute Assignment Admin able to assign
upvoted 1 times

sca88 3 weeks, 2 days ago

Exam topic should not allow comments without documentation link...
upvoted 1 times

155e6a0 2 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

SeMo0o0o0o 3 months ago

WRONG

No
No
No

upvoted 1 times

pasangawa 3 months, 1 week 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 4 times

Adx_YT 1 month, 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-atributes>
upvoted 1 times

kjujuai 3 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 3 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 service 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 3 months, 2 weeks ago

1,2. <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/custom-security-attributes-apps?pivot=portal>
3. <https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-overview>

upvoted 2 times

upvoted 2 times

arunyadav09 3 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 3 months, 2 weeks ago

Shouldn't First option be Yes, since Admin 1 is global admin ?

upvoted 1 times

itismadu 2 months, 1 week 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 3 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



Exam AZ-104 All Actual Questions

Question #113

Topic 2

You have a Microsoft Entra tenant configured as shown in the following exhibit.

The screenshot shows the Microsoft Entra ID Overview page. At the top, there's a banner stating "Azure Active Directory is now Microsoft Entra ID." Below the banner, there are tabs for Overview, Monitoring, Properties, Recommendations, and Tutorials. The Overview tab is selected. A search bar at the bottom left contains the placeholder "Search your tenant".

Default Directory | Overview

Microsoft Entra ID

Add Manage tenants What's new Preview features

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 **Most Voted**

B. User1 and Group1 only

C. User1 and Group2 only

D. User1, Group1, and Group2

Correct Answer: A

Community vote distribution



Comments

examprepboy **Highly Voted** 2 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 13 times

Sunth65 1 week ago

<https://www.apps4rent.com/microsoft-entra-id-free-vs-p1-vs-p2-vs-governance.html>

upvoted 1 times

eduardovzermen0 2 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** 3 months 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

amsioso **Most Recent** 2 days, 19 hours ago

Selected Answer: A

Entra ID Free support only users assignment.

<https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing#licensing-requirements>

upvoted 1 times

minura 1 week, 2 days ago

Selected Answer: A

Microsoft Fabric licenses are per user licenses.

upvoted 1 times

SeMo0o0o0o 2 months, 4 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 2 months, 3 weeks ago

I even could not enable Microsoft Fabric with the Microsoft Entra ID Free license.

upvoted 1 times

155e6a0 2 months, 3 weeks ago

Please post the link that supports your answer.

upvoted 1 times

SeMo0o0o0o 3 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 2 times

27f57ef 3 months, 1 week 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 3 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 3 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 3 months, 2 weeks ago

Selected Answer: D

I think its D, Correct me if I'm wrong

upvoted 1 times

alsmk2 3 months, 2 weeks ago

Selected Answer: D

I think you can assign this to all three.

upvoted 1 times

alsmk2 3 months, 2 weeks ago

Scrap that - only if the m365 group was security-enabled, which isn't mentioned. C is correct.

upvoted 1 times



Exam AZ-104 All Actual Questions

Question #114

Topic 2

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. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

sca88 3 weeks, 2 days ago

Selected Answer: D

<https://learn.microsoft.com/en-us/azure/storage/common/sas-expiration-policy?tabs=azure-portal>
upvoted 1 times

Sweden2022 2 months, 1 week ago

Selected Answer: D

D is correct.
upvoted 1 times

SeMo0o0o0o 3 months ago

Selected Answer: D

D is correct
upvoted 1 times

KAM2023 3 months, 2 weeks ago

Selected Answer: D

Correct
upvoted 3 times

Shakka 3 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 4 times

Brzzzzz4489 2 months 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

DJHASH786 3 months, 2 weeks ago

Correct Answer
upvoted 1 times