Question #1 *Topic 1*

Your company recently created an Azure subscription.
You have been tasked with making sure that a specified user is able to implement Azure AD Privileged Identity Management (PIM).
Which of the following is the role you should assign to the user?

A. The Global administrator role.

B. The Security administrator role.

C. The Password administrator role.

D. The Compliance administrator role.

Suggested Answer: *A*
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

Community vote distribution

A (97%)

Shahrezza Highly Voted 3 years, 9 months ago
Given answer is correct.
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
upvoted 11 times

kakakayayaya Highly Voted 3 years, 10 months ago
Today, this not 100% correct. PIM ready to use without consent. Any user that have active role enables PIM.
upvoted 6 times

kktamang 3 years, 9 months ago
No. You havent got the meaning of question. "Anyone" can enable PIM and get the admin access for assigned duration but who has right and permission to assign admin role using PIM to others ? I hope its clear for you.
upvoted 1 times

khamrumunnu Most Recent 1 month, 1 week ago
Selected Answer: A
Required Role:
Only a user with the Global administrator role can enable PIM and configure it for Azure AD roles.

Why not the others?
B. Security administrator
Can manage some security settings but cannot enable or configure PIM.

C. Password administrator
Limited to password resets; no PIM-related permissions.

D. Compliance administrator
Focuses on compliance solutions like Microsoft Purview; not related to PIM setup.
upvoted 1 times

Tessy25 2 months, 2 weeks ago
Selected Answer: A
PIM itself is a high-privilege service because it controls admin role assignments.
Other roles like Security administrator, Password administrator, and Compliance administrator don't have permission to enable/configure PIM or assign roles at that level.

upvoted 1 times

hellboysecret 3 months, 2 weeks ago

Selected Answer: A

Privileged Role Administrator or Global Administrator role can manage assignments for other administrators

upvoted 1 times

siya.mthi 3 months, 3 weeks ago

Selected Answer: A

A. The Global administrator role.

Explanation:
To implement Azure AD Privileged Identity Management (PIM), a user must have elevated privileges that allow them to manage role assignments and access controls. The Global Administrator role has the highest level of permissions in Azure AD, including the ability to enable and configure Privileged Identity Management (PIM).

Why not the other options?
B. Security Administrator → Can manage security-related policies but does not have permissions to configure PIM.
C. Password Administrator → Only manages password-related tasks and cannot implement PIM.
D. Compliance Administrator → Focuses on compliance settings and auditing but lacks control over PIM.

upvoted 3 times

stonwall12 4 months, 2 weeks ago

Selected Answer: A

Answer: A, Global Administrator

Reason: Azure AD Privileged Identity Management (PIM) requires Global Administrator permissions to be configured initially. While other administrators can manage specific PIM roles once it's set up, only Global Administrators can implement and configure PIM for the first time in an Azure AD tenant.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started#prerequisites

Note: Although a Security Administrator can manage some PIM settings after initial setup, they cannot implement PIM for the first time in an organization.

upvoted 1 times

pentium75 9 months, 1 week ago

Selected Answer: A

"Only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators"
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan

Privileged Role Administrator is not an option, thus Global Administrator it is.

upvoted 3 times

Andre369 9 months, 1 week ago

Selected Answer: A

The Global administrator role has the highest level of privilege in Azure AD and provides full access to all administrative features, including the ability to configure and manage Azure AD PIM. This role allows the user to enable and configure Azure AD PIM for managing privileged roles and access in the Azure subscription.

Therefore, the correct answer is:

A. The Global administrator role.

upvoted 1 times

zellck 9 months, 1 week ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan#assign-and-activate-azure-ad-roles
For Azure AD roles in PIM, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other

administrators. Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in PIM.

upvoted 3 times

msoh9637 9 months, 1 week ago

Seems an outdated question as PIM now is automatically enabled when a P2 license enabled user logs in?
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-getting-started

When a user who is active in a privileged role in a Microsoft Entra organization with a Premium P2 license goes to Roles and administrators in Microsoft Entra ID and selects a role (or even just visits Privileged Identity Management):

"We automatically enable PIM for the organization
Their experience is now that they can either assign a "regular" role assignment or an eligible role assignment"

upvoted 1 times

QueZee 1 year, 2 months ago

B. Security administrator role

Here's why:
The Security administrator role provides the necessary permissions to manage Azure AD security features, including PIM.
It grants control over security policies, access management, and monitoring, which aligns with PIM's functionalities.

upvoted 1 times

pentium75 11 months ago

"Only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators"
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan

upvoted 1 times

MPB 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 3 times

Ashi_321 1 year, 6 months ago

B. The Security administrator role.

The Security administrator role in Azure AD is required to manage Azure AD Privileged Identity Management. This role allows the user to configure and manage PIM settings, including configuring role assignments, activating PIM for specific roles, and managing the PIM security settings.

upvoted 2 times

wardy1983 1 year, 7 months ago

To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com

upvoted 1 times

ESAJRR 1 year, 12 months ago

Selected Answer: A

A. The Global administrator role.

upvoted 1 times

JunetGoyal 2 years, 1 month ago

In real world you should always give Privileged Role Administrator over global admin
For Azure AD roles in Privileged Identity Management, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators. Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in Privileged Identity Management.

upvoted 1 times

Question #2 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of pass-through authentication and seamless SSO with password hash synchronization.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*
For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Community vote distribution
A (76%) B (24%)

kakakayayaya Highly Voted 3 years, 10 months ago
We have 3 options for solution:
1) Password hash synchronization + Seamless SSO
2) Pass-through Authentication + Seamless SSO
3) Federation with AD FS
1 - doesn't support "password policies and user logon limitations".
2 and 3 - support, but 3 requres more servers.
upvoted 56 times

kakakayayaya 3 years, 10 months ago
.. so answer YES
upvoted 5 times

omw2wealth 3 years, 7 months ago
Exactly.
upvoted 1 times

cfsxtuv33 3 years, 6 months ago
I will have to agree with this assessment based on supporting evidence and kakakayayaya "options for solution."
upvoted 1 times

ThatDowntownSmell 2 years, 8 months ago
There is a 4th option not listed: Pass-through Auth+Seamless SSO with Password Hash Sync:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 4 times

moutaz1983 Highly Voted 3 years, 10 months ago
I will go Yes here because this password policy enfocement can be done only using Pass through auth

See decision tree: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
upvoted 22 times

Shahrezza 3 years, 9 months ago
Agree with answer : YES . The decision tree support this

upvoted 4 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: A

Answer: A, Yes

Reason: Pass-through authentication with password hash sync meets the goals by enforcing on-premises password policies while providing backup authentication, all with minimal server infrastructure.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn#cloud-authentication-pass-through-authentication

upvoted 1 times

somenick 9 months, 1 week ago

Selected Answer: A

We have 3 options for solution:
1) Password hash synchronization + Seamless SSO
2) Pass-through Authentication + Seamless SSO
3) Federation with AD FS
1 - doesn't support "password policies and user logon limitations".
2 and 3 - support, but 3 requres more servers.

upvoted 4 times

fahrulnizam 9 months, 1 week ago

Selected Answer: A

"must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant"
keyword here in this question is 'synced'. So, answer is YES

Password hash synchronization. A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD.

Pass-through authentication. A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.

upvoted 3 times

fr3ngdf 9 months, 1 week ago

Selected Answer: A

Answer is A (YES)

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

"Azure AD Password Hash Synchronization (...) provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead"

upvoted 3 times

zellck 9 months, 1 week ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn#cloud-authentication-pass-through-authentication
- Effort.
For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

upvoted 1 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn#cloud-authentication
Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method.

upvoted 1 times

BigShot0 9 months, 1 week ago

Selected Answer: A

Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn

upvoted 1 times

123lmn 9 months, 1 week ago

Selected Answer: A

the solution of using pass-through authentication and seamless Single Sign-On (SSO) with password hash synchronization aligns with your goal of integrating Active Directory and the Azure AD tenant while ensuring that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant. Additionally, this solution helps reduce the number of necessary servers as it doesn't require additional infrastructure components like federation servers, which would be the case if you were to implement Active Directory Federation Services (AD FS) for SSO.

In summary, the proposed solution is a valid and efficient approach for achieving the integration and meeting the specified requirements.

upvoted 1 times

yonie 9 months, 1 week ago

Selected Answer: A

Answer is YES

organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn

See also: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn#decision-tree

upvoted 1 times

pentium75 9 months, 1 week ago

Selected Answer: A

"Make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant" - requires pass-through authentication or federation

"amount of necessary servers are reduced" - federation would require additional servers while pass-through does not

So we need pass-through authentication, which is part of the suggested solution here. Additional (!) password hash sync for seamless SSO is not required by the question, but it doesn't harm.

upvoted 2 times

Ruffyit 1 year, 2 months ago

We have 3 options for solution:
1) Password hash synchronization + Seamless SSO
2) Pass-through Authentication + Seamless SSO
3) Federation with AD FS
1 - doesn't support "password policies and user logon limitations".
2 and 3 - support, but 3 requres more servers.

upvoted 1 times

examexamtopics 1 year, 3 months ago

Yes, the solution does meet the goal.
Azure AD Connect with pass-through authentication and seamless Single Sign-On (SSO) with password hash synchronization would allow you to integrate your on-premises Active Directory with Azure AD.

Pass-through authentication allows users to use the same username and password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.

Seamless SSO automatically signs users in when they are on their corporate devices connected to your corporate network, providing a more integrated experience.

Password hash synchronization is an extension to the same sign-on feature where the hash of the on-premises AD user's password is synchronized to Azure AD, which can help reduce the number of servers since you don't need to deploy Active Directory Federation Services (ADFS).

upvoted 1 times

Jastix 1 year, 4 months ago

Answer = B

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn

upvoted 1 times

b9e98e8 1 year, 4 months ago

PTA requires OnPrem AD to process authentication and PHS requires Azure AD to process authentication. If you want to reduce on prem servers using SSO then you should recommend PTA with SSO but not PHS with SSO.

upvoted 1 times

wardy1983 1 year, 7 months ago

Yes" - the main sign-in method is PTA fulfills the requirements and the PH sync is just for failover and for Identity protection. It is also recommended to do.

Azure AD Identity Protection requires Password Hash Sync regardless of which sign-in method you choose, to provide the Users with leaked credentials report. Organizations can fail over to Password Hash Sync if their primary sign-in method fails and it was configured before the failure event.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 1 times

Ssc91 1 year, 7 months ago

Selected Answer: B

Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn

upvoted 1 times

upvoted 1 times

Question #3 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of federation with Active Directory Federation Services (AD FS).
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*
A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Community vote distribution
B (100%)

⊟ **trevax** Highly Voted 3 years, 10 months ago
- "password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant" → Federation or PTA
- "the amount of necessary servers are reduced" → Federation > PTA > PHS (number of server)

So the answer is PTA.
upvoted 18 times

⊟ **Shahrezza** 3 years, 9 months ago
Agreed answer is : PTA
upvoted 1 times

⊟ **cometoit** 3 years, 8 months ago
Agreed, while federation would force user logon limitations it would require minimum 4 servers (2 ADFS/2 WAP).
upvoted 1 times

⊟ **LeDefatman** Highly Voted 3 years, 9 months ago
the phrase ...amount of necessary servers is reduced eliminate Federation as an answer choice.
upvoted 7 times

⊟ **Tessy25** Most Recent 2 months, 2 weeks ago
Selected Answer: B
While federation with AD FS enforces real-time password policies, it increases server count, violating the "reduce number of servers" requirement
upvoted 1 times

⊟ **stonwall12** 4 months, 2 weeks ago
Selected Answer: B
Answer: B, No

Reason: Federation with AD FS doesn't meet the requirement to reduce server count as it requires additional infrastructure including multiple AD FS servers and web application proxies for high availability.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn#federation-authentication-with-ad-fs
upvoted 1 times

Vaibhav39 5 months, 3 weeks ago

Selected Answer: B

No password write back is needed

upvoted 1 times

rysano 10 months, 3 weeks ago

the phrase ...amount of necessary servers is reduced eliminate Federation as an answer choice. Guide:
https://sites.google.com/view/learnmicrosoftcomenustrainingm/home

upvoted 2 times

pentium75 11 months ago

Selected Answer: B

No because ADFS does anything but 'reduce the amount of necessary servers'.

upvoted 1 times

Ruffyit 1 year, 2 months ago

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

upvoted 2 times

ESAJRR 1 year, 12 months ago

Selected Answer: B

B. Answer is No

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn#cloud-authentication
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?
Federation with AD FS
- Two or more AD FS servers
- Two or more WAP servers in the perimeter/DMZ network

upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. Answer is No

upvoted 1 times

Fal991l 2 years, 4 months ago

the solution of using federation with Active Directory Federation Services (AD FS) meets the goal of integrating Active Directory and the Azure AD tenant while making sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and reducing the number of necessary servers.

Federation with AD FS allows for a single sign-on (SSO) experience for users, where they can authenticate with their on-premises Active Directory credentials and gain access to resources in both the on-premises environment and in the cloud. This ensures that password policies and user logon limitations applied to on-premises Active Directory also apply to Azure AD.(ChatGPT)

upvoted 1 times

AZ5cert 2 years, 6 months ago

B. No
AD FS will trust third party trusted domains across the enterprise for seamless authentication

upvoted 1 times

salmantarik 2 years, 6 months ago

The correct answer is B
However, correct answer is SSO + PHS as it enforces two password policies (Password complexity policy and Password expiration policy also User Logon Restrictions) and it doesnt require any agents.

upvoted 1 times

God2029 2 years, 7 months ago

Can go with PTA and Standby PHS. Need to think of ADFS only when third party application authentication is required. Question doesn't speak about third-party apps. So you don't need ADFS.

upvoted 1 times

MarcusPlexus 2 years, 9 months ago

The 'correct answer' misses the point. You have recommended (in a badly stated fashion) 2 options: (1) PTA and (2) PHS with SSO. Option 2 does not care about your on prem settings, but option 1 does. Since you recommend both options and only one does the job, mission failed. This answer is incorrect (but not for the reason mentioned in 'correct answer').

upvoted 1 times

TheLegendPasha 3 years, 2 months ago

Selected Answer: B

Less server means instantly not federation.

upvoted 3 times

Question #4 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of password hash synchronization and seamless SSO.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Community vote distribution
B (88%) 12%

⊟ **Dushank** Highly Voted 👍 3 years, 11 months ago
Answer should be "No"
password hash synchronization cannot support the password policies and user logon limitations
For this you need to implement Pass-through authentication
upvoted 46 times

⊟ **rawrkadia** 3 years, 10 months ago
Correction, it does somewhat support password policies like complexity, (but does not support expiration) and does not support logon restrictions at all.

There's about 20 versions of this question in the dump and I'm glad by this point people are arriving at the correct answer and realizing PHS doesn't work for the use case. :)
upvoted 8 times

⊟ **kakakayayaya** Highly Voted 👍 3 years, 10 months ago
There are 3 options for solution:
1) Password hash synchronization + Seamless SSO
2) Pass-through Authentication + Seamless SSO
3) Federation with AD FS
1 - doesn't support "password policies and user logon limitations".
upvoted 21 times

⊟ **kakakayayaya** 3 years, 10 months ago
So answer is NO
upvoted 9 times

⊟ **stonwall12** Most Recent ⏲ 4 months, 2 weeks ago
Selected Answer: B
Answer: B, No

Reason: Password hash synchronization with seamless SSO doesn't meet the goal as it doesn't enforce on-premises password policies and logon restrictions since authentication happens in the cloud.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-password-hash-synchronization

upvoted 1 times

ITFranz 6 months ago

Selected Answer: B

To Support the answer:

Password hash synchronization (PHS) partially supports on-premises password policies and user logon limitations, but with some important caveats:

Password policies: PHS respects the on-premises Active Directory password policies to some extent. When users change their passwords on-premises, these changes are synchronized to Azure AD, ensuring that the same password complexity and expiration rules apply14.

User logon limitations: PHS does not fully support all on-premises user logon limitations. For example:

If an account is expired but still active in on-premises AD, cloud authentication through Azure AD may still succeed, even though an on-premises sign-on would fail4.

Not all Active Directory policies are respected in the cloud environment when using PHS

Answer = B

upvoted 1 times

awfnewf1q243 9 months, 1 week ago

Selected Answer: B

B. No

Correct path through the decision tree is Yes -> Yes -> No -> No, which results in "Pass-though Auth + Seamless SSO"

The only reason we would want PHS is if we answered "No" to "Do you want to enforce user-level Active Directory security policies during sign in?"

The stated objective is "make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant"

If you read footnote #3 of the decision tree it says "If you need to apply, user-level Active Directory security policies such as account expired, disabled account, password expired, account locked out, and sign-in hours on each user sign-in, Azure AD requires some on-premises components."

Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#decision-tree

upvoted 2 times

pentium75 11 months ago

Selected Answer: B

No because "[some] password policies [like expiration] and user logon limitations" are not supported by password hash sync

upvoted 1 times

b9e98e8 1 year, 4 months ago

PHS ensures that the password complexity policies from your on-premises AD instance override the complexity policies in the cloud for synchronized users1.

For PHS If your AD enforces specific password complexity rules (e.g., minimum length, character requirements), those rules apply to synchronized users accessing Microsoft Entra services.

For PHS if your on-premises AD enforces password expiration (e.g., passwords must be changed every 90 days), that policy remains in effect.

upvoted 2 times

wardy1983 1 year, 7 months ago

Answer: B

Explanation:

password hash synchronization cannot support the password policies and user logon limitations For this you need to implement Pass-through authentication

upvoted 1 times

[Removed] 1 year, 8 months ago

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn

Use the decision making chart and answer is NO

upvoted 2 times

MeisAdriano 1 year, 8 months ago

Selected Answer: B

Absolutelly NO

upvoted 1 times

JunetGoyal 1 year, 8 months ago

NO, Coz of this line "make sure that password policies and user logon limitations "

Example: Organisation has user policy that user can login for specific date & time which is example of "make sure that password policies and user logon limitations ", Sp we cannot use PHS.

We need Pass through.

Ans for all situations: Pass through -- yes

ADFS- NO

PHS-NO

upvoted 2 times

BigShot0 1 year, 9 months ago

Selected Answer: B

You cannot enforce logon requirements with this solution.

upvoted 1 times

ESAJRR 1 year, 12 months ago

Selected Answer: B

B. Answer is No

upvoted 1 times

jambarka 2 years, 2 months ago

Selected Answer: A

hash sync simply syncs the hashes of passwords that already onprem ADDS policies.

User logon limitations are reflected by account properties affecting its state, which get synced with the account and should be supported

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. Answer is No

upvoted 1 times

tichyrb 2 years, 5 months ago

The reference in the explanation is the PTA link (:

upvoted 2 times

Seelearndo 2 years, 5 months ago

Selected Answer: B

Password policy enforcement can be done only using Pass through authentication. https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 1 times

Question #5 *Topic 1*

Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to

Azure AD.

Which of the following actions should you take?

A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.

B. You should configure a DNAT rule on the Firewall.

C. You should configure a network traffic filtering rule on the Firewall.

D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

Suggested Answer: *A*

Use the Synchronization Rules Editor and write attribute-based filtering rule.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

Community vote distribution

A (100%)

⊟ **nexel** Highly Voted 3 years, 11 months ago

Should be A

upvoted 18 times

⊟ **CK9797** Highly Voted 2 years, 7 months ago

40 Questions

1 Case Study = 6 Questions

1 Lab = 10 Tasks - You need to be comfortable navigating in Azure

Total 56 Questions

Some new questions, most are from this site. Big thank you to Exam Topics and everyone for their comments. Rule of thumb, go with the most votes.

upvoted 10 times

⊟ **stonwall12** Most Recent 4 months, 2 weeks ago

Selected Answer: A

Answer: A, Synchronization Rules Editor

Reason: Synchronization Rules Editor is the correct tool for creating attribute-based filtering rules in Azure AD Connect to control which objects sync to Azure AD based on their attributes.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration#create-an-attribute-based-filtering-rule

upvoted 3 times

⊟ **pentium75** 11 months ago

Selected Answer: A

A, because it's correct while everything else is nonsense

upvoted 3 times

⊟ **Ruffyit** 1 year, 2 months ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fix-default-rules

upvoted 1 times

⊟ **ESAJRR** 1 year, 10 months ago

Selected Answer: A

A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.

upvoted 1 times

⊟ **ESAJRR** 1 year, 12 months ago

Selected Answer: A

A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.

upvoted 1 times

⊟ **JunetGoyal** 2 years, 1 month ago

There are 4 types of filter you can apply: 1.Domain base 2 OU 3. Group base 4. Attribute base in AD connect!!

As per ques we will put attribute base filter!! So A

upvoted 2 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-create-custom-sync-rule

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these

upvoted 1 times

⊟ **majstor86** 2 years, 4 months ago

Selected Answer: A

A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.

upvoted 2 times

⊟ **God2029** 2 years, 7 months ago

Agreed. It is A

upvoted 1 times

⊟ **mung** 2 years, 7 months ago

B,C, and D is definitely No so no choice other than A

upvoted 1 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: A

A is the only correct answer.

upvoted 3 times

⊟ **DarkCyberGhost** 3 years, 5 months ago

Agree it is A

upvoted 1 times

⊟ **giladliam** 3 years, 5 months ago

Selected Answer: A

aaaaaaaaa

upvoted 1 times

⊟ **BinuHaneef** 3 years, 6 months ago

Selected Answer: A

Correct

upvoted 1 times

⊟ **AS179** 3 years, 6 months ago

Selected Answer: A

correct

upvoted 1 times

Question #6 *Topic 1*

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).
The process involves assessing the risk events and risk levels.
Which of the following is the risk level that should be configured for users that have leaked credentials?

A. None

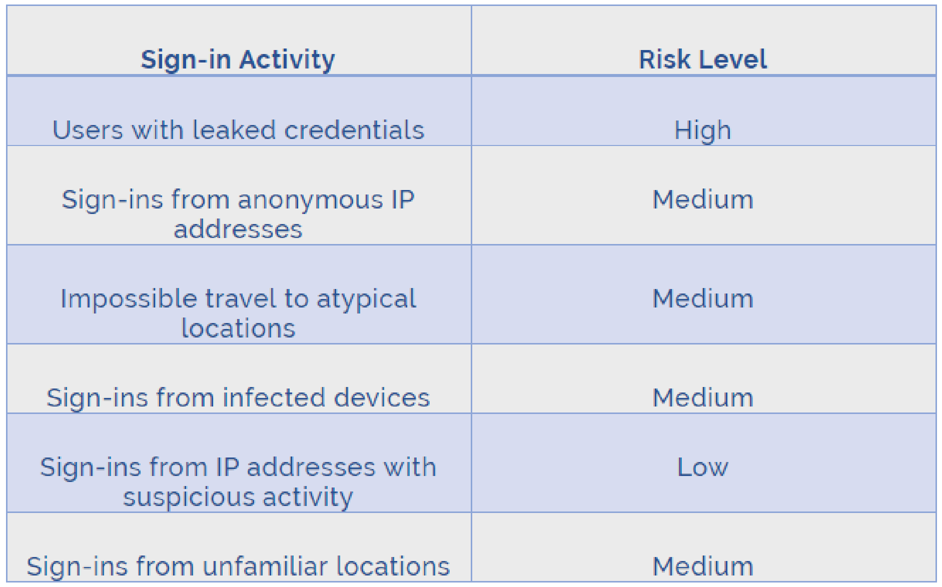
B. Low

C. Medium

D. High

Suggested Answer: *D*

These six types of events are categorized in to 3 levels of risks ג€" High, Medium & Low:



Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Reference:

http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

Community vote distribution

D (92%) 8%

greatadhesiveness Highly Voted 3 years, 11 months ago

Yes, he's High!

upvoted 21 times

us3r 3 years, 3 months ago

cheers

upvoted 1 times

awfnewf1q243 Highly Voted 9 months, 1 week ago

Selected Answer: D

D. High

Note: It is very unlikely the Microsoft will require the memorization of specific risk levels given that they have changed the documentation.

Previously the risk levels were very well defined, however they now provide this very vague paragraph:

"Microsoft doesn't provide specific details about how risk is calculated. Each level of risk brings higher confidence that the user or sign-in is compromised. For example, something like one instance of unfamiliar sign-in properties for a user might not be as threatening as leaked credentials for another user."

Modern Documentation: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#investigate-risk

Legacy Documentation: https://web.archive.org/web/20190419234045/https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events

upvoted 9 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: D

Answer: D, High

Reason: Leaked credentials are classified as a high-risk level in Azure AD Identity Protection because they indicate that valid username/password combinations are available to malicious actors, posing a significant security threat to the organization.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#risk-levels

upvoted 1 times

Vaibhav39 5 months, 3 weeks ago

Selected Answer: D

Risk level define is high

upvoted 1 times

ITFranz 6 months ago

Selected Answer: D

To support the answer:
When a user has leaked credentials detected in Azure, the risk level is typically set to "High" in Conditional Access policies. This is because leaked credentials pose a significant security threat, as they indicate that the user's valid credentials have been compromised and are potentially available to unauthorized parties.
To configure a Conditional Access policy for leaked credentials:
In the Azure portal, navigate to Microsoft Entra ID > Security > Conditional Access.
Create a new policy or edit an existing one.
Under "Conditions", select "User risk".
Set "Configure" to "Yes".
Choose "High" as the risk level.
By setting the risk level to "High" for leaked credentials, you ensure that the policy takes immediate action when such a threat is detected, such as requiring a password reset or multi-factor authentication
Answer = D

upvoted 1 times

Fal991l 9 months, 1 week ago

Selected Answer: D

The risk level that should be configured for users that have leaked credentials in a conditional access policy is High.

When a user's credentials are leaked, it means that their username and password have been compromised and are potentially in the hands of an attacker. This puts the user's account and the resources that they have access to at a high level of risk, making it important to apply strict access controls and security measures.

By setting the risk level to High, conditional access policies can be configured to enforce stricter security measures, such as requiring multifactor authentication or blocking access to certain resources entirely.
Therefore, the correct answer is D. High.

upvoted 2 times

zellck 9 months, 1 week ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-user-accounts#unusual-sign-ins
Leaked credentials user risk detection
- Risk Level: High

upvoted 1 times

xRiot007 11 months, 2 weeks ago

If your users credentials are leaked, you are yiffed, so it should always be the highest risk value, in this case "High"

upvoted 2 times

Urqlexandra 1 year, 9 months ago

Selected Answer: D

Yes, It's High!

upvoted 2 times

ESAJRR 1 year, 12 months ago

Selected Answer: D

D. High

upvoted 2 times

Holii 2 years, 1 month ago

Someone confirm if these questions are still on the exam. These are no longer up to date, and now analyzed as Real-Time and Offline.

upvoted 3 times

Andre369 2 years, 2 months ago

Selected Answer: D

The correct answer is D

upvoted 1 times

pekay 2 years, 3 months ago

Selected Answer: A

High is the right answer

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: D

D. High

upvoted 2 times

AZ5cert 2 years, 6 months ago

D: High

upvoted 1 times

salmantarik 2 years, 6 months ago

The question is outdated and not relevant now

upvoted 2 times

God2029 2 years, 7 months ago

Use logic and think like a security professional, users with Leaked credentials are always at high risk. Imagine the user is global admin. MFA is there, but still it is high risk.

Nothing is secure and privacy is a myth before Advance Persistent Threat.

upvoted 2 times

Question #7 *Topic 1*

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).
The process involves assessing the risk events and risk levels.
Which of the following is the risk level that should be configured for sign ins that originate from IP addresses with dubious activity?

A. None

B. Low

C. Medium

D. High

Suggested Answer: *C*
Reference:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

Community vote distribution
C (69%) B (31%)

⊟ **Ucy** Highly Voted 3 years, 12 months ago
Correct Answer is B
IP addresses with suspicious/dubious activity risk level is LOW
upvoted 50 times

⊟ **bur88** 3 years, 3 months ago
Update: in 2022 it is C : Medium already
https://github.com/toddkitta/azure-content/blob/master/articles/active-directory/active-directory-identityprotection-risk-events-types.md#sign-ins-from-ip-addresses-with-suspicious-activity
upvoted 26 times

⊟ **koreshio** 2 years, 8 months ago
I think this should be 'Medium' too considering the "Microsoft's recommendation" section under this doco:
https://learn.microsoft.com/sr-cyrl-rs/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies
upvoted 2 times

⊟ **siecz** 3 years, 3 months ago
This repo last commit if from 2016... is it u to date ???
upvoted 6 times

⊟ **thienvupt** Highly Voted 3 years, 12 months ago
The same with Sign-ins from IP addresses with suspicious activity
so B is correct
upvoted 15 times

⊟ **Knighthell** Most Recent 3 weeks, 1 day ago
Selected Answer: C
Medium
upvoted 1 times

⊟ **stonwall12** 4 months, 2 weeks ago
Selected Answer: C
Answer: C, Medium

Reason: Sign-ins from IP addresses with suspicious activity are classified as medium-risk in Azure AD Identity Protection. It was consisted LOW, but was updated a couple years back.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#risk-levels
upvoted 2 times

⊟ **awfnewf1q243** 9 months, 1 week ago
Selected Answer: C

C. Medium

Note: It is very unlikely the Microsoft will require the memorization of specific risk levels given that they have changed the documentation.

Previously the risk levels were very well defined, however they now provide this very vague paragraph:

"Microsoft doesn't provide specific details about how risk is calculated. Each level of risk brings higher confidence that the user or sign-in is compromised. For example, something like one instance of unfamiliar sign-in properties for a user might not be as threatening as leaked credentials for another user."

Modern Documentation: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#investigate-risk

Legacy Documentation: https://web.archive.org/web/20190419234045/https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events

upvoted 9 times

ittchmh 9 months, 1 week ago

Selected Answer: C

Latest information on MS Learn:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks?source=recommendations#risk-levels

Risk levels
Identity Protection categorizes risk into three tiers: low, medium, and high. When configuring Identity protection policies, you can also configure it to trigger upon No risk level. No Risk means there's no active indication that the user's identity has been compromised.

Microsoft doesn't provide specific details about how risk is calculated. Each level of risk brings higher confidence that the user or sign-in is compromised. For example, something like one instance of unfamiliar sign-in properties for a user might not be as threatening as leaked credentials for another user.

upvoted 5 times

MeisAdriano 9 months, 1 week ago

Selected Answer: B

ChatGPT:

1) Low Risk Level:

Use this level if you believe the suspicious activity is low-risk or if you are conducting further investigations.
It may be appropriate for situations where the IP address is not well-known as a source of malicious activity.

2) Medium Risk Level:

This risk level is a common choice and represents a compromise between security and convenience.
It might be suitable for suspicious activities that have some level of risk but are not considered severe.

3) High Risk Level:

Use this level if you believe the suspicious activity represents a serious and immediate threat.
It may require additional authentication and security verification to mitigate the risk.

upvoted 1 times

Jimmy500 9 months, 1 week ago

Leaked Credentials = High
Impossible travel to atypical locations =Medium
Sign IN from infected device =Low
Sign-ins from anonymous Ip addresses = Medium
Sign-ins from Ip address with suspicious Activity = Medium
Sign-ins from unfamiliar locations = Medium

upvoted 2 times

WilianCArias 1 year, 6 months ago

Answer is LOW

upvoted 3 times

⊟ **flafernan** 1 year, 6 months ago

Selected Answer: C

This rating was upgraded in 2022 and went from low to medium.

upvoted 3 times

⊟ **cometorule** 1 year, 7 months ago

can you guys please stop asking ChatGPT for the answers? if you have answers based on Microsoft document, then state it in the comments, otherwise stfu.

upvoted 6 times

⊟ **JunetGoyal** 1 year, 8 months ago

Its Low

upvoted 1 times

⊟ **timHAG** 1 year, 11 months ago

Selected Answer: C

updated categorization

upvoted 1 times

⊟ **ESAJRR** 1 year, 11 months ago

Selected Answer: C

C. Medium

upvoted 1 times

⊟ **Khairulanuar** 2 years, 1 month ago

correct asnwer is C

upvoted 1 times

⊟ **slick_orange** 2 years, 2 months ago

Selected Answer: C

Correct Answer is C

Question outdated: It's C for now, only "Sign-ins from infected devices" is a "low" risk.

Check with the link: https://github.com/toddkitta/azure-content/blob/master/articles/active-directory/active-directory-identityprotection-risk-events-types.md

upvoted 6 times

⊟ **Strive_for_greatness_kc** 1 year, 5 months ago

Last update from this page is 2016, 9 years ago.

upvoted 1 times

⊟ **Andre369** 2 years, 2 months ago

Selected Answer: B

I'm going with B it seems to match the question best

upvoted 1 times

Question #8 *Topic 1*

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.
You start by creating an access review program and an access review control.
You now need to configure the Reviewers.
Which of the following should you set Reviewers to?

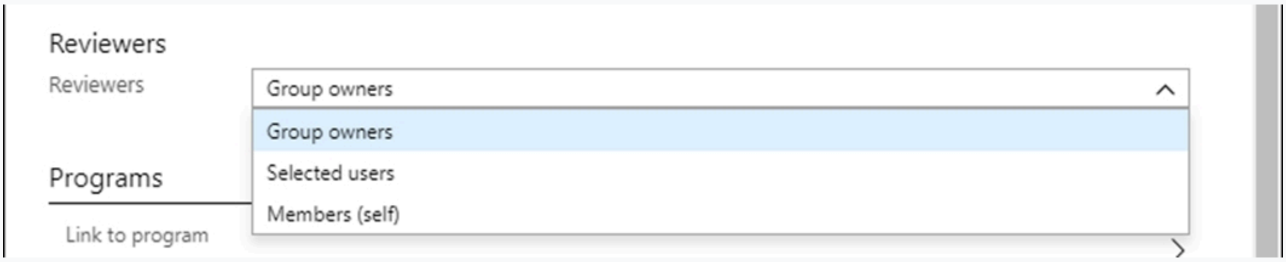
A. Selected users.

B. Members (Self).

C. Group Owners.

D. Anyone.

Suggested Answer: *C*
In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

Community vote distribution
C (85%) A (15%)

ssidlabs Highly Voted 3 years, 8 months ago
"You also have to make sure that the reviews can be reviewed by resource owners.". If you see here it's talking about "resource owners" and it no where in the question says that Access Review needs to be created for evaluation of groups. Hence the Answer C should be incorrect. Correct answer should be A, because different resources may have different owners, hence you can select accordingly as reviewer.
upvoted 23 times

arseyam 3 years, 2 months ago
Because it's mentioned in the question "you start by creating an access review program" then it can't be used with ARM access reviews as programs are used to review group memberships and application access only. Therefore the correct answer is "group owners"
upvoted 5 times

theOldOne 3 years, 8 months ago
I was thinking the same thing.
upvoted 2 times

mung 2 years, 7 months ago
I would definitely go with A.
upvoted 1 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: C
Answer: C, Group Owners

Reason: When you want resource owners to review access, you should select "Group Owners" as the reviewer type. This ensures that the owners of the resources can review and manage access to their resources directly.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review#select-reviewers
upvoted 1 times

codeunit 8 months, 3 weeks ago

For configuring reviewers to ensure that reviews can be conducted by resource owners, you should set the Reviewers option to “Resource Owners” or “Group Owners”, depending on the access review solution you’re using.

In many access review tools, assigning the resource or group owners as reviewers allows them to evaluate and approve access rights to their respective resources. This aligns with your requirement for resource owners to be the reviewers.

If the available options specifically include “Resource Owners”, that would be the correct choice.

upvoted 1 times

MeisAdriano 9 months, 1 week ago

Selected Answer: A

I am not really sure about the answer.
The question says "the reviews can be reviewed by resource owners" not by "owner group"; "resource owners" should be different to "owner group members"

Here:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
- Group owner(s): This option is only available when you do a review on a team or group.

I think the question is poorly phrased, I hope it won't be in exam worded like this.

upvoted 4 times

shashii82 9 months, 1 week ago

Based on the task of configuring an access review where you want resource owners to review the access, the most appropriate choice for setting the Reviewers would be:

C. Group Owners.

Explanation:

"Group Owners" refers to the owners or administrators of the groups or resources being reviewed. These individuals typically have the necessary permissions and authority to review and manage access to the resources.
By setting the Reviewers to "Group Owners", you ensure that the access review will be performed by those who are directly responsible for the resources or groups being reviewed. This helps ensure that access permissions are accurately assessed and validated by the appropriate stakeholders.

upvoted 2 times

2dc6125 1 year ago

Are you sure? Be cause resource owner don't need to be a group owner which means a resource in a group can have an owner that is not a group owner

upvoted 1 times

Jimmy500 1 year ago

You also have to make sure that the reviews can be reviewed by resource owners means Group owner .If we choose self we can chose someone who is not owner of group but in the condition it says we have to make sure the reviewers can be review by resource owners.

upvoted 1 times

2dc6125 1 year ago

Resource owner can be different from group owners. Example you can have vm assigned ownership to a user is not a group owner of where the vm inside that group

upvoted 1 times

NotAChatBot 1 year, 6 months ago

B. Members (Self).
The question states" You also have to make sure that the reviews can be reviewed by resource owners." That implies that the review is a PIM review not Identity governance one - witch could be group or application not a resource. The options for Reviewers are "Selected users or groups", "Members(self)" or "Managers". Only "Members (self)" from the list is available option in PIM.

upvoted 1 times

wardy1983 1 year, 7 months ago

Answer: C

Explanation:

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review

upvoted 1 times

ESAJRR 1 year, 10 months ago

Selected Answer: C

C. Group Owners.

upvoted 3 times

ESAJRR 1 year, 12 months ago

Selected Answer: C

C. Group Owners.

upvoted 2 times

JunetGoyal 2 years, 1 month ago

Let me Clear it: there are two types of access reviews: AD role and RBAC.

AD role access review are for just AD level and RBAC for resources(VM,storage, bla-bla).

As question says resources owner does not mean groups.

The correct ans is A.

upvoted 3 times

Andre369 2 years, 2 months ago

Selected Answer: C

I am going with C thinking someone has to have posed this question to their lecturer/intelligent person and that's why it's most voted

upvoted 1 times

MeisAdriano 1 year, 8 months ago

Wtf...

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: C

C. Group Owners.

upvoted 1 times

asaulu 2 years, 6 months ago

I think the correct answer is A, because the question doesn't say the review source is a Group or Application. Therefore, you can assign a specific user for an application as a Reviewer while you can assign a Group Owner as a group resource. There is a little trick in the Q.

upvoted 2 times

koreshio 2 years, 8 months ago

bit confused about this one. there is an 'Access Reviews' option under PIM (Privileged Identity Management) and the options there for reviewers are:

Selected Users, Members (self), Manager

see (step 14) below:

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review

upvoted 1 times

koreshio 9 months, 1 week ago

actually bit more digging below and this answers my question. so I agree it should be 'C - Group Owners'

Difference between Access Review in Identity Governance and Privileged Identity Management:

"Kind of the same thing, but not exactly. It's the same engine, but covers different objects. Access reviews under Identity Governance cover Groups/Teams and application access, whereas Access reviews for admin roles is what PIM does. Refer to this article for comparison"

ref:

https://learn.microsoft.com/en-us/answers/questions/1036421/difference-between-access-review-in-identity-gover.html

upvoted 3 times

God2029 2 years, 7 months ago

Koreshio's explanation is correct. C is the answer

upvoted 1 times

⊟ **koreshio** 2 years, 8 months ago

therefore should'nt this be B - Members (self) , based on above doco?

upvoted 2 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 2 times

⊟ **Chun** 3 years, 3 months ago

Selected Answer: C

Correct

upvoted 2 times

Question #9 *Topic 1*

Your company recently created an Azure subscription. You have, subsequently, been tasked with making sure that you are able to secure Azure AD roles by making use of Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
Which of the following actions should you take FIRST?

A. You should sign up Azure Active Directory (Azure AD) Privileged Identity Management (PIM) for Azure AD roles.

B. You should consent to Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

C. You should discover privileged roles.

D. You should discover resources.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

Community vote distribution
C (47%) D (37%) Other

⊟ **Rume** Highly Voted 4 years ago
"Consent to PIM" is deprecated. No more required.
So now only priv users needs to access/ visits PIM (Premium P2 is enabled") - Access will be provided automatically.

"When a user who is active in a privileged role in an Azure AD organization with a Premium P2 license goes to Roles and administrators in Azure AD and selects a role (or even just visits Privileged Identity Management):

We automatically enable PIM for the organization
Their experience is now that they can either assign a "regular" role assignment or an eligible role assignment"
upvoted 46 times

⊟ **Bjarki2330** 3 years, 11 months ago
Yeah this question in particular is outdated.
upvoted 5 times

⊟ **Hot_156** 4 months ago
AOUTDATED

Prepare PIM for Microsoft Entra roles
Here are the tasks we recommend for you to prepare Privileged Identity Management to manage Microsoft Entra roles:

Configure Microsoft Entra role settings
Give eligible assignments
Allow eligible users to activate their Microsoft Entra role just-in-time
Prepare PIM for Azure roles
Here are the tasks we recommend for you to prepare Privileged Identity Management to manage Azure roles for a subscription:

Discover Azure resources
Configure Azure role settings
Give eligible assignments
Allow eligible users to activate their Azure roles just-in-time

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-getting-started#prepare-pim-for-azure-roles
upvoted 1 times

⊟ **cris_exam** Highly Voted 9 months, 1 week ago
Selected Answer: D
Correct answer is D. First thing you do is Discover Azure resources.

1. Discover Azure resources
2. Configure Azure role settings.
3. Give eligible assignments.
4. Allow eligible users to activate their Azure roles just-in-time.

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-getting-started#prepare-pim-for-azure-roles

upvoted 10 times

⊟ **Jimmy500** 1 year ago

Hi please read question carefully , it does not say Enable role for Azure subscription, Your solution is correct but it is for Azure Subscription not Azure Roles. So since we are not talking about resources we must choose C. If in the condiition it says for Azure resource we must chose D in this case - Discover Azure resources.

upvoted 6 times

⊟ **Rednevi** 3 months, 1 week ago

Actually according to Learn:
"Prepare PIM for Azure roles
Here are the tasks we recommend for you to prepare Privileged Identity Management to manage Azure roles for a subscription:
1) Discover Azure resources
2) Configure Azure role settings
3) Give eligible assignments
4) Allow eligible users to activate their Azure roles just-in-time"

D seems correct

upvoted 2 times

⊟ **Agwuocha** Most Recent 2 weeks, 3 days ago

Selected Answer: B

A year 2025 version of this questions would look like this:

Your company has an Azure subscription integrated with an Entra ID tenant. You need to secure Azure AD roles using Privileged Identity Management (PIM), minimizing standing privileges and using just-in-time access where possible.

What is the first action you should take to prepare?

A. Discover existing Azure resource and Entra roles
B. Sign up for PIM in the Entra tenant
C. Consent to PIM from an Entra administrator account
D. Discover resources to protect with PIM

The correct answer would be B: Sign up for PIM in the Entra tenant

You must first enable the PIM service in Entra ID Governance or P2 license terms. This step appears when you first open the “Privileged Identity Management” blade—essentially “turning on PIM” for your tenant.
Without doing this, no other PIM configuration (like discovering roles or resources) is available in the portal.

upvoted 1 times

⊟ **Knighthell** 3 weeks, 3 days ago

Selected Answer: C

List who has privileged roles in your organization. Review the users assigned, identify administrators who no longer need the role, and remove them from their assignments.

upvoted 1 times

⊟ **a59c97f** 1 month, 1 week ago

Selected Answer: D

Accoding to the MS Doc:
When you first set up Privileged Identity Management for Azure resources, you need to discover and select the resources you want to protect with Privileged Identity Management.

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-resource-roles-discover-resources

upvoted 1 times

cuongdo1793 1 month, 1 week ago

Selected Answer: D

D , no more https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-getting-started#prepare-pim-for-azure-roles

upvoted 1 times

mmmyo 1 month, 3 weeks ago

Selected Answer: A

The correct first step in securing Azure AD roles using Privileged Identity Management (PIM) is A. You should sign up for Azure AD Privileged Identity Management (PIM) for Azure AD roles.

Here's why: Before you can manage and secure privileged roles with PIM, your organization must first activate PIM for Azure AD roles. This step enables role assignments to be eligible, providing just-in-time access, approval workflows, and auditing capabilities for privileged roles.

Once PIM is enabled, the next logical steps would be:

Discover Privileged Roles (C) to identify which roles are currently assigned.

Consent to PIM (B) to ensure necessary permissions are in place.

Discover Resources (D) if you're expanding PIM governance beyond Azure AD into Azure resources.

upvoted 1 times

gauravwagh16193 2 months, 3 weeks ago

Selected Answer: A

To secure Azure AD roles using Azure AD Privileged Identity Management (PIM), the first action you should take is to sign up for Azure AD Privileged Identity Management (PIM) for Azure AD roles1. This step is crucial as it enables PIM for your tenant, allowing you to manage, control, and monitor access to privileged roles.

Once PIM is enabled, you can proceed with discovering privileged roles and resources, configuring role settings, and assigning eligible users2.

upvoted 1 times

stonwall12 4 months, 2 weeks ago

Selected Answer: A

Answer: Question is outdated

Reason: Per current Microsoft documentation, with Microsoft Entra ID P2 or Microsoft Entra ID Governance license, PIM is automatically enabled for the tenant and doesn't require sign-up or consent.

Reference: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-getting-started#prerequisites

upvoted 1 times

Hot_156 4 months, 3 weeks ago

Selected Answer: A

To enable Azure AD Privileged Identity Management (PIM) for Azure AD roles, you can follow these steps:

Step 1: Sign Up for PIM
Go to the Azure portal.

In the left-hand navigation pane, select Azure Active Directory.

Under Manage, select Privileged Identity Management.

If this is your first time accessing PIM, click Sign up to enable it for your Azure AD directory.

upvoted 2 times

ndtmartin 5 months ago

Selected Answer: A

Before you can manage and secure Azure AD roles using PIM, you need to sign up for PIM. This is the first step in enabling PIM for Azure AD roles, after which you can configure role management, policies, and other settings.

upvoted 1 times

AlaNaj003 5 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/training/modules/manage-authorization-microsoft-entra-id/15-configure-privileged-identity-management

upvoted 1 times

jamju 5 months, 2 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-getting-started#prepare-pim-for-azure-roles

upvoted 2 times

aocferreira 7 months, 3 weeks ago

Selected Answer: C

As per the below site, the correct answer is C. Before implementing PIM for Entra or RBAC roles, the first step is to "discover and mitigate privileged roles":

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan

upvoted 3 times

codeunit 8 months, 3 weeks ago

To secure Azure AD roles using Azure Active Directory Privileged Identity Management (PIM), the first action you should take is to enable Privileged Identity Management (PIM) for Azure AD. This step is essential as it sets up PIM for your Azure AD environment, allowing you to manage and secure privileged roles.

After enabling PIM, you can proceed with other tasks like assigning eligible roles, configuring role settings, and setting up just-in-time (JIT) access. However, enabling PIM is the foundational step.

upvoted 1 times

purek77 9 months, 1 week ago

Selected Answer: C

Yes, question is outdated (consent is no longer required), however looking at below link - it seems that you have to "Discover and mitigate privileged roles" - therefore C is potentially correct answer nowadays.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

upvoted 4 times

Andre369 9 months, 1 week ago

Selected Answer: C

Before you can effectively manage and secure privileged roles in Azure AD using PIM, you need to discover the existing privileged roles in your Azure subscription. This involves identifying the roles that have elevated permissions and need to be managed through PIM.

By discovering privileged roles, you gain visibility into the current role assignments and can determine which roles should be subject to PIM and undergo the access review and just-in-time (JIT) activation process.

upvoted 3 times

Question #10 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
You have been tasked with creating a different subscription for each of your company's divisions. However, the subscriptions will be linked to a single Azure Active
Directory (Azure AD) tenant.
You want to make sure that each subscription has identical role assignments.
You make use of Azure AD Privileged Identity Management (PIM).
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required

B. Azure Blueprints

C. Conditional access policies

D. Azure DevOps

Suggested Answer: *A*
The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

Community vote distribution
B (100%)

⊟ **Rume** Highly Voted 👍 4 years ago
B. Azure Blueprints
upvoted 53 times

⊟ **kakakayayaya** 3 years, 10 months ago
100% B
Blueprint Role Assignment (Subscription, Resource Group) - Add an existing user or group to a built-in role to make sure the right people always have the right access to your resources. Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.
upvoted 15 times

⊟ **ChinkSantana** 3 years, 12 months ago
Yes Azure Blueprints
upvoted 11 times

⊟ **adamsca** Highly Voted 👍 3 years, 6 months ago
Selected Answer: B
azure Blueprints
upvoted 8 times

⊟ **stonwall12** Most Recent ⏲ 4 months, 2 weeks ago
Selected Answer: B
Answer: B, Azure Blueprints

Reason: When you need to replicate identical role assignments across multiple subscriptions, Azure Blueprints is the correct tool, not PIM. PIM manages just-in-time access and role activation, while Azure Blueprints allows you to define and deploy consistent role assignments across multiple subscriptions.

Reference: https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

Note: Azure Blueprints will soon be called "Templates for Azure resource" but the functionality remains the same. (July 11, 2026)
upvoted 3 times

⊟ **Vaibhav39** 5 months, 3 weeks ago
Selected Answer: B

Blue print
upvoted 1 times

Janmigs 9 months, 1 week ago

Selected Answer: B

Blueprint Role Assignment (Subscription, Resource Group) - Add an existing user or group to a built-in role to make sure the right people always have the right access to your resources. Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.
upvoted 3 times

Andre369 9 months, 1 week ago

Selected Answer: B

To ensure that each subscription has identical role assignments, you should make use of Azure Blueprints. Azure Blueprints provide a declarative way to orchestrate the deployment of various Azure resources, including role assignments, policies, and resource configurations.

By creating an Azure Blueprint that defines the desired role assignments, you can apply the same blueprint to each subscription, ensuring consistent role assignments across all divisions.
upvoted 1 times

zellck 9 months, 1 week ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups
upvoted 1 times

God2029 9 months, 1 week ago

Reading the question again. Your Task is to create different subscriptions for each of your company's divisions. Can blue print be used to create new subscriptions? I have been going through Microsoft docs but nowhere found that a new subscription can be created with blueprint. Once you create subscription with PIM you can use blue print to assign various resources groups, into the subscription and add resources to resource group.

As you already have the PIM previlage go ahead create subscriptions and once it is created use blueprint to check if the resources/roles are identical. But First go ahead and create subscriptions.

No adjustment required is the perfect answer in this context.
upvoted 4 times

fonte 2 years, 6 months ago

The way I read it is that the blueprints are going to be used to create the role assignments in each subscriptions, not to create the subscriptions.
upvoted 2 times

Mazhar1993 9 months, 1 week ago

 No adjustment required: Inaccurate because it overlooks the need for a solution to ensure consistent role assignments across subscriptions.
 Azure Blueprints: Suitable as it enables the automated deployment of Azure resources with predefined configurations and role assignments, ensuring consistency across subscriptions.
 Conditional access policies: Not suitable as they focus on access controls based on conditions like user location or device compliance, rather than ensuring identical role assignments.
 Azure DevOps: Not suitable as it primarily facilitates software development processes and infrastructure management, lacking direct relevance to ensuring consistent role assignments across subscriptions.

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-add-role-to-user
upvoted 3 times

xRiot007 11 months, 2 weeks ago

To make sure that all current and future subs are compliant, use Azure Blueprints (B). In the future, I think mid 2026, Blueprints will be deprecated, so you should start migrating to Template Specs and Deployment Stacks.
upvoted 1 times

ctlearn 1 year, 6 months ago

Selected Answer: B

Azure Blueprints for ensuring identical role assignments across multiple subscriptions. PIM only manages, controls, and monitors access within a subscription.

upvoted 2 times

ESAJRR 1 year, 10 months ago

Selected Answer: B

B. Azure Blueprints

upvoted 1 times

vicwelly 1 year, 11 months ago

Answer is Azure Blueprints. ET sometimes give wrong answers on purpose to make sure we are not doing Parrot Learning.

upvoted 1 times

Andre369 2 years, 2 months ago

Selected Answer: B

The answer is Azure Blueprints

upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. Azure Blueprints

upvoted 2 times

Brandonzzm 2 years, 4 months ago

Correct one is C. Azure Blueprints, Azure Blueprints can be used to create and manage resources across multiple subscriptions, ensuring that each subscription has the same set of resources, policies, and roles. By creating a blueprint that includes the required roles and permissions, you can ensure that each subscription has identical role assignments.

upvoted 1 times

Seelearndo 2 years, 5 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

upvoted 1 times

Question #11 *Topic 1*

Your company has an Azure Container Registry.
You have been tasked with assigning a user a role that allows for the uploading of images to the Azure Container Registry. The role assigned should not require more privileges than necessary.
Which of the following is the role you should assign?

A. Owner

B. Contributor

C. AcrPush

D. AcrPull

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

Community vote distribution

C (100%)

⊟ **Rume** Highly Voted 3 years, 12 months ago
given answer is correct
upvoted 22 times

⊟ **ech** Highly Voted 3 years, 8 months ago
AcrPush role can push and pull image. https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli answer is AcrPush
upvoted 10 times

⊟ **D3D1997** 2 years, 5 months ago
one more well named role by Microsoft
upvoted 6 times

⊟ **stonwall12** Most Recent 4 months, 2 weeks ago
Selected Answer: C
Answer: C, AcrPush

Reason: AcrPush role provides minimum required permissions to push/upload images to Azure Container Registry while following the principle of least privilege. Owner and Contributor roles would grant excessive permissions, while AcrPull only allows downloading images.

Reference: https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles
upvoted 3 times

⊟ **Ruffyit** 8 months, 2 weeks ago
The role you should assign is AcrPush. This role specifically grants the ability to push (upload) images to the Azure Container Registry, which is the required permission for the user. Assigning the Owner role would provide excessive privileges, as it includes full control over the registry and all its resources, which is not necessary for simply uploading images. The Contributor role also grants more privileges than needed, as it includes permissions for creating, deleting, and modifying resources beyond just uploading images. The AcrPull role, on the other hand, grants permission to pull (download) images from the registry, which is not relevant to the task described. Therefore, AcrPush is the most appropriate role that meets the requirement of allowing image uploading without granting unnecessary privileges.
https://learn.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli
upvoted 1 times

⊟ **Mazhar1993** 9 months, 1 week ago
The role you should assign is AcrPush. This role specifically grants the ability to push (upload) images to the Azure Container Registry, which is the required permission for the user. Assigning the Owner role would provide excessive privileges, as it includes full control over the registry and all its resources, which is not necessary for simply uploading images. The Contributor role also grants more privileges than needed, as it includes permissions for creating, deleting, and modifying resources beyond just uploading images. The AcrPull role, on the other hand, grants permission to pull (download) images from the registry, which is not relevant to the task described. Therefore, AcrPush is the most appropriate role that meets the

requirement of allowing image uploading without granting unnecessary privileges.

https://learn.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli

upvoted 3 times

ESAJRR 1 year, 12 months ago

Selected Answer: C

C. AcrPush

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles

upvoted 1 times

MOldFox 2 years, 3 months ago

Selected Answer: C

C is correct

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: C

C. AcrPush

upvoted 2 times

AZ5cert 2 years, 6 months ago

C. AcrPush

upvoted 2 times

God2029 2 years, 7 months ago

Voting for AcrPush

upvoted 1 times

Lutu 2 years, 9 months ago

C is correct

upvoted 2 times

Eltooth 3 years, 3 months ago

Selected Answer: C

C is correct.

https://docs.microsoft.com/en-gb/learn/modules/enable-containers-security/6-enable-azure-container-registry-authentication

upvoted 4 times

DoctorCOmputer 3 years, 5 months ago

Pull is downloading and push is uploading !

Definitely answers are correct!

upvoted 3 times

> **Holii** 2 years, 1 month ago
>
> Note: ArcPush can also Pull/Download.
>
> Uploading/Writing is normally a higher-security privilege, so a role that can upload can also (obviously) Download/Read as well.
>
> upvoted 2 times

DarkCyberGhost 3 years, 5 months ago

I agree that the GIven answer here is the Correct Answer.

upvoted 1 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 1 times

PBA1211 3 years, 7 months ago

A, B and C are all 3 right,

D definitely NOT!

upvoted 1 times

PBA1211 3 years, 7 months ago

My Mistake, they are all 3 correct, only the question states "not more rights then neccesary" that way the answer is correct.

upvoted 2 times

Question #12 *Topic 1*

Your company has an Azure Container Registry.
You have been tasked with assigning a user a role that allows for the downloading of images from the Azure Container Registry. The role assigned should not require more privileges than necessary.
Which of the following is the role you should assign?

A. Reader

B. Contributor

C. AcrDelete

D. AcrPull

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

Community vote distribution

D (100%)

Lyonel Highly Voted 9 months, 1 week ago
Question gives the condition, "The role assigned should not require more privileges than necessary."

Therefore, D (Acrpull) is CORRECT because it provides the least number of permissions required for downloading images from a Container Registry.

Answer A (Reader): provides at least two (2) permissions, which would be one (1) more than Acrpull allows for.

[Ref. https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli]
upvoted 81 times

ashxos 3 years, 7 months ago
Perfect!
upvoted 3 times

[Removed] 3 years, 7 months ago
correct
upvoted 1 times

ech 3 years, 8 months ago
agree read can Access Resource Manager and Pull, but AcrPull role is just for pulling the image.
upvoted 4 times

heatfan900 1 year, 9 months ago
CORRECT. NOT SURE Y EVERYONE THINKS YOU NEED THE READER ROLE FOR THIS SCENARIO.

FROM MICROSOFT:
Azure Resource Manager access is required for the Azure portal and registry management with the Azure CLI. For example, to get a list of registries by using the az acr list command, you need this permission set.
upvoted 1 times

Ucy Highly Voted 3 years, 12 months ago
Answer is Wrong....
Correct answer is D AcrPull
upvoted 15 times

Sinemorec2024 Most Recent 2 months, 2 weeks ago
Selected Answer: D
Reference: https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles
upvoted 1 times

stonwall12 4 months, 2 weeks ago

Selected Answer: D

Answer: D, AcrPull

Reason: AcrPull role provides minimum required permissions to pull/download images from Azure Container Registry while following the principle of least privilege. Reader, Contributor, and AcrDelete either provide insufficient or excessive permissions.

Reference: https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles

upvoted 1 times

Ruffyit 8 months, 2 weeks ago

Question gives the condition, "The role assigned should not require more privileges than necessary."

Therefore, D (Acrpull) is CORRECT because it provides the least number of permissions required for downloading images from a Container Registry.

Answer A (Reader): provides at least two (2) permissions, which would be one (1) more than Acrpull allows for.

[Ref. https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli]

upvoted 1 times

Janmigs 9 months, 1 week ago

Selected Answer: D

Therefore, D (Acrpull) is CORRECT because it provides the least number of permissions required for downloading images from a Container Registry.

Answer A (Reader): provides at least two (2) permissions, which would be one (1) more than Acrpull allows for.

[Ref. https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli]

upvoted 1 times

smilinghacker 9 months, 1 week ago

Question gives the condition, "The role assigned should not require more privileges than necessary."

Therefore, D (Acrpull) is CORRECT because it provides the least number of permissions required for downloading images from a Container Registry.

Answer A (Reader): provides at least two (2) permissions, which would be one (1) more than Acrpull allows for.

[Ref. https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli]

upvoted 2 times

amondal354 9 months, 1 week ago

Selected Answer: D

Question gives the condition, "The role assigned should not require more privileges than necessary."

Therefore, D (Acrpull) is CORRECT because it provides the least number of permissions required for downloading images from a Container Registry.

Answer A (Reader): provides at least two (2) permissions, which would be one (1) more than Acrpull allows for.

upvoted 1 times

Fal991l 9 months, 1 week ago

Selected Answer: D

The role that should be assigned to allow for the downloading of images from the Azure Container Registry without granting unnecessary privileges is "AcrPull".

The AcrPull role provides read-only permissions to pull images from the registry. This role is the minimum required permission to pull an image. It does not allow pushing or modifying images or managing the registry itself.

The other options are not the best fit for this scenario:

The Reader role provides read-only access to all resources within a resource group, which includes the container registry. However, this role is too broad and provides more access than needed for just pulling images.
The Contributor role provides the ability to manage all aspects of a resource, including creating, modifying, and deleting. This role is more permissions than are necessary for just pulling images.

The AcrDelete role provides the ability to delete repositories and images from the registry. This role is more permissions than are necessary for just pulling images.

upvoted 2 times

xRiot007 11 months, 2 weeks ago

Wrong answer. Correct answer is D - AcrPull. Viewing the available images in the registry is not enough, you actually have to be able to download (pull) them.

upvoted 1 times

Mazhar1993 1 year, 2 months ago

The role you should assign is AcrPull because it specifically grants the ability to pull (download) images from the Azure Container Registry, which is the required permission for the user. Assigning the Reader role would provide broader access than necessary, as it includes permissions beyond image pulling. Similarly, assigning the Contributor role would grant excessive privileges, as it includes permissions for creating, deleting, and modifying resources, which are not required for simply downloading images. The AcrDelete role is also not suitable, as it specifically grants permission to delete image data from the registry, which is not needed for the task described. Therefore, AcrPull is the most appropriate role that meets the requirement of allowing image downloading without granting unnecessary privileges.
https://learn.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli

upvoted 1 times

TheFamousSpy 1 year, 3 months ago

Selected Answer: D

Clearly stated in the reference

upvoted 1 times

kb1342 1 year, 4 months ago

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli

D. Arc Pull

Since Reader has more access than necessary

upvoted 2 times

codeunit 1 year, 7 months ago

Following and article from Microsoft, ArcPull role will provide the least privilege access: https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli

upvoted 2 times

wardy1983 1 year, 8 months ago

Answer is ARCPULL

Arcpull can only pull and image

Reader can access access Resource Manager and PULL

Least access is ArcPull

case closed!!!

upvoted 1 times

16116 1 year, 10 months ago

Selected Answer: D

Most certainly agreed with the above statements.

Unless proven otherwise, the answer D is correct as pert MS documentation.

upvoted 1 times

ESAJRR 1 year, 12 months ago

Selected Answer: D

D. ArcPull

upvoted 1 times

Question #13 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your Company's Azure subscription includes a virtual network that has a single subnet configured.
You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.
You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure
SQL databases via the service endpoint.
You need to perform a task on the virtual machine prior to deploying containers.
Solution: You create an application security group.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

billibarou Highly Voted 3 years, 6 months ago

Selected Answer: B

So the question states "You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint". Since the containers are deployed inside a virtual machine the service endpoint will allow the virtual machine and anything hosted inside(applications/containers) to access Azure services directly. So since the creation of the service endpoint allows access to Azure Storage and Azure SQL databases there is no need to create an Application Security Group(ASG). B is the correct answer.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 60 times

God2029 2 years, 7 months ago

Well explained!

upvoted 2 times

God2029 2 years, 7 months ago

adding to the above. By default Azure has been configured with default route and so resource within the same virtual network can communicate each other irrespective of subnet. But in prod we define custom subnet for security which will override azure default route, you need to enable routing using network virtual appliance (NVA) in such scenario. Also ASG and ACL would be required to define more stringent policy. We need to apply zero Trust principles and least privileges. Based on budget, can even go for microsegementaion for host/device based access control.

upvoted 4 times

DarkCyberGhost 3 years, 5 months ago

This is Correct i need say no more. Thanks billibarou

upvoted 3 times

mT3 Highly Voted 3 years, 10 months ago

answer is correct

upvoted 9 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: B

Answer: B, No

Reason: Creating an application security group won't enable containers to use service endpoints.

Reference: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#limitations

upvoted 1 times

Ruffyit 8 months, 2 weeks ago

So the question states "You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint". Since the containers are deployed inside a virtual machine the service endpoint will allow the virtual machine and anything hosted inside(applications/containers) to access Azure services directly. So since the creation of the service endpoint allows access to Azure Storage and Azure SQL databases there is no need to create an Application Security Group(ASG). B is the correct answer.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 1 times

wardy1983 9 months, 1 week ago

Answer: B

Explanation:

You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint". Since the containers are deployed inside a virtual machine the service endpoint will allow the virtual machine and anything hosted inside(applications/containers) to access Azure services directly. So since the creation of the service endpoint allows access to Azure Storage and Azure SQL databases there is no need to create an Application Security Group(ASG). B is the correct answe

upvoted 1 times

Mazhar1993 1 year, 2 months ago

NO

Creating an application security group on the virtual machine does not directly enable the containers to access Azure Storage resources and Azure SQL databases via the service endpoint. Application security groups are used to define network security policies based on application workloads. To ensure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint, you need to configure the necessary network settings or firewall rules on the virtual machine itself.

upvoted 1 times

ErikPJordan 1 year, 9 months ago

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

upvoted 1 times

ESAJRR 1 year, 10 months ago

Selected Answer: B

B is the answer.

upvoted 1 times

DatBroNZ 2 years ago

Creating an application security group is not directly related to enabling container access to Azure Storage and Azure SQL databases. Application security groups are used for network security purposes, such as defining network security group (NSG) rules.

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#configuration

upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. Answer is NO

upvoted 2 times

Bill831231 2 years, 8 months ago

Seems the answer is correct, but the explaination is not that correct, an ASG cannot bring more connectivity for a container inside a VM, but a CNI could

upvoted 7 times

chamka 2 years, 9 months ago

Selected Answer: B

Given answer is correct

upvoted 1 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

⊟ **yoton** 3 years, 4 months ago

Selected Answer: B

The creation of the service endpoint negates the need for an ASG.

upvoted 2 times

⊟ **satishba** 3 years, 6 months ago

Service End Point are configured in VNET settings and allow Subnet Traffic to the settings in a view it is more routing specific and not related to Blocking , ASG and NSG are more from blocking perspective so do not apply here

upvoted 6 times

⊟ **AbsG** 3 years, 6 months ago

can someone explain why No.

upvoted 2 times

> ⊟ **PhilMultiCloud** 3 years, 6 months ago
>
> You can simply look at what is the function of a ASG and you will understand why..
>
> upvoted 1 times

Question #14 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your Company's Azure subscription includes a virtual network that has a single subnet configured.
You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.
You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure
SQL databases via the service endpoint.
You need to perform a task on the virtual machine prior to deploying containers.
Solution: You create an AKS Ingress controller.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

dumdada Highly Voted 3 years, 10 months ago

Ingress Controller is used to establish a reverse proxy, so obviously answer is No

upvoted 13 times

PhilMultiCloud 3 years, 7 months ago

wth is that supposed to mean? reverse proxy is actually required here.

upvoted 1 times

cfsxtuv33 3 years, 6 months ago

Thats kinda what I was thinking.

upvoted 1 times

Patchfox 3 years, 5 months ago

Your are correct when you need AKS. But in this case you install only Docker Containers on Virtual Machines.

upvoted 6 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: B

Answer: B, No

Reason: Creating an AKS Ingress controller is not relevant for standalone Docker containers on a VM. Ingress controllers are used in Kubernetes (AKS) environments for managing inbound traffic, not for enabling container access to service endpoints.

Reference: https://learn.microsoft.com/en-us/azure/virtual-network/container-networking-overview

upvoted 3 times

Ruffyit 8 months, 2 weeks ago

No, the solution does not meet the goal.

Creating an AKS (Azure Kubernetes Service) Ingress controller is not necessary for enabling the Docker containers deployed on the virtual machine to access Azure Storage resources and Azure SQL databases via the service endpoint. The AKS Ingress controller is specifically designed to manage traffic routing for applications running on AKS clusters, not for individual virtual machines.

To enable access to Azure Storage resources and Azure SQL databases via the service endpoint from the virtual machine, you should ensure that the necessary configurations are made within the virtual machine itself. This might involve configuring network settings or installing appropriate drivers or libraries to facilitate communication with Azure services.

Therefore, the proposed solution of creating an AKS Ingress controller does not align with the goal of enabling access to Azure Storage resources and Azure SQL databases from the virtual machine.

upvoted 2 times

pentium75 11 months ago

Selected Answer: B

No AKS here

upvoted 2 times

Mazhar1993 1 year, 2 months ago

No, the solution does not meet the goal.

Creating an AKS (Azure Kubernetes Service) Ingress controller is not necessary for enabling the Docker containers deployed on the virtual machine to access Azure Storage resources and Azure SQL databases via the service endpoint. The AKS Ingress controller is specifically designed to manage traffic routing for applications running on AKS clusters, not for individual virtual machines.

To enable access to Azure Storage resources and Azure SQL databases via the service endpoint from the virtual machine, you should ensure that the necessary configurations are made within the virtual machine itself. This might involve configuring network settings or installing appropriate drivers or libraries to facilitate communication with Azure services.

Therefore, the proposed solution of creating an AKS Ingress controller does not align with the goal of enabling access to Azure Storage resources and Azure SQL databases from the virtual machine.

upvoted 4 times

ITFranz 1 year, 7 months ago

https://www.nginx.com/resources/glossary/kubernetes-ingress-controller/

Answer = no

upvoted 1 times

trashbox 1 year, 8 months ago

Selected Answer: B

We need to be aware of the direction of accessing Storage Account and SQL Database "from" Container (Pod). Once you are aware of this, it is clear that Ingress does not apply.

upvoted 2 times

ITFranz 1 year, 9 months ago

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. Kubernetes ingress resources are used to configure the ingress rules and routes for individual Kubernetes

upvoted 1 times

TheProfessor 1 year, 9 months ago

Selected Answer: B

answer is B

upvoted 1 times

ESAJRR 1 year, 10 months ago

Selected Answer: B

B is the answer.

upvoted 1 times

DatBroNZ 2 years ago

Creating an AKS Ingress controller is specific to Azure Kubernetes Service (AKS) and is used for managing external access to services running on AKS. It is not directly related to enabling container access to Azure Storage and Azure SQL databases on a virtual machine.

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: B

Answer is B.

There is no AKS deployed, so no need for AKS ingress controller.

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. Answer is NO

upvoted 4 times

⊟ **rohitmedi** 3 years, 7 months ago

correct answer

upvoted 3 times

Question #15

Topic 1

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your Company's Azure subscription includes a virtual network that has a single subnet configured.
You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.
You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure
SQL databases via the service endpoint.
You need to perform a task on the virtual machine prior to deploying containers.
Solution: You install the container network interface (CNI) plug-in.
Does the solution meet the goal?

A. Yes

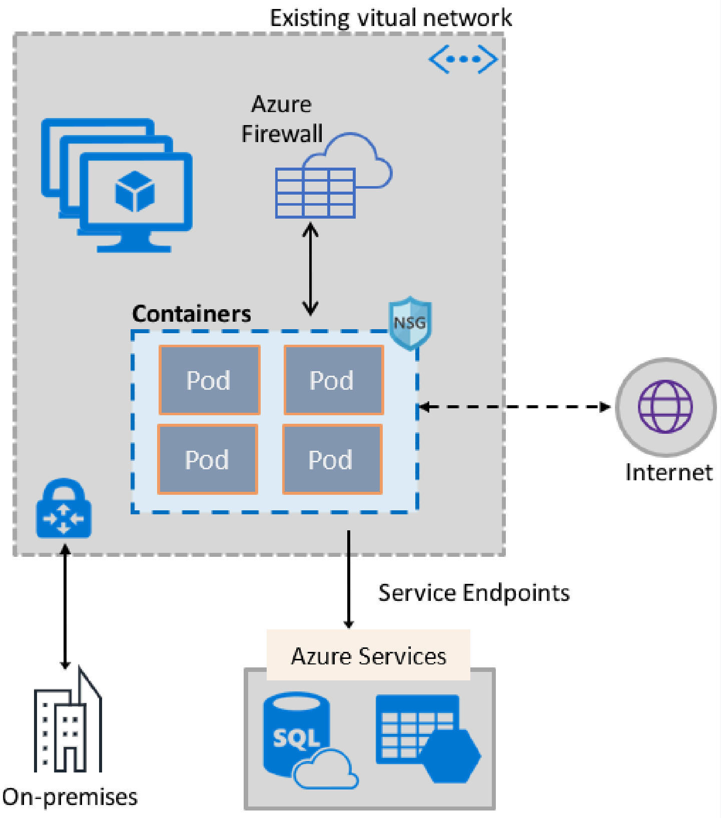
B. No

Suggested Answer: *A*

The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform.

The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.

The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

Community vote distribution

A (100%)

mT3 Highly Voted 3 years, 10 months ago

answer is correct

upvoted 16 times

Duyons Highly Voted 2 months ago

Selected Answer: B

Hey folks, just wanted to clarify this one.
A lot of people are picking A. Yes because of the CNI docs, but this question is about a regular Ubuntu VM running Docker, not AKS or Kubernetes.

In this setup, Docker containers can already access Azure Storage and SQL via Service Endpoints as long as the VM is in the right subnet — which the question says it is.

You don't need to install the CNI plugin for that.
So the correct answer here is B. No.

Hope that helps!
upvoted 8 times

Knighthell Most Recent 3 weeks, 1 day ago
Selected Answer: B
https://learn.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services
upvoted 1 times

stonwall12 4 months, 2 weeks ago
Selected Answer: A
Answer: A, Yes

Reason: Installing the Container Network Interface (CNI) plugin is the correct solution as it enables containers to use the host's networking capabilities, including service endpoints configured on the VM's subnet.

Reference: https://learn.microsoft.com/en-us/azure/virtual-network/container-networking-overview
upvoted 1 times

Ruffyit 8 months, 2 weeks ago
A is the answer.

Bring the rich set of Azure network capabilities to containers, by utilizing the same software defined networking stack that powers virtual machines. The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
upvoted 3 times

zellck 9 months, 1 week ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/virtual-network/container-networking-overview
Bring the rich set of Azure network capabilities to containers, by utilizing the same software defined networking stack that powers virtual machines. The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
upvoted 7 times

wardy1983 9 months, 1 week ago
Answer: A
Explanation:
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform.
The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
upvoted 2 times

Mazhar1993 1 year, 2 months ago
Yes, the solution meets the goal. By installing the container network interface (CNI) plug-in on the virtual machine, you enable the Docker containers to be attached to the Azure virtual network and utilize the same network connectivity as the virtual machine. This allows the containers to access

Azure Storage resources and Azure SQL databases via the service endpoint configured for the subnet. Therefore, the solution aligns with the requirement of ensuring that the containers can access the specified Azure resources via the service endpoint.

https://learn.microsoft.com/en-us/azure/virtual-network/container-networking-overview

upvoted 1 times

ESAJRR 1 year, 10 months ago

Selected Answer: A

A is the answer.

upvoted 1 times

DatBroNZ 2 years ago

The container network interface (CNI) plug-in is responsible for providing network connectivity to containers running on a host. Answer is correct.

upvoted 2 times

JunetGoyal 2 years, 1 month ago

There are two ways to assign IPs to containers

Kubectl: It will create a new Vnet for cluster.

Azure CNI: It can either llow ypu to use existing vnet or create new vnet.

As per Q. Answer is YES, Coz CNI can allow you to give ip from exiting vnet(Subnet),As we already have Service endpoints configure, the Container can directly talk to SQL, storage.

upvoted 3 times

sylar83 2 years, 2 months ago

Answer from GPT is no:

No, installing the CNI plug-in on the virtual machine will not achieve the goal.

The goal is to ensure that Docker containers deployed to the VM can access Azure Storage and SQL DB via the service endpoint configured on the subnet.

Installing the CNI plug-in will create network interfaces for Docker containers and attach them to networks. However, it does not configure routing rules to direct traffic to the service endpoint.

To meet the goal, you need to perform the following:

1. Install the Azure CLI on the Ubuntu VM
2. Install Docker on the VM
3. Restart the Docker service to pick up the environment variables
4. Add routing rules to direct traffic from containers to the subnet's service endpoint
5. Deploy containers and test access to Storage/SQL DB.

So in summary, installing the CNI plug-in alone will not configure the network routing needed for the containers to utilize the service endpoint. Additional configuration using the Azure CLI is required.

Therefore, the solution does not meet the goal. The correct option is B - No.

upvoted 3 times

Holii 2 years, 1 month ago

Note: Using ChatGPT for cloud work provides me with the wrong answer 9 times out of 10. Since GPT doesn't have Azure access, and the Microsoft stack is very intricate, please be wary when accepting these as answers without your own research.

upvoted 5 times

vicwelly 1 year, 11 months ago

When it comes to Azure! Chat GPT is garbage

upvoted 3 times

majstor86 2 years, 4 months ago

Selected Answer: A

A. Answer is YES

upvoted 3 times

Te2ya 2 years, 8 months ago

This is just a question about Linux / Docer rather than AKS. No need for CNI. 'No' is the answer.

upvoted 3 times

mung 2 years, 7 months ago

Any reference?

upvoted 1 times

OrangeSG 2 years, 5 months ago

Enable containers to use Azure Virtual Network capabilities
https://learn.microsoft.com/en-us/azure/virtual-network/container-networking-overview

Using the plug-in
The plug-in can be used in the following ways, to provide basic virtual network attach for Pods or Docker containers:
• Virtual network attach for Docker containers in Azure: The plug-in can be used in cases where you don't want to create a Kubernetes cluster, and would like to create Docker containers with virtual network attach, in virtual machines
upvoted 1 times

⊟ **TheLegendPasha** 3 years, 2 months ago
Selected Answer: A
Answer is Yes because this is what container docker interface is used for
upvoted 2 times

⊟ **TJ001** 3 years, 5 months ago
perfect - correct answer
upvoted 1 times

⊟ **ateeb** 3 years, 7 months ago
given answer is correct
upvoted 3 times

Question #16 *Topic 1*

You make use of Azure Resource Manager templates to deploy Azure virtual machines.
You have been tasked with making sure that Windows features that are not in use, are automatically inactivated when instances of the virtual machines are provisioned.
Which of the following actions should you take?

A. You should make use of Azure DevOps.

B. You should make use of Azure Automation State Configuration.

C. You should make use of network security groups (NSG).

D. You should make use of Azure Blueprints.

Suggested Answer: *B*
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.
Reference:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

Community vote distribution
B (100%)

adsdadasdad Highly Voted 3 years, 12 months ago
answer is correct
upvoted 16 times

Rume Highly Voted 4 years ago
B is correct.
upvoted 9 times

Ruffyit Most Recent 2 months, 2 weeks ago
Selected Answer: B
Reference: https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview
upvoted 1 times

stonwall12 4 months, 2 weeks ago
Selected Answer: B
Answer: B, Azure Automation State Configuration

Reason: Azure Automation State Configuration allows you to define and maintain desired state configurations for VMs, including which Windows features should be enabled or disabled automatically during and after provisioning.

Reference: https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview
upvoted 2 times

kosmaty 5 months, 2 weeks ago
Selected Answer: B
Vote for B but still remember it will be retired:
Azure Automation State Configuration will be retired on September 30, 2027, please transition to Azure Machine Configuration by that date. For more information, see the blog post announcement. The Azure Machine Configuration service combines features of DSC Extension, Azure Automation State Configuration, and the most commonly requested features from customer feedback. Azure Machine Configuration also includes hybrid machine support through Arc-enabled servers.
upvoted 6 times

Ruffyit 8 months, 2 weeks ago

You should make use of Azure Automation State Configuration.

Azure Automation State Configuration allows for defining and enforcing the desired state of virtual machines, ensuring that Windows features are configured correctly upon provisioning.
Azure DevOps is a continuous integration/continuous deployment (CI/CD) platform, which focuses on automating software delivery processes rather than managing VM configurations.
Network security groups (NSGs) are used to control network traffic to/from Azure resources and wouldn't directly address the task of managing Windows features on VMs.
Azure Blueprints provide a way to package templates, policies, role assignments, and resource groups into a single blueprint, but they do not specifically address VM configuration management like Azure Automation State Configuration does.

https://learn.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

upvoted 4 times

Mazhar1993 9 months, 1 week ago

You should make use of Azure Automation State Configuration.

Azure Automation State Configuration allows for defining and enforcing the desired state of virtual machines, ensuring that Windows features are configured correctly upon provisioning.
Azure DevOps is a continuous integration/continuous deployment (CI/CD) platform, which focuses on automating software delivery processes rather than managing VM configurations.
Network security groups (NSGs) are used to control network traffic to/from Azure resources and wouldn't directly address the task of managing Windows features on VMs.
Azure Blueprints provide a way to package templates, policies, role assignments, and resource groups into a single blueprint, but they do not specifically address VM configuration management like Azure Automation State Configuration does.

https://learn.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

upvoted 4 times

ESAJRR 1 year, 10 months ago

Selected Answer: B

B. You should make use of Azure Automation State Configuration.

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. You should make use of Azure Automation State Configuration.

upvoted 1 times

Eltooth 3 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 3 times

Chun 3 years, 3 months ago

Selected Answer: B

B. is correct

upvoted 1 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 3 times

Question #17 *Topic 1*

Your company's Azure subscription includes Windows Server 2016 Azure virtual machines.
You are informed that every virtual machine must have a custom antimalware virtual machine extension installed. You are writing the necessary code for a policy that will help you achieve this.
Which of the following is an effect that must be included in your code?

A. Disabled

B. Modify

C. AuditIfNotExists

D. DeployIfNotExists

Suggested Answer: *D*
DeployIfNotExists executes a template deployment when the condition is met.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

Community vote distribution
D (100%)

Rume Highly Voted 4 years ago
D is correct.
upvoted 18 times

Ruffyit Most Recent 2 months, 2 weeks ago
Selected Answer: D
Reference: https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists
upvoted 1 times

stonwall12 4 months, 2 weeks ago
Selected Answer: D
Answer: D, DeployIfNotExists

Reason: DeployIfNotExists effect is required to automatically deploy the antimalware extension to VMs that don't have it installed. AuditIfNotExists would only report non-compliance, while Disabled and Modify don't provide the required functionality.

Reference: https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists
upvoted 1 times

Mazhar1993 9 months, 1 week ago
You should include the effect "DeployIfNotExists" in your code.

The "DeployIfNotExists" effect ensures that the specified custom antimalware virtual machine extension is deployed if it doesn't already exist on the Azure virtual machine.
"Disabled" is not suitable as it doesn't address the requirement of ensuring the presence of the antimalware extension.
"Modify" is not directly related to deploying extensions and wouldn't ensure the presence of the antimalware extension.
"AuditIfNotExists" is more focused on auditing the existence of resources rather than deploying them, which is not aligned with the task of installing the antimalware extension.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-basics
upvoted 4 times

TheProfessor 1 year, 9 months ago
Selected Answer: D
The answer is: D
upvoted 3 times

ESAJRR 1 year, 11 months ago
Selected Answer: D

D. DeployIfNotExists

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists
Similar to AuditIfNotExists, a DeployIfNotExists policy definition executes a template deployment when the condition is met. Policy assignments with effect set as DeployIfNotExists require a managed identity to do remediation.

upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: D

D. DeployIfNotExists

upvoted 1 times

dRealTony 2 years, 9 months ago

D is the correct answer

upvoted 2 times

ahmadmohdrudin 2 years, 9 months ago

Selected Answer: D

D is correct
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

upvoted 2 times

Eltooth 3 years, 3 months ago

Selected Answer: D

D is correct answer

upvoted 4 times

AS179 3 years, 6 months ago

Selected Answer: D

correct

upvoted 2 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 3 times

Question #18 *Topic 1*

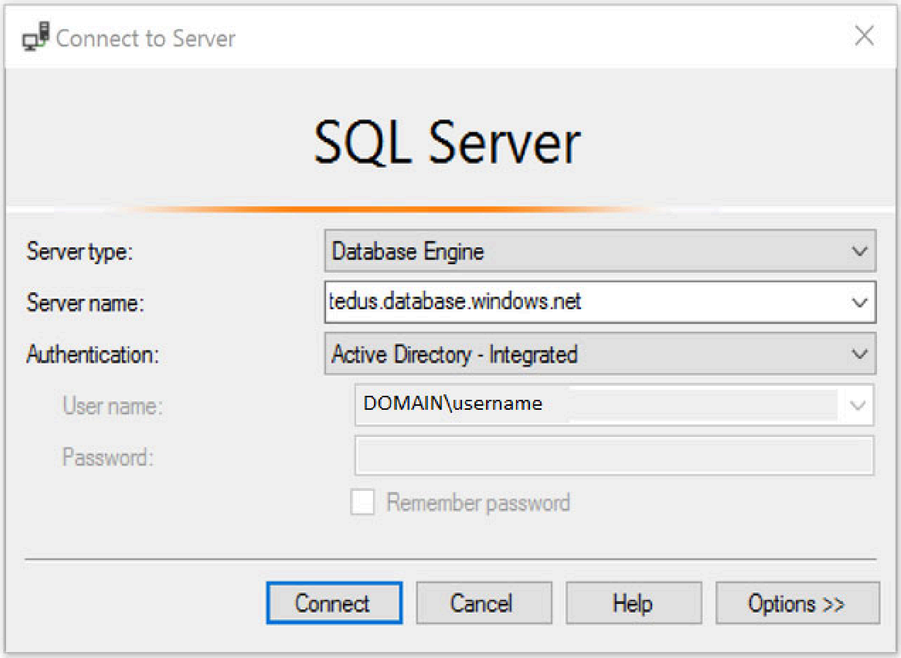
Your company makes use of Azure Active Directory (Azure AD) in a hybrid configuration. All users are making use of hybrid Azure AD joined Windows 10 computers.
You manage an Azure SQL database that allows for Azure AD authentication.
You need to make sure that database developers are able to connect to the SQL database via Microsoft SQL Server Management Studio (SSMS).
You also need to make sure the developers use their on-premises Active Directory account for authentication. Your strategy should allow for authentication prompts to be kept to a minimum.
Which of the following is the authentication method the developers should use?

A. Azure AD token.

B. Azure Multi-Factor authentication.

C. Active Directory integrated authentication.

Suggested Answer: *C*
Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure
AD.
Using an Azure AD identity to connect using SSMS or SSDT
The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database
Tools.
Active Directory integrated authentication
Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.
1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active
Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



Connect to Server

SQL Server

Server type: Database Engine
Server name: tedus.database.windows.net
Authentication: Active Directory - Integrated
User name: DOMAIN\username
Password:
□ Remember password

2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to.
(The AD domain name or tenant IDו€ option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

Community vote distribution
C (100%)

Mazhar1993 Highly Voted 9 months, 1 week ago
The authentication method the developers should use is Active Directory integrated authentication.

Active Directory integrated authentication: Seamless integration with on-premises Active Directory, minimizing authentication prompts and ensuring

efficient user experience.
Azure AD token: Not suitable for on-premises Active Directory authentication in a hybrid environment.
Azure Multi-Factor authentication: Adds unnecessary complexity and authentication steps, not ideal for minimizing prompts.

https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/azure-ad-authentication-sql-server-overview?view=sql-server-ver16#azure-active-directory-integrated

upvoted 8 times

zellck Highly Voted 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/azure-ad-authentication-sql-server-overview?view=sql-server-ver16#azure-active-directory-integrated
When the Windows domain is synchronized with Azure AD, and a user is logged into the Windows domain, the user's Windows credentials are used for Azure AD authentication.

upvoted 5 times

STC007 1 year, 9 months ago

Thanks for your explanation and for sharing the Azure lynk.

upvoted 1 times

Ash_B38 1 year, 6 months ago

Great explanation!

upvoted 1 times

Ruffyit Most Recent 2 months, 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/azure-ad-authentication-sql-server-overview?view=sql-server-ver16#azure-active-directory-integrated

upvoted 1 times

stonwall12 4 months, 2 weeks ago

Selected Answer: C

Answer: C, Active Directory integrated authentication

Reason: This method allows seamless authentication using the developers' on-premises Active Directory accounts, which are synchronized with Azure AD in the hybrid setup. It minimizes authentication prompts by leveraging the existing Windows login credentials on their hybrid Azure AD joined Windows 10 computers.

Reference: https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-overview?view=azuresql#connecting-using-azure-ad-identities

upvoted 1 times

Ruffyit 8 months, 2 weeks ago

The authentication method the developers should use is Active Directory integrated authentication.

Active Directory integrated authentication: Seamless integration with on-premises Active Directory, minimizing authentication prompts and ensuring efficient user experience.
Azure AD token: Not suitable for on-premises Active Directory authentication in a hybrid environment.
Azure Multi-Factor authentication: Adds unnecessary complexity and authentication steps, not ideal for minimizing prompts.

https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/azure-ad-authentication-sql-server-overview?view=sql-server-ver16#azure-active-directory-integrated

upvoted 2 times

ESAJRR 1 year, 11 months ago

Selected Answer: C

C. Active Directory integrated authentication.

upvoted 3 times

majstor86 2 years, 4 months ago

Selected Answer: C

C. Active Directory integrated authentication.

upvoted 2 times

awron_durat 2 years, 6 months ago

Selected Answer: C

C is correct.

upvoted 2 times

God2029 2 years, 6 months ago

It is correct. I am using the same config in Prod env.

upvoted 1 times

ahmadmohdrudin 2 years, 9 months ago

C is Correct, Tested in lab environment

upvoted 1 times

9to5 2 years, 10 months ago

Selected Answer: C

C is correct.

upvoted 2 times

Armanas 2 years, 10 months ago

Any link to verify that the answer is correct?

upvoted 1 times

coyoteee 2 years, 5 months ago

Its clearly C. Active Directory integrated authentication.
Other answers are wrong so no need to link to verify. Just think.

upvoted 1 times

Wis10 2 years, 5 months ago

https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?view=azuresql&tabs=azure-powershell#using-an-azure-ad-identity-to-connect-using-ssms-or-ssdt

upvoted 4 times

Question #19 *Topic 1*

You have been tasked with enabling Advanced Threat Protection for an Azure SQL Database server.
Advanced Threat Protection must be configured to identify all types of threat detection.
Which of the following will happen if when a faulty SQL statement is generate in the database by an application?

A. A Potential SQL injection alert is triggered.

B. A Vulnerability to SQL injection alert is triggered.

C. An Access from a potentially harmful application alert is triggered.

D. A Brute force SQL credentials alert is triggered.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

Community vote distribution
B (63%) A (37%)

⊟ **Rume** Highly Voted 👍 4 years ago
A possible vulnerability to SQL Injection
(SQL.VM_VulnerabilityToSqlInjection
SQL.DB_VulnerabilityToSqlInjection
SQL.MI_VulnerabilityToSqlInjection
SQL.DW_VulnerabilityToSqlInjection)
An application has generated a faulty SQL statement in the database. This can indicate a possible vulnerability to SQL injection attacks. There are two possible reasons for a faulty statement. A defect in application code might have constructed the faulty SQL statement. Or, application code or stored procedures didn't sanitize user input when constructing the faulty SQL statement, which can be exploited for SQL injection.)

https://docs.microsoft.com/en-us/azure/security-center/alerts-reference#alerts-sql-db-and-warehouse
upvoted 52 times

⊟ **MeisAdriano** 1 year, 8 months ago
I agree: possibile
upvoted 2 times

⊟ **NarenderSingh** Highly Voted 👍 3 years, 7 months ago
Selected Answer: B
correct
upvoted 6 times

⊟ **Knighthell** Most Recent 🕒 3 weeks, 1 day ago
Selected Answer: A
https://learn.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview?view=azuresql
upvoted 2 times

⊟ **mmmyo** 1 month, 3 weeks ago
Selected Answer: A
The correct answer is A. A Potential SQL injection alert is triggered.

Here's why: Azure SQL Database Advanced Threat Protection (ATP) includes built-in security monitoring for detecting potential SQL injection attacks, which occur when an application generates faulty or suspicious SQL statements that could be exploited by attackers to manipulate database queries. When ATP is enabled, it actively analyzes queries and flags anomalous patterns indicative of SQL injection attempts.

Option B (Vulnerability to SQL injection alert) is not correct, as this type of alert is raised when ATP detects misconfigurations or weak security settings that could make the database susceptible to SQL injection—not when an actual faulty SQL statement is executed.

Option C (Access from a potentially harmful application alert) applies when an application known for malicious behavior tries to access the database.

Option D (Brute force SQL credentials alert) detects repeated authentication attempts trying to guess database credentials.
upvoted 2 times

eldoktor 2 months ago

Selected Answer: A

this question is worded in weird way that makes you answer wrong
upvoted 1 times

Ruffyit 2 months, 2 weeks ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/security-center/alerts-reference#alerts-sql-db-and-warehouse
upvoted 1 times

Fule 2 months, 3 weeks ago

Selected Answer: A

SQL Vulnerability Assessment - Identifies misconfiguration or weak points in your database

When Advanced Threat Protection (ATP) is enabled for an Azure SQL Database, it continuously monitors database activity and uses machine learning and behavioral analysis to detect potential security threats.
upvoted 1 times

Paarth 3 months ago

Selected Answer: A

If an application generates a faulty SQL statement, Azure ATP might detect it as a potential SQL injection attempt, especially if the statement appears to be malformed or crafted to exploit vulnerabilities. For Option B: This alert is not triggered by an actual faulty SQL statement execution, but rather by a security assessment scan that detects misconfigured security settings that make SQL injection possible.
upvoted 1 times

9a0549a 3 months, 1 week ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview?view=azuresql under "Explore detection of a suspicious event"
upvoted 1 times

nahdft 3 months, 1 week ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview?view=azuresql
upvoted 1 times

Saluk_DE 4 months ago

Selected Answer: B

Reference: https://learn.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview?view=azuresql#advanced-threat-protection-alerts
It literally says in red on the screenshot seen in the link "Potential exploitation of application code - vulnerability to SQL Injection was detected." So B is correct.
upvoted 1 times

stonwall12 4 months, 2 weeks ago

Selected Answer: A

Answer: A, Potential SQL injection alert is triggered.

Reason: Check the reference link and you'll see the system triggers a "Potential SQL injection" alert to notify administrators for this type of suspicious acitivty.

Reference: https://learn.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview?view=azuresql#advanced-threat-protection-alerts
upvoted 1 times

> **Saluk_DE** 4 months ago
>
> It literally says on the screenshot seen in your link "Potential exploitation of application code - vulnerability to SQL Injection was detected." So B is correct.
> upvoted 1 times

Ruffyit 8 months, 2 weeks ago

b correct

upvoted 1 times

Custodian 9 months, 1 week ago

What kind of alerts does Microsoft Defender for SQL provide?
Threat intelligence enriched security alerts are triggered when there's:

Potential SQL injection attacks - including vulnerabilities detected when applications generate a faulty SQL statement in the database
Anomalous database access and query patterns - for example, an abnormally high number of failed sign-in attempts with different credentials (a brute force attempt)
Suspicious database activity - for example, a legitimate user accessing an SQL Server from a breached computer which communicated with a crypto-mining C&C server

Alerts include details of the incident that triggered them, as well as recommendations on how to investigate and remediate threats.

upvoted 1 times

awfnewf1q243 9 months, 1 week ago

Selected Answer: B

A possible vulnerability to SQL Injection:

"An application has generated a faulty SQL statement in the database. This can indicate a possible vulnerability to SQL injection attacks. There are two possible reasons for a faulty statement. A defect in application code might have constructed the faulty SQL statement. Or, application code or stored procedures didn't sanitize user input when constructing the faulty SQL statement, which can be exploited for SQL injection."

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference#alerts-sql-db-and-warehouse

upvoted 2 times

Seelearndo 9 months, 1 week ago

Selected Answer: B

Alert: A possible vulnerability to SQL Injection
Description: An application has generated a faulty SQL statement in the database. This can indicate a possible vulnerability to SQL injection attacks. There are two possible reasons for a faulty statement. A defect in application code might have constructed the faulty SQL statement. Or, application code or stored procedures didn't sanitize user input when constructing the faulty SQL statement, which can be exploited for SQL injection.
↑ B is the correct answer since a faulty SQL statement will result in a possible vulnerability alert.

Alert: Potential SQL injection
Description: An active exploit has occurred against an identified application vulnerable to SQL injection. This means an attacker is trying to inject malicious SQL statements by using the vulnerable application code or stored procedures.
↑ A is incorrect since a potential SQL injection alert is triggered when an active exploit is identified.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference#alerts-sql-db-and-warehouse

upvoted 3 times

majstor86 9 months, 1 week ago

Selected Answer: B

B. Vulnerability to SQL injection – an alert is triggered when an application generates a faulty SQL statement in your SQL database

Potential SQL injection - This alert is triggered when the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

upvoted 4 times

Question #20 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
You are in the process of creating an Azure Kubernetes Service (AKS) cluster. The Azure Kubernetes Service (AKS) cluster must be able to connect to an Azure
Container Registry.
You want to make sure that Azure Kubernetes Service (AKS) cluster authenticates to the Azure Container Registry by making use of the auto-generated service principal.
Solution: You create an Azure Active Directory (Azure AD) role assignment.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *A*
When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

Community vote distribution
B (77%) A (23%)

romaso82 Highly Voted 3 years, 11 months ago
correct answer
upvoted 18 times

PKPKPK Highly Voted 3 years, 6 months ago
Selected Answer: B
i think its B as it wold need an RBAC role instead AAD role
upvoted 16 times

xRiot007 11 months, 2 weeks ago
The answer is B, but not because of that. The Microsoft Entra group will attach the AcrPull permission automatically, completing RBAC. The reason why the answer is No is because the authentication is done automatically, you don't have to create any roles. You just need to attach the service (AKS) to the container (ACR)
upvoted 7 times

chema77 8 months, 2 weeks ago
Sorry to dissagree:

The answer is B instead of A because of the Entra/RBAC thing. But we'd rather choose A when the option is RBAC (az-500 is about security):

"To avoid needing an Owner or Azure account administrator role, you can also manually configure a service principal to pull images from ACR. For more information, see ACR authentication with service principals or Authenticate from Kubernetes with a pull secret. Alternatively, you can use a managed identity instead of a service principal for easier management."

https://learn.microsoft.com/en-us/azure/aks/tutorial-kubernetes-deploy-cluster?tabs=azure-cli
upvoted 2 times

chema77 8 months, 2 weeks ago
https://learn.microsoft.com/en-us/azure/container-registry/container-registry-auth-service-principal#when-to-use-a-service-principal
upvoted 1 times

Knighthell Most Recent 3 weeks, 1 day ago
Selected Answer: B
need AcrPull on Container Registry.

upvoted 1 times

Duyons 2 months ago

Selected Answer: A

Hey everyone, just to clarify this question is correct as written.

AKS does not get AcrPull permission by default when using a service principal, unless you explicitly grant it.

This solution says:

"You create an Azure Active Directory (Azure AD) role assignment."

That means you manually assign the required role (like AcrPull) to the auto-generated service principal, so that AKS can pull images from the Azure Container Registry.

So yes, this meets the goal.
Correct answer: A. Yes

Hope that helps!

upvoted 3 times

alber0077 1 month, 2 weeks ago

acrpull is not an azure ad role

upvoted 1 times

Ruffyit 2 months, 2 weeks ago

Selected Answer: B

The answer is B, but not because of that. The Microsoft Entra group will attach the AcrPull permission automatically, completing RBAC. The reason why the answer is No is because the authentication is done automatically, you don't have to create any roles. You just need to attach the service (AKS) to the container (ACR)

upvoted 1 times

gauravwagh16193 2 months, 3 weeks ago

Selected Answer: B

No, the solution does not meet the goal.

To ensure that the Azure Kubernetes Service (AKS) cluster can authenticate to the Azure Container Registry using the auto-generated service principal, you need to assign the AcrPull role to the service principal associated with the AKS cluster. Creating an Azure Active Directory (Azure AD) role assignment alone does not automatically configure the necessary permissions for the AKS cluster to pull images from the Azure Container Registry.

upvoted 1 times

stonwall12 4 months, 2 weeks ago

Selected Answer: B

Answer: B, No

Reason: Creating an Azure AD role assignment alone does not enable AKS to authenticate to ACR using the auto-generated service principal. Instead, you need to grant the AKS-generated service principal the appropriate permissions on the ACR using the AcrPull role. This allows AKS to pull images from the ACR without additional configuration.

Reference: https://learn.microsoft.com/en-us/azure/aks/cluster-container-registry-integration?tabs=azure-cli#create-a-new-aks-cluster-with-acr-integration

upvoted 1 times

AdityaGupta 5 months, 3 weeks ago

Selected Answer: B

A service principal is recommended in several Kubernetes scenarios to pull images from an Azure container registry. With Azure Kubernetes Service (AKS), you can also use an automated mechanism to authenticate with a target registry by enabling the cluster's managed identity.

upvoted 1 times

AdityaGupta 3 months, 1 week ago

Correction: Answer is A.
Referring to question, we already have an auto-generated SPN the next task should be AAD role assignment to this SPN.

Explanation: -
When to Use Each?

Use SPN if:
AKS and ACR are in different subscriptions or different tenants.
You require manual control over credentials and role assignments.
You are using an automation system that depends on SPNs.

Use Managed Identity if:
You want passwordless authentication and automatic identity management.
AKS and ACR are in the same subscription.
You follow Azure best practices for security and identity management.
upvoted 1 times

Ruffyit 8 months, 2 weeks ago
b is correct
upvoted 1 times

forfuntwo2 9 months, 1 week ago
Selected Answer: B
In Azure Active Directory (Azure AD), if another administrator or non-administrator needs to manage Azure AD resources, you assign them an Azure AD role that provides the permissions they need. For example, you can assign roles to allow adding or changing users, resetting user passwords, managing user licenses, or managing domain names.

This article lists the Azure AD built-in roles you can assign to allow management of Azure AD resources. For information about how to assign roles, see Assign Azure AD roles to users. If you are looking for roles to manage Azure resources, see Azure built-in roles.
upvoted 1 times

Mazhar1993 9 months, 1 week ago
The answer is No.

When an AKS cluster is created, Azure automatically generates a service principal to facilitate interactions with other Azure resources, including ACR.
This auto-generated service principal can be directly used for authenticating the AKS cluster to the ACR registry.
Therefore, creating an additional Azure AD role assignment is unnecessary as the auto-generated service principal already fulfills the authentication requirements.
The proposed solution of creating an Azure AD role assignment adds complexity without providing any additional benefit, making it unnecessary and not meeting the goal efficiently.

https://learn.microsoft.com/bs-latn-ba/azure/aks/cluster-container-registry-integration?tabs=azure-cli
upvoted 5 times

pentium75 11 months ago
Why would the auto-generated service principal already have access to my ACR without me assigning a role for that?
upvoted 2 times

pentium75 11 months ago
Selected Answer: B
Unless there's a typo in the question, B because it refers specifically to an "Azure AD role" which is not required here.
upvoted 1 times

fastline112003 11 months, 2 weeks ago
This should be usually done with Azure RBAC:
az aks update -n myAKSCluster -g myResourceGroup --attach-acr <acr-name>
upvoted 1 times

Atom270 1 year ago
Selected Answer: B
Obviously answer is B, why would anyone select A as it is related to role assigment

upvoted 1 times

⊟ **Slawekyo** 1 year, 1 month ago

In Topic 3, question 16. You have the same question but to choose answer, there "Azure Active Directory (Azure AD) role assignment" is correct so answer is def A

upvoted 3 times

⊟ **Jkayx94** 1 year, 4 months ago

Selected Answer: B

Requires ACR-Pull which is an Azure RBAC Built in Role: https://learn.microsoft.com/bs-latn-ba/azure/role-based-access-control/built-in-roles#acrpull

Answer is B

upvoted 1 times

⊟ **[Removed]** 1 year, 6 months ago

The AKS to ACR integration assigns the AcrPull role to the Microsoft Entra ID managed identity associated with the agent pool in your AKS cluster.

upvoted 2 times

Question #21 *Topic 1*

Your company has an Azure subscription that includes two virtual machines, named VirMac1 and VirMac2, which both have a status of Stopped (Deallocated).

The virtual machines belong to different resource groups, named ResGroup1 and ResGroup2.

You have also created two Azure policies that are both configured with the virtualMachines resource type. The policy configured for ResGroup1 has a policy definition of Not allowed resource types, while the policy configured for ResGroup2 has a policy definition of Allowed resource types.

You then create a Read-only resource lock on VirMac1, as well as a Read-only resource lock on ResGroup2.

Which of the following is TRUE with regards to the scenario? (Choose all that apply.)

A. You will be able to start VirMac1.

B. You will NOT be able to start VirMac1.

C. You will be able to create a virtual machine in ResGroup2.

D. You will NOT be able to create a virtual machine in ResGroup2.

Suggested Answer: *BC*

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

Community vote distribution

BD (93%) 4%

SajjadKarim Highly Voted 3 years, 11 months ago

Correct answer is B and D,

When you will create a virtual machine in ResGroup2 it will give you error

"The selected resource group is read only"

upvoted 75 times

dumdada 3 years, 10 months ago

correct

upvoted 5 times

[Removed] 3 years, 7 months ago

correct

upvoted 4 times

justjeroen 2 years, 1 month ago

But you dont crate virmac2, you only start virmac2. This should not be considered a change in the resource group.

upvoted 1 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#considerations-before-applying-your-locks

A read-only lock on a resource group that contains a virtual machine prevents all users from starting or restarting a virtual machine. These operations require a POST method request.

upvoted 11 times

Yiannisthe7th Highly Voted 3 years, 11 months ago

B and D for sure.

When you create a new VM and select a read-only resource group you get a "The selected resource group is read only"

upvoted 12 times

DarkCyberGhost 3 years, 5 months ago

but the Rrsource group is not set to read-only. Virmac1 and 2 is set to read-only, the resource group 2 in which virmac2 sits has a policy of resource is allowed. so machines can be created in the group. so to me the Answer is B and C

upvoted 3 times

Joshing 3 years, 4 months ago

Virmac1 is read-only and so is ResGroup2. You cannot start Virmac1 and cannot create a VM in ResGroup2.

upvoted 4 times

Rednevi Most Recent 3 months, 1 week ago

Selected Answer: BD

Statement B is true: The Read-only lock on VirMac1 prevents it from being started.

Statement D's validity depends on the specific configuration of the Allowed resource types policy in ResGroup2. If virtual machines are not permitted by the policy, then Statement D is true; otherwise, it is false.

upvoted 1 times

Ruffyit 8 months, 2 weeks ago

A read-only lock on a resource group that contains a virtual machine prevents all users from starting or restarting a virtual machine. These operations require a POST method request

upvoted 2 times

153a793 9 months, 2 weeks ago

Answer should be BD. if a resource group has a read-only lock, you won't be able to start a virtual machine (VM) that is in a Stopped (Deallocated) state. A read-only lock prevents any changes to the resources within the resource group, including starting or stopping VMs.

upvoted 1 times

thatazureguy 9 months, 4 weeks ago

B and C

A Read only lock on RG doesn't prevent to create new resources

upvoted 1 times

xRiot007 11 months, 2 weeks ago

B - You cannot start Mac1 because starting a VM involves a POST request, which will not be done while the resource is Read-only

D - for the same reason.

upvoted 2 times

Data_Works 1 year ago

Selected Answer: BD

Read-only lock on a resource prevents all write operations, including changing the state of the VM (such as starting or stopping it)

upvoted 3 times

Jimmy500 1 year ago

For virtual machine Virmac1 we have read only lock which will not allow to start stop delete it so the answer for the VirMac1 will be B . For the resource group - ResGroup2 we also have same Read only which basically will not allow to do anyything else besides current config then answer for this will be D.

Correct answer will be here BD but keep in mind that question says Read Only lock there can be also CanNotDelete lock as well in the other question then we can start machine for example but can not delete machine. Please refer this link for more information but here answer is BD.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json

upvoted 2 times

Mazhar1993 1 year, 2 months ago

You will be able to start VirMac1.

TRUE: Read-only locks don't affect starting a virtual machine; they only prevent modifications or deletions.

You will NOT be able to start VirMac1.

NOT TRUE: Read-only locks don't restrict starting a virtual machine; they only prevent modifications or deletions.

You will be able to create a virtual machine in ResGroup2.

TRUE: The policy for ResGroup2 allows virtual machine creation, and read-only locks only prevent modifications, not creations.

You will NOT be able to create a virtual machine in ResGroup2.

NOT TRUE: The policy for ResGroup2 permits virtual machine creation, and read-only locks only prevent modifications, not creations.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#considerations-before-applying-your-locks

upvoted 2 times

> **Wezen** 1 year ago
>
> A read-only lock on a resource group that contains a virtual machine prevents all users from starting or restarting a virtual machine. These operations require a POST method request
>
> upvoted 1 times

Ruffyit 1 year, 3 months ago

Correct answer is B and D,
When you will create a virtual machine in ResGroup2 it will give you error
"The selected resource group is read only"
upvoted 1 times

b9e98e8 1 year, 4 months ago

Azure Policy focuses on pre-deployment compliance, while Resource Locks safeguard resources post-deployment against accidental changes.
Given a scenario where VM is allowed policy and resource lock both are working on RG level then according to pre deployment compliance you are able to create a VM in that RG
but according to post deployment protection through resource lock you wont be able to make any write activity(restarting or changing disk etc) on existing VM in that RG.
upvoted 1 times

zied01 1 year, 7 months ago

i can't understand what is the relation here between the azure policy and azure locks ?!!! cause the question indicate two different things !
upvoted 1 times

Feraso 1 year, 8 months ago

Selected Answer: BD

I just tested in the lab and BD are the correct answers.

B:
You can't start the VM that has read only lock, you will be getting this error:
Failed to start virtual machine 'WinServer1'. Error: The scope 'WinServer1' cannot perform write operation because following scope(s) are locked: '/subscriptions/be739432-1223-4cbf-bc85-1287e4269fe6/resourceGroups/TestLAB/providers/Microsoft.Compute/virtualMachines/WinServer1'. Please remove the lock and try again.

D:
Setting the resource group to read only will prevent you from creating virtual machines.
You will get an error that the resource group is read only.
upvoted 7 times

MeisAdriano 1 year, 8 months ago

Selected Answer: BD

B: A read-only lock on a resource group that contains a virtual machine prevents all users from starting or restarting a virtual machine. These operations require a POST method request

D: A read-only lock on a resource group prevents users from moving any new resource into that resource group.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#considerations-before-applying-your-locks
upvoted 1 times

ittchmh 1 year, 9 months ago

Selected Answer: BD

Mistyped, I can't remove or change my comments

I will go with BD
upvoted 1 times

ittchmh 1 year, 9 months ago

Selected Answer: BC

I will go with BC
upvoted 1 times

Question #22 *Topic 1*

You have been tasked with delegate administrative access to your company's Azure key vault.
You have to make sure that a specific user can set advanced access policies for the key vault. You also have to make sure that access is assigned based on the principle of least privilege.
Which of the following options should you use to achieve your goal?

A. Azure Information Protection B. RBAC

C. Azure AD Privileged Identity Management (PIM)

D. Azure DevOps

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

wallythebos Highly Voted 👍 3 years, 9 months ago
For those that won't see it B is right in front of the option A.
upvoted 56 times

> **cfsxtuv33** 3 years, 6 months ago
> Ahh, thats funny, I kept seeing contributors saying B sits in front of A. i was like what the heck are they talking about!? Then I saw it....sitting in the same row as "A." So yeah, option "B" RBAC is correct.
> upvoted 4 times

somenick Highly Voted 👍 2 years, 9 months ago
Admins please fix formatting so the option B is on the new line
upvoted 16 times

stonwall12 Most Recent 🕒 4 months, 2 weeks ago
Selected Answer: C
Answer: It's cooked, the answer is B, RBAC

Reason: Role-Based Access Control (RBAC) in Azure allows you to assign specific permissions to users based on their roles, adhering to the principle of least privilege. For managing advanced access policies in Azure Key Vault, the 'Key Vault Contributor' role provides the necessary permissions without granting excessive access.

Reference: https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide
upvoted 1 times

AdityaGupta 5 months, 2 weeks ago
Selected Answer: A
It can be either RBAC or Access Policies. We have option B as RBAC.
upvoted 2 times

xRiot007 11 months, 2 weeks ago
You can't use PIM (C) for this scenario so go for RBAC (B).
In a real life scenario, the user would have a ticket on a backlog that he is required to complete after setting up. Then you de-assign the role from his identity, to respect the least privilege principle, unless the user is explicitly required permanent access from then onwards.
upvoted 1 times

Mazhar1993 1 year, 2 months ago
The correct answer is RBAC.
RBAC allows you to assign specific roles like Key Vault Contributor, which grants the user the ability to set advanced access policies, ensuring access based on the principle of least privilege.
Azure Information Protection focuses on data classification, labeling, and protection, not managing access to Azure Key Vault.
While Azure AD Privileged Identity Management offers time-based and approval-based role activation, it doesn't directly manage access to Azure Key Vault or allow setting advanced access policies for it.
Azure DevOps is primarily a set of services for software development, not for managing access to Azure Key Vault.

https://learn.microsoft.com/en-us/azure/key-vault/general/security-features

upvoted 3 times

Andre369 2 years, 1 month ago

B. RBAC (Role-Based Access Control)

RBAC allows you to grant specific permissions to users, groups, or service principals based on their roles. By assigning the appropriate RBAC role to the specific user, you can grant them the necessary permissions to set advanced access policies for the Key Vault, while ensuring that they only have the minimum privileges required for their tasks.

RBAC provides a granular level of control over access to Azure resources, allowing you to assign roles such as "Key Vault Contributor" or "Key Vault Administrator" to the user, depending on the level of access needed. This ensures that the user has the necessary permissions to manage the Key Vault without granting excessive privileges.

upvoted 4 times

FedericoBellotti 2 years, 1 month ago

the b is not visible

upvoted 1 times

zellck 2 years, 1 month ago

B is the answer.

https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-migration

Azure role-based access control (Azure RBAC) is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources. With Azure RBAC you control access to resources by creating role assignments, which consist of three elements: a security principal, a role definition (predefined set of permissions), and a scope (group of resources or individual resource).

upvoted 2 times

Dinya_jui 2 years, 3 months ago

correct answer B

upvoted 1 times

majstor86 2 years, 4 months ago

B. RBAC

upvoted 2 times

brutananadilewski0000 2 years, 4 months ago

Just to notify you that the answer B is RBAC

upvoted 1 times

AZ5cert 2 years, 6 months ago

B: RBAC

upvoted 1 times

Irishtk 3 years, 2 months ago

Ans is B (RBAC)

"Authorization in Key Vault uses a combination of Azure role-based access control (Azure RBAC) and Azure Key Vault access policies"

https://docs.microsoft.com/en-us/azure/key-vault/general/security-features

upvoted 6 times

TheLegendPasha 3 years, 2 months ago

The answer is B but for some reason is BUGGED.

upvoted 2 times

in_da_cloud 3 years, 3 months ago

The answer is B:

The management plane uses RBAC - this is where you manage Key Vault itself which implies creating and deleting key vaults, retrieving Key Vault properties, and updating access policies.

https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#access-model-overview

upvoted 2 times

Eltooth 3 years, 3 months ago

B is correct answer.

upvoted 1 times

Question #23 *Topic 1*

You have been tasked with delegate administrative access to your company's Azure key vault.
You have to make sure that a specific user is able to add and delete certificates in the key vault. You also have to make sure that access is assigned based on the principle of least privilege.
Which of the following options should you use to achieve your goal?

A. A key vault access policy

B. Azure policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure DevOps

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

Community vote distribution

A (96%) 4%

SecurityAnalyst Highly Voted 3 years, 4 months ago
# IN EXAM - 31/8/2021
upvoted 15 times

nexel Highly Voted 3 years, 5 months ago
A is correct
upvoted 13 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: A
Answer: A, Key vault access policy

Reason: Key vault access policies allow you to grant specific permissions for managing certificates in Azure Key Vault. This method provides granular control over actions like adding and deleting certificates, adhering to the principle of least privilege by granting only the necessary permissions to the user.

Reference: https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal
upvoted 2 times

AdityaGupta 5 months, 2 weeks ago
Selected Answer: A
Azure Key Vault Access Policies are used for granular control on key vault Keys, secrets, certificates.
upvoted 1 times

Ruffyit 9 months, 1 week ago
These operations are done on the key vault's data plane. The suitable built-in role would be a Key Vault Certificates Officer - able to perform any action on the certificates of a key vault, except manage permissions.
upvoted 4 times

jacqs101 11 months, 1 week ago
Answer A is correct - RBAC gives you access to the vault (management plane), Key vault policies grants access to the data within the vault (data plane)
upvoted 4 times

wardy1983 1 year, 1 month ago
Answer: A

Explanation:
These operations are done on the key vault's data plane. The suitable built-in role would be a Key Vault Certificates Officer - able to perform any action

on the certificates of a key vault, except manage permissions.

Reference: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

upvoted 2 times

⊟ **JunetGoyal** 1 year, 2 months ago

KW has 2 models for access 1. RBAC 2. KW policy.

If you want more control one should go for KW policy

Ans a

upvoted 1 times

⊟ **TheProfessor** 1 year, 3 months ago

Selected Answer: A

The answer is: A

upvoted 2 times

⊟ **ESAJRR** 1 year, 4 months ago

Selected Answer: A

A. A key vault access policy

upvoted 1 times

⊟ **zellck** 1 year, 7 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy

A Key Vault access policy determines whether a given security principal, namely a user, application or user group, can perform different operations on Key Vault secrets, keys, and certificates. You can assign access policies using the Azure portal, the Azure CLI, or Azure PowerShell.

upvoted 2 times

⊟ **Dinya_jui** 1 year, 9 months ago

correct answer A

upvoted 1 times

⊟ **majstor86** 1 year, 10 months ago

Selected Answer: A

A. A key vault access policy

upvoted 2 times

⊟ **AZ5cert** 2 years ago

A. A key vault access policy

upvoted 1 times

⊟ **jore041** 2 years, 2 months ago

Selected Answer: A

A is correct

upvoted 1 times

⊟ **us3r** 2 years, 8 months ago

Selected Answer: A

vote A

upvoted 3 times

⊟ **in_da_cloud** 2 years, 9 months ago

Selected Answer: A

The answer is A:

These operations are done on the key vault's data plane. The suitable built-in role would be a Key Vault Certificates Officer - able to perform any action on the certificates of a key vault, except manage permissions.

https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli#azure-built-in-roles-for-key-vault-data-plane-operations

upvoted 5 times

Question #24 *Topic 1*

You have an Azure virtual machine that runs Windows Server R2.
You plan to deploy and configure an Azure Key vault, and enable Azure Disk Encryption for the virtual machine.
Which of the following is TRUE with regards to Azure Disk Encryption for a Windows VM?

A. It is supported for basic tier VMs.

B. It is supported for standard tier VMs.

C. It is supported for VMs configured with software-based RAID systems.

D. It is supported for VMs configured with Storage Spaces Direct (S2D).

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows

Community vote distribution

B (100%)

cfsxtuv33 Highly Voted 3 years, 6 months ago
The answer is correct. It seems there is quite a few Key Vault questions so far. There is a guy "John Savill" on Youtube who has an excellent "deep dive" course on Azure Key Vault that is worth watching.
Link: https://www.youtube.com/results?search_query=john+savill+key+vault
upvoted 34 times

g2s 2 years, 9 months ago
I love his videos
upvoted 6 times

perkarelei Highly Voted 3 years, 12 months ago
Seems to be correct.

From the reference link, Unsupported scenarios:

- Encrypting basic tier VM or VMs created through the classic VM creation method.
- Encrypting VMs configured with software-based RAID systems.
- Encrypting VMs configured with Storage Spaces Direct (S2D)

This leaves us with only one option: B
upvoted 19 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: B
Answer: B, standard tier VMs.

Reason: Azure Disk Encryption is supported for standard tier VMs running Windows Server. It is not supported for basic tier VMs, VMs configured with software-based RAID systems, or VMs using Storage Spaces Direct (S2D). Standard tier VMs provide the necessary capabilities and performance to support disk encryption without compromising functionality.

Reference: https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview#unsupported-scenarios
upvoted 2 times

Cafisho 7 months, 2 weeks ago
B. All the others are not supported:
https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows#restrictions
upvoted 2 times

ESAJRR 1 year, 10 months ago
Selected Answer: B
B. It is supported for standard tier VMs.

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows#unsupported-scenarios
Azure Disk Encryption does not work for the following scenarios, features, and technology:
- Encrypting basic tier VM or VMs created through the classic VM creation method.
- Encrypting VMs configured with software-based RAID systems.
- Encrypting VMs configured with Storage Spaces Direct (S2D), or Windows Server versions before 2016 configured with Windows Storage Spaces.

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. It is supported for standard tier VMs.

upvoted 3 times

AldoM 3 years, 2 months ago

Supported VMs
Windows VMs are available in a range of sizes. Azure Disk Encryption is supported on Generation 1 and Generation 2 VMs. Azure Disk Encryption is also available for VMs with premium storage.

Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines with a less than 2 GB of memory. For more exceptions, see Azure Disk Encryption: Unsupported scenarios.

upvoted 4 times

us3r 3 years, 2 months ago

Selected Answer: B

standard it is

upvoted 2 times

Eltooth 3 years, 3 months ago

Supported VMs
Windows VMs are available in a range of sizes. Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines with a less than 2 GB of memory.
Azure Disk Encryption is also available for VMs with premium storage.
Azure Disk Encryption is now available on Generation 2 VMs and Lsv2-series VMs.

Supported operating systems
Windows client: Windows 8 and later.
Windows Server: Windows Server 2008 R2 and later.
Windows 10 Enterprise multi-session.

https://docs.microsoft.com/en-gb/learn/modules/host-security/8-disk-encryption

upvoted 2 times

Eltooth 3 years, 3 months ago

Selected Answer: B

B is correct answer

upvoted 2 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 3 times

Sumeetsingh555 3 years, 7 months ago

Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines with a less than 2 GB of memory. For more exceptions, see Azure Disk Encryption: Unsupported scenarios. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview. Option B is correct

upvoted 7 times

Question #25 *Topic 1*

You have an Azure virtual machine that runs Ubuntu 16.04-DAILY-LTS.
You plan to deploy and configure an Azure Key vault, and enable Azure Disk Encryption for the virtual machine.
Which of the following is TRUE with regards to Azure Disk Encryption for a Linux VM?

A. It is NOT supported for basic tier VMs.

B. It is NOT supported for standard tier VMs.

C. OS drive encryption for Linux virtual machine scale sets is supported.

D. Custom image encryption is supported.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux

Community vote distribution
A (75%) D (25%)

azcourse Highly Voted 👍 3 years, 8 months ago
option A is correct . you can find Unsupported scenarios
Azure Disk Encryption does not work for the following Linux scenarios, features, and technology:

Encrypting basic tier VM or VMs created through the classic VM creation method.
Disabling encryption on an OS drive or data drive of a Linux VM when the OS drive is encrypted.
Encrypting the OS drive for Linux virtual machine scale sets.
Encrypting custom images on Linux VMs.
Integration with an on-premises key management system.
Azure Files (shared file system).
Network File System (NFS).
Dynamic volumes.
Ephemeral OS disks.
upvoted 17 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: A
Answer: A, NOT supported for basic tier VMs.

Reason: Azure Disk Encryption is not supported for basic tier VMs in Linux, just as with Windows VMs. It is supported for standard tier VMs. OS drive encryption for Linux virtual machine scale sets is not supported, and custom image encryption is also not supported for Linux VMs. These limitations apply specifically to Linux VMs to ensure compatibility and performance.

Reference: https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#unsupported-scenarios
upvoted 2 times

Andreas_Czech 7 months, 1 week ago
Selected Answer: A
Option A is correct (It is NOT supported for basic tier VMs)

https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux?tabs=azcliazure%2Cenableadecli%2Cefacli%2Cadedatacli#restrictions

regarding the Information in the upper Link:

Azure Disk Encryption does NOT work for the following Linux scenarios, features, and technology:

1. Encrypting basic tier VM or VMs created through the classic VM creation method.
2. Encrypting the OS drive for Linux Virtual Machine Scale Sets.

3. Encrypting custom images on Linux VMs.

1. is exactly A (It is NOT supported for basic tier VMs.)
2. permits C (OS drive encryption for Linux virtual machine scale sets is supported.)
3. permits D (Custom image encryption is supported.)

the Option A is exactly met

upvoted 1 times

Ruffyit 8 months, 2 weeks ago

A because ADE is not supported for Basic tier
Not D because ADE is not supported on Ubuntu 16

upvoted 1 times

pentium75 11 months ago

Selected Answer: A

A because ADE is not supported for Basic tier
Not D because ADE is not supported on Ubuntu 16

upvoted 1 times

djiongocedrigue 11 months, 3 weeks ago

Selected Answer: D

Azure Disk Encryption supports encryption of custom images for Linux VMs.

upvoted 1 times

cluqueg 9 months, 2 weeks ago

This case is in the list of scenarios that does NOT work:
https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux

upvoted 2 times

JaridB 1 year, 1 month ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux

Here is a quote from the document:
Azure Disk Encryption is supported on both basic and standard tier VMs.
The document also says that custom image encryption is supported.
Here is a quote from the document:
Custom image encryption is supported.

The answer is not A
Answer is D

upvoted 1 times

March2023 10 months ago

Ubuntu 16.xx is not a supported OS https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#supported-vms-and-operating-systems

upvoted 1 times

2c7fd04 11 months, 3 weeks ago

This is not correct (https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview); MS says this: Azure Disk Encryption is also not available on Basic, A-series VMs, or on virtual machines that do not meet these minimum memory requirements....)

upvoted 2 times

Jimmy500 1 year ago

yes questions also says is not supported and you also same same but you choose D why answer is A

upvoted 1 times

ESAJRR 1 year, 10 months ago

Selected Answer: A

A. It is NOT supported for basic tier VMs.

upvoted 1 times

AzureAdventure 1 year, 11 months ago https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#:~:text=Azure%20Disk%20Encryption%20is%20also%20not%20available%20on%20Basic%2C%20A%2Dseries%20VMs

upvoted 1 times

Sonall 2 years, 1 month ago

It feels like the question is specific towards the version of the Linux Distribution: Ubuntu 16.04-DAILY-LTS, which is not supported by Azure Disk Encryption, based on this article:
https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview
and according to the link, the lowest version supported is 18.04-DAILY-LTS.

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: D

D. Custom image encryption is supported.

With Azure Disk Encryption, you can encrypt the OS and data disks of Linux virtual machines. It is supported for both basic tier and standard tier VMs.

upvoted 2 times

onewheelwheelie 1 year, 7 months ago

This is not correct, "Encrypting custom images on Linux VMs." is listed directly under the list of scnearios where a Linux VM can NOT be encrypted.

upvoted 5 times

zellck 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux#unsupported-scenarios
Azure Disk Encryption does not work for the following Linux scenarios, features, and technology:
- Encrypting basic tier VM or VMs created through the classic VM creation method.

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: A

A. It is NOT supported for basic tier VMs.

upvoted 3 times

003nickm 2 years, 4 months ago

On 2-March-2023, I passed AZ-500 with flying colur. Not direct question.
Asked about steps to configure Azure Disk Encryption using Keyvault

upvoted 4 times

Irishtk 3 years, 2 months ago

Answer is A.
Linux VMSS is not supported, so answer C is false.
"Azure Disk Encryption does not work for the following Linux scenarios, features, and technology: Encrypting basic tier VM or VMs created through the classic VM creation method. Disabling encryption on an OS drive or data drive of a Linux VM when the OS drive is encrypted. Encrypting the OS drive for Linux virtual machine scale sets."
see https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux

upvoted 1 times

MauricioBarrosP 3 years, 2 months ago

Selected Answer: A

Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview

upvoted 1 times

Eltooth 3 years, 3 months ago

Selected Answer: A

A is correct answer.

Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines that do not meet these minimum memory requirements:

https://docs.microsoft.com/en-gb/learn/modules/host-security/8-disk-encryption

upvoted 1 times

Question #26 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
You have configured an Azure Kubernetes Service (AKS) cluster in your testing environment.
You are currently preparing to deploy the cluster to the production environment.
After disabling HTTP application routing, you want to replace it with an application routing solution that allows for reverse proxy and TLS termination for AKS services via a solitary IP address.
You must create an AKS Ingress controller.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. a network security group

C. an application security group

D. an Azure Basic Load Balancer

Suggested Answer: *A*
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
Reference:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

Community vote distribution
A (76%) D (24%)

Lobe Highly Voted 3 years, 11 months ago
Answer is correct
upvoted 19 times

[Removed] Highly Voted 3 years, 8 months ago
Correct! Azure Ingress Controller is used to establish a reverse proxy
upvoted 7 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: A
Answer: A, No adjustment required.

Reason: An AKS Ingress controller is indeed the correct solution for implementing reverse proxy and TLS termination for AKS services using a single IP address. It provides a way to route traffic to multiple services within the Kubernetes cluster, handling TLS termination and acting as a reverse proxy, which aligns with the requirements stated in the question.

Reference: https://learn.microsoft.com/en-us/azure/aks/ingress-basic?tabs=azure-cli
upvoted 1 times

Andreas_Czech 7 months, 1 week ago
Selected Answer: A
A. No adjustment required is correct

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/containers/aks-microservices/aks-microservices#ingress
upvoted 1 times

Ruffyit 8 months, 2 weeks ago
Answer: A
Explanation:
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
Reference:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls
upvoted 3 times

wardy1983 1 year, 7 months ago

Answer: A

Explanation:

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

Reference:

https://docs.microsoft.com/en-us/azure/aks/ingress-tls

upvoted 4 times

ESAJRR 1 year, 10 months ago

Selected Answer: A

A. It is NOT supported for basic tier VMs.

upvoted 2 times

Andre369 2 years, 1 month ago

Selected Answer: D

The correct option to replace HTTP application routing with a solution that allows for reverse proxy and TLS termination for AKS services via a solitary IP address is:

D. an Azure Application Gateway

Azure Application Gateway is a Layer 7 load balancer that can act as an Ingress controller for an AKS cluster. It provides reverse proxy functionality, SSL/TLS termination, and routing capabilities, allowing you to expose your AKS services using a single IP address.

upvoted 4 times

Holii 2 years, 1 month ago

Answer D. is an Azure Basic Load Balancer...not an Azure Gateway Load Balancer.

Besides, the question is already suggesting deploying the AKS Ingress Controller, which achieves the same functionality.

This is A.

upvoted 3 times

zone9gardening 2 years ago

Which (D) are u referring to? there is no option for Azure Application Gateway!

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/aks/ingress-basic

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. Kubernetes ingress resources are used to configure the ingress rules and routes for individual Kubernetes services. When you use an ingress controller and ingress rules, a single IP address can be used to route traffic to multiple services in a Kubernetes cluster.

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: A

A. No adjustment required.

upvoted 3 times

salmantarik 2 years, 6 months ago

A is correct answer. However, to further explain, there are 2 components at AKS cluster which may be deployed.

Azure CNI (Ly 3 - 4): The AKS cluster is connected to existing virtual network resources and configurations.

Pods get full virtual network connectivity and can be directly reached via their private IP address from connected networks.

Requires more IP address space.

Ingress Controller Reverse Proxy

Application Gateway Ingress Controller : (Ly 7) : leverage Azure's native Application Gateway L7 load-balancer to expose cloud software to the Internet.

upvoted 2 times

vasile_fetcu 2 years, 6 months ago

Selected Answer: A

Correct answer

upvoted 3 times

somenick 2 years, 9 months ago

Selected Answer: A

Correct! Azure Ingress Controller is used to establish a reverse proxy

upvoted 4 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 3 times

Question #27 *Topic 1*

You want to gather logs from a large number of Windows Server 2016 computers using Azure Log Analytics.
You are configuring an Azure Resource Manager template to deploy the Microsoft Monitoring Agent to all the servers automatically.
Which of the following should be included in the template? (Choose all that apply.)

A. WorkspaceID

B. AzureADApplicationID

C. WorkspaceKey

D. StorageAccountKey

Suggested Answer: *AC*
Reference:
https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/

Community vote distribution
AC (100%)

Rume Highly Voted 4 years ago
repeat question - however, answer is correct
upvoted 14 times

blazefather Highly Voted 2 years, 7 months ago
In exam 31/10/2022
upvoted 6 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: AC
Answer:
1. A, WorkspaceID
2. C, WorkspaceKey

Reason: When deploying the Microsoft Monitoring Agent to connect servers to Azure Log Analytics, you need to provide the WorkspaceID and WorkspaceKey. These credentials allow the agent to authenticate and send data to the correct Log Analytics workspace. The AzureADApplicationID and StorageAccountKey are not required for this specific scenario.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agent-windows#install-agent-using-setup-wizard
upvoted 1 times

schpeter_091 7 months, 3 weeks ago
OMG, so outdated, RIP MMA :)
upvoted 1 times

schpeter_091 8 months, 1 week ago
MMA is just a lovely memory by now:)
upvoted 1 times

Ruffyit 8 months, 2 weeks ago
It should also be noted that with Azure Monitor Agent (AMA) that the WorkspaceID and Key are not valid options. This fact should make this question invalid for the test.
upvoted 1 times

SrWalk49 9 months ago
Agent is no longer used. Replaced by AMA.
upvoted 2 times

TinyTrexArmz 8 months, 3 weeks ago
It should also be noted that with Azure Monitor Agent (AMA) that the WorkspaceID and Key are not valid options. This fact should make this question invalid for the test.
upvoted 1 times

Rjaesh 1 year, 2 months ago

A & C

```
type: 'MicrosoftMonitoringAgent'
typeHandlerVersion: '1.0'
autoUpgradeMinorVersion: true
settings: {
workspaceId: workspaceId
}
protectedSettings: {
workspaceKey: workspaceKey
```

upvoted 1 times

brooklyn510 1 year, 5 months ago

On exam 1/2/24

upvoted 6 times

ESAJRR 1 year, 10 months ago

Selected Answer: AC

A. WorkspaceID

C. WorkspaceKey

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/services-hub/health/mma-setup#download-and-install-the-microsoft-monitoring-agent-setup-file

On the Overview, Settings Dashboard page, select Connected Sources, and then copy and paste the Workspace ID and Workspace Key (Primary Key) from the log analytics portal.

upvoted 3 times

majstor86 2 years, 4 months ago

Selected Answer: AC

A. WorkspaceID

C. WorkspaceKey

upvoted 2 times

Nerd101 3 years, 2 months ago

The answers are correct. In exam 04/23/2022. 2 Case studies and 48 questions (multiple choice).

upvoted 4 times

Eltooth 3 years, 3 months ago

Selected Answer: AC

A and C are correct.

upvoted 2 times

vecajif5812k 3 years, 4 months ago

in the exam 01/03/22

upvoted 3 times

Payday123 3 years, 4 months ago

Selected Answer: AC

Correct

upvoted 1 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 2 times

Question #28 *Topic 1*

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

Your company has Azure subscription linked to their Azure Active Directory (Azure AD) tenant.

As a Global administrator for the tenant, part of your responsibilities involves managing Azure Security Center settings.

You are currently preparing to create a custom sensitivity label.

Solution: You start by altering the pricing tier of the Security Center.

Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

salmantarik Highly Voted 3 years, 8 months ago

Here is the documentation for this question.

1- Create Sensitive Info type

2- Create Pattern

3- Choose Confidence level

4- Choose and define primary elements

5- Value for char prox

6- Choose recommend confidence level

7 - Submit

upvoted 39 times

Irishtk Highly Voted 3 years, 2 months ago

Technology in this question has been obsolete by newer products.

Some pricing changes to Microsoft Defender for Cloud(formerly Azure Security Center). "Purchase of a Microsoft Purview account is required to apply data sensitivity classifications and run the scans."

https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection

upvoted 16 times

koreshio 2 years, 8 months ago

also this does not seem included in the exam topics anymore

ref: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VC70

https://learn.microsoft.com/en-us/certifications/exams/az-500

upvoted 3 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: B

Answer: B, No

Reason: Altering the pricing tier of Security Center is not related to creating custom sensitivity labels. Sensitivity labels are part of Microsoft Information Protection, not Azure Security Center.

Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

upvoted 1 times

schpeter_091 7 months, 3 weeks ago

This is what you should do before creating a sensitivity label:

"To make sure you have permissions to create and manage sensitivity labels, see Permissions required to create and manage sensitivity labels"

Depending on the portal you're using, navigate to one of the following locations:

+Sign in to the Microsoft Purview portal > Information Protection card > Sensitivity labels.

If the Information Protection solution card isn't displayed, select View all solutions and then select Information Protection from the Data Security section.

+Sign in to the Microsoft Purview compliance portal > Solutions > Information protection > Labels

On the Labels page, select + Create a label to start the new sensitivity label configuration.

upvoted 1 times

⊟ **Ruffyit** 8 months, 2 weeks ago

Here is the documentation for this question.

1- Create Sensitive Info type

2- Create Pattern

3- Choose Confidence level

4- Choose and define primary elements

5- Value for char prox

6- Choose recommend confidence level

7 - Submit

upvoted 1 times

⊟ **pentium75** 11 months ago

Selected Answer: B

"Security Center" is not a product anymore (it would be Defender for Cloud or Purview). But it does not seem that custom labels would require a special tier.

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels

First, create and configure the sensitivity labels that you want to make available for apps and other services. For example, the labels you want users to see and apply from Office apps.

upvoted 2 times

⊟ **majstor86** 2 years, 4 months ago

Selected Answer: B

B. No is correct answer

upvoted 3 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: B

No is correct answer

upvoted 2 times

⊟ **rohitmedi** 3 years, 7 months ago

correct answer

upvoted 4 times

⊟ **PBA1211** 3 years, 7 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide

upvoted 3 times

⊟ **trevax** 3 years, 10 months ago

No - First you have to create a custom sensitive information type.

upvoted 14 times

> ⊟ **AmitDeorukhkar** 3 years, 8 months ago
>
> Hello Trevax, Do you mind sharing documentation please.
>
> upvoted 2 times

Question #29 *Topic 1*

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

Your company has Azure subscription linked to their Azure Active Directory (Azure AD) tenant.

As a Global administrator for the tenant, part of your responsibilities involves managing Azure Security Center settings.

You are currently preparing to create a custom sensitivity label.

Solution: You start by integrating Security Center and Microsoft Cloud App Security.

Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

Shahrezza Highly Voted 3 years, 8 months ago

Given answer is correct. Must create Custom Information type first for description of the sensitive Label

upvoted 7 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: B

Answer: B, No

Reason: Integrating Security Center and Microsoft Cloud App Security is not directly related to creating custom sensitivity labels.

Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

upvoted 1 times

Ruffyit 8 months, 2 weeks ago

Microsoft Cloud App Security is now called Microsoft Defender for Cloud Apps

Answer B - First step is to connect Defender for Cloud Apps to Azure via the Connected Apps page.

https://docs.microsoft.com/en-us/defender-cloud-apps/connect-azure

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration#how-it-works

upvoted 2 times

Irishtk 3 years, 2 months ago

Microsoft Cloud App Security is now called Microsoft Defender for Cloud Apps

Answer B - First step is to connect Defender for Cloud Apps to Azure via the Connected Apps page.

https://docs.microsoft.com/en-us/defender-cloud-apps/connect-azure

upvoted 1 times

Eltooth 3 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

rc05 3 years, 3 months ago

Answer Is Correct

Microsoft Cloud App Security is now called Microsoft Defender for Cloud Apps

https://docs.microsoft.com/en-us/defender-cloud-apps/connect-azure

Before you create the Sensitive Info Type, you need to connect Security Center to MS Defender for Cloud Apps.

Process that Salmantarik has on Q28 is correct.

upvoted 1 times

⊟ **Holii** 2 years, 1 month ago

? What you said is basically "Answer B is correct, but here's the reason as to why A is correct"

upvoted 1 times

⊟ **Holii** 2 years, 1 month ago

To follow this, you do not need to connect Security Center or enable MDCA prior to creating a custom Sensitive Information Type. This can be done by the Microsoft Purview portal today, and could have before been done via the AIP portal (legacy).

Therefore, it's still B...because this technology is redundant in the process of creating a SIT.

upvoted 4 times

⊟ **rohitmedi** 3 years, 7 months ago

correct answer

upvoted 2 times

⊟ **salmantarik** 3 years, 8 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide

upvoted 2 times

Question #30 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has Azure subscription linked to their Azure Active Directory (Azure AD) tenant.
As a Global administrator for the tenant, part of your responsibilities involves managing Azure Security Center settings.
You are currently preparing to create a custom sensitivity label.
Solution: You start by creating a custom sensitive information type.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

Community vote distribution

A (100%)

cosine Highly Voted 3 years, 9 months ago
Correct. This can be achieved by using MS AIP.
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection
upvoted 8 times

STC007 1 year, 9 months ago
this link is insteresting to read too: https://learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels
upvoted 1 times

adamsca 3 years, 7 months ago
I get the answer is correct but I am confused as to what MS AIP has to do with managing Azure Security Center settings. I find this question misleading, unless I am missing the connection.
upvoted 5 times

InnaB 3 years, 6 months ago
Not even sure why sensitive info type is the correct answer, given that the question is only asking about a label. Custom labels can be created without being associated to a sensitive info type...
upvoted 2 times

wooyourdaddy 3 years, 6 months ago
create Custom Information type first for description of the sensitive Label.
upvoted 2 times

AZ5002023 1 year, 7 months ago
exact ...
upvoted 1 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: A
Answer: A, Yes

Reason: Creating a custom sensitive information type is a step in the right direction for creating a custom sensitivity label. Custom sensitive information types can be used as conditions in sensitivity labels, allowing for more precise control over data classification and protection.

Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide
upvoted 2 times

derf225 8 months ago
1- Create Sensitive Info type
2- Create Pattern
3- Choose Confidence level

4- Choose and define primary elements

5- Value for char prox

6- Choose recommend confidence level

7 - Submit

upvoted 3 times

⊟ **Ruffyit** 8 months, 2 weeks ago

Correct. This can be achieved by using MS AIP.

https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

upvoted 1 times

⊟ **brooklyn510** 1 year, 5 months ago

On exam 1/2/24

upvoted 2 times

⊟ **wardy1983** 1 year, 7 months ago

Answer: A

Explanation:

create Custom Information type first for description of the sensitive Label. Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information- type

upvoted 1 times

⊟ **KyDD** 1 year, 9 months ago

Seems like it would be a M365 Security Center.

upvoted 2 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: A

A. Yes

upvoted 3 times

⊟ **Irishtk** 3 years, 2 months ago

Ans A is correct

upvoted 1 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 2 times

⊟ **AS179** 3 years, 6 months ago

A is correct

upvoted 1 times

⊟ **wooyourdaddy** 3 years, 6 months ago

Answer A is correct: create Custom Information type first for description of the sensitive Label.

upvoted 1 times

⊟ **rohitmedi** 3 years, 7 months ago

correct answer

upvoted 1 times

⊟ **dumdada** 3 years, 10 months ago

sounds legit

upvoted 4 times

⊟ **Lobe** 3 years, 11 months ago

Answer is correct

upvoted 4 times

Question #31 *Topic 1*

You have a sneaking suspicion that there are users trying to sign in to resources which are inaccessible to them.
You decide to create an Azure Log Analytics query to confirm your suspicions. The query will detect unsuccessful user sign-in attempts from the last few days.
You want to make sure that the results only show users who had failed to sign-in more than five times.
Which of the following should be included in your query?

A. The EventID and CountIf() parameters.

B. The ActivityID and CountIf() parameters.

C. The EventID and Count() parameters.

D. The ActivityID and Count() parameters.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

Community vote distribution

C (79%) A (21%)

⊟ **Ram9533** Highly Voted 👍 3 years, 8 months ago

```
-- KUSTO Query

let timeframe = 1d;
SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1
```

upvoted 41 times

⊟ **xRiot007** 11 months, 2 weeks ago

You don't need this part "latest_failed_login=arg_max(TimeGenerated, Account)". It is not important when the last login occurred, you already have a filter that will retrieve everything newer than the timeframe. Regarding timeframe, if you define, you should also use it like this "| where TimeGenerated > ago(timeframe)"

upvoted 1 times

⊟ **Rume** Highly Voted 👍 4 years ago

too many repeat questions -
Answer is correct.

upvoted 7 times

⊟ **kakakayayaya** 3 years, 10 months ago

Slightly different, note count and countIF

upvoted 3 times

⊟ **stonwall12** Most Recent ⏱ 4 months, 2 weeks ago

Selected Answer: C

Answer: C, The EventID and Count() parameters.

Reason: To detect unsuccessful sign-in attempts, you need to use the EventID parameter to filter for failed sign-in events. The Count() function is used to aggregate and count these events per user. By using these together, you can identify users with more than five failed sign-in attempts, meeting the requirement of the query.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/query-language

upvoted 4 times

⊟ **Ruffyit** 8 months ago

You don't need this part "latest_failed_login=arg_max(TimeGenerated, Account)". It is not important when the last login occurred, you already have a filter that will retrieve everything newer than the timeframe. Regarding timeframe, if you define, you should also use it like this "| where TimeGenerated > ago(timeframe)"

upvoted 1 times

pentium75 11 months ago

Selected Answer: C

I was tricked because the question doesn't say it would be about on-premises AD logins. Entra ID signins have neither ActivityID not EventID column.

upvoted 1 times

DLR 1 year, 3 months ago

the answer is A as the question is asking only to show users who failed to sign in at least 5 times.

upvoted 1 times

Srihari0908 1 year, 5 months ago

Selected Answer: C

In Azure Log Analytics, you typically use the Kusto Query Language (KQL) to analyze and query data. When you want to detect unsuccessful user sign-in attempts and ensure that the results only show users who had failed to sign in more than five times, you need to count the occurrences of failed sign-ins per user and then filter the results based on that count.

For sign-in logs, the relevant information is usually stored in fields like EventID (which identifies the type of event) and UserPrincipalName (or a similar field that identifies the user). The actual names of these fields can vary depending on how the data is structured in your specific Azure Log Analytics workspace.

Option C, "The EventID and Count() parameters," is the closest to what you need, but it's important to use the correct KQL syntax and structure the query properly. Here's how you can structure the query:

upvoted 3 times

wardy1983 1 year, 7 months ago

Answer: C

Explanation:

KUSTO Query

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1
```

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

upvoted 1 times

ESAJRR 1 year, 9 months ago

Selected Answer: C

C. The EventID and Count() parameters.

upvoted 1 times

ArchitectX 1 year, 9 months ago

Selected Answer: C

C is the right answer

upvoted 3 times

ESAJRR 1 year, 11 months ago

Selected Answer: C

C. The EventID and Count() parameters.

upvoted 2 times

Andre369 2 years, 1 month ago

Selected Answer: A

To create an Azure Log Analytics query that detects unsuccessful user sign-in attempts and filters for users who failed to sign in more than five times, you would need to include the EventID and CountIf() parameters in your query.

The EventID parameter helps identify the sign-in events, typically represented by specific event IDs in the logs.

The CountIf() parameter allows you to specify a condition to count the occurrences that meet that condition. In this case, you would set the condition to count the unsuccessful sign-in attempts.

Therefore, the correct answer is:

A. The EventID and CountIf() parameters.

upvoted 5 times

MaryamNesa 2 years, 2 months ago

Answer A is correct.

The count() function and countif() function are both used in Azure Log Analytics queries to count the number of records that match a certain condition. However, they differ in the way they apply the condition.

The count() function simply counts all records in a given table, without applying any conditions. For example, count(*) would count all records in a table.

The countif() function, on the other hand, applies a condition to the count operation. It counts the number of records that match a specific condition, specified using a Boolean expression. For example, countif(Severity == 'Error') would count the number of records where the severity is 'Error'.

In summary, the count() function counts all records, while the countif() function counts only the records that match a specified condition.

upvoted 2 times

justjeroen 2 years, 2 months ago

Can I do something like countif(EventID == 4625) ?

upvoted 3 times

jaanya 2 years, 2 months ago

SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(2d)
| summarize count() by AccountName
| where count_ > 5

upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: C

C. The EventID and Count() parameters.

upvoted 2 times

salmantarik 2 years, 6 months ago

Correct answer. CountIf returns True of False and can used at a column. Count returns the number of records.

upvoted 3 times

Irishtk 3 years, 2 months ago

Ans is C. Example of the Kusto query at:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/failed-login-report-using-log-analytics-and-logic-apps/ba-p/745025

upvoted 5 times

AzureAdventure 1 year, 11 months ago

Thanks

upvoted 1 times

Question #32 *Topic 1*

Your company uses Azure DevOps with branch policies configured.
Which of the following is TRUE with regards to branch policies? (Choose all that apply.)

A. It enforces your team's change management standards.

B. It controls who can read and update the code in a branch.

C. It enforces your team's code quality.

D. It places a branch into a read-only state.

Suggested Answer: *AC*
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts

Community vote distribution

AC (100%)

Lobe Highly Voted 2 years, 11 months ago
correct answer.
DevOps question though
upvoted 15 times

omw2wealth Highly Voted 2 years, 6 months ago
Hey devops, i'm coming after clearin this one!
upvoted 14 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: AC
Answer:
1. A, It enforces your team's change management standards.
2. C, It enforces your team's code quality.

Reason: Branch policies in Azure DevOps are designed to enforce team standards for change management and code quality.

Reference: https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies-overview?view=azure-devops
upvoted 1 times

trashbox 8 months, 3 weeks ago
Selected Answer: AC
A & C.

"Policies enforce your team's code quality and change management standards"
https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&tabs=browser
upvoted 1 times

ArchitectX 9 months, 2 weeks ago
Selected Answer: AC
A. It enforces your team's change management standards.
C. It enforces your team's code quality.
upvoted 2 times

TheProfessor 9 months, 3 weeks ago
Selected Answer: AC
The answer is: A & C
upvoted 1 times

ESAJRR 11 months, 4 weeks ago

Selected Answer: AC

A. It enforces your team's change management standards.

C. It enforces your team's code quality.

upvoted 2 times

Andre369 1 year, 1 month ago

Selected Answer: AC

A. It enforces your team's change management standards.

C. It enforces your team's code quality.

Branch policies in Azure DevOps are used to enforce certain rules and standards on code branches within a repository. They help maintain code quality, ensure proper change management, and enforce best practices.

upvoted 2 times

zellck 1 year, 1 month ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

upvoted 2 times

majstor86 1 year, 4 months ago

Selected Answer: AC

A. It enforces your team's change management standards.

C. It enforces your team's code quality.

upvoted 3 times

danlo 1 year, 6 months ago

Not in the skills measured
https://learn.microsoft.com/en-us/certifications/exams/az-500

upvoted 3 times

ramujamu 2 years, 2 months ago

Didn't expect a DevOps question

upvoted 4 times

Eltooth 2 years, 3 months ago

Selected Answer: AC

A and C are correct.

https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&tabs=browser

upvoted 4 times

bur88 2 years, 3 months ago

A,C - Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&tabs=browser

upvoted 3 times

Siwel72 2 years, 5 months ago

Is this really in AZ-500, DevOps?

upvoted 3 times

rohitmedi 2 years, 7 months ago

correct answer

upvoted 1 times

Question #33 *Topic 1*

After creating a new Azure subscription, you are tasked with making sure that custom alert rules can be created in Azure Security Center.
You have created an Azure Storage account.
Which of the following is the action you should take?

A. You should make sure that Azure Active Directory (Azure AD) Identity Protection is removed.

B. You should create a DLP policy.

C. You should create an Azure Log Analytics workspace.

D. You should make sure that Security Center has the necessary tier configured.

Suggested Answer: *C*
C: You need write permission in the workspace that you select to store your custom alert.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

Community vote distribution

C (68%) D (32%)

⊟ **amitdimpy** Highly Voted 2 years, 5 months ago

Question was in 8-Jan-2023 exam.

upvoted 15 times

⊟ **Andre369** Highly Voted 2 years, 1 month ago

Selected Answer: C

C. You should create an Azure Log Analytics workspace.

Azure Security Center leverages Azure Log Analytics to store and analyze security-related data and generate alerts. By creating an Azure Log Analytics workspace, you provide the necessary storage and analysis capabilities for Security Center to generate and manage custom alert rules.

Option A, removing Azure Active Directory (Azure AD) Identity Protection, is unrelated to enabling the creation of custom alert rules in Security Center.

Option B, creating a Data Loss Prevention (DLP) policy, is not directly related to enabling custom alert rules in Security Center. DLP policies are used for managing and preventing data loss in various services and applications.

Option D, configuring the necessary tier in Security Center, may impact the availability of certain features and capabilities, but it is not specifically required to enable the creation of custom alert rules.

upvoted 8 times

⊟ **Knighthell** Most Recent 3 weeks, 2 days ago

Selected Answer: C

Enhanced Security (Standard) You must enable the Microsoft Defender plan

upvoted 1 times

⊟ **Knighthell** 3 weeks, 2 days ago

Sorry D Answer

upvoted 1 times

⊟ **khamrumunnu** 1 month, 1 week ago

Selected Answer: D

To create custom alert rules in Azure Security Center (now Microsoft Defender for Cloud), you need:
An Azure Log Analytics workspace

This is where the security data and logs (such as alerts, assessments, and recommendations) are collected and stored.

Custom alert rules are built using Kusto Query Language (KQL) against this data.

The correct pricing tier for Microsoft Defender for Cloud

You must enable the Microsoft Defender plan (formerly the Standard tier) on the subscription or resource level.

This enables advanced features like:

Custom alert rules

Threat detection

Security recommendations

upvoted 2 times

mmmyo 1 month, 3 weeks ago

Selected Answer: C

Azure Security Center relies on Azure Log Analytics to collect and analyze security data. To enable custom alert rules, you need a Log Analytics workspace where Security Center can store and process security events. This allows you to define and configure alerts based on security insights, queries, and threat detection patterns.

Analysis of Other Options:
A (Remove Azure AD Identity Protection) ✖ Incorrect

Azure AD Identity Protection enhances security; removing it has no relevance to enabling custom alerts in Security Center.

B (Create a DLP policy) ✖ Incorrect

Data Loss Prevention (DLP) policies are used in Microsoft Purview and do not directly impact custom alert rules in Security Center.

D (Configure the necessary Security Center tier) ✅ Relevant but secondary

Standard tier of Security Center offers advanced threat protection and custom alert rules, but the first step for alerts is ensuring Log Analytics is set up.

upvoted 1 times

stonwall12 4 months, 2 weeks ago

Selected Answer: D

--Questions looks to be outdated--
Azure Security Center has been rebranded as Microsoft Defender for Cloud, and some features and terminology have changed.

Answer: D, You should make sure that Microsoft Defender for Cloud has the necessary plan enabled.

Reason: To create custom alert rules in Microsoft Defender for Cloud (formerly Azure Security Center), you need to have the appropriate Microsoft Defender plan enabled for the resources you want to monitor. Custom alert rules are part of the advanced threat detection capabilities provided by these plans. Simply creating a storage account or Log Analytics workspace is not sufficient to enable this functionality.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/custom-alert-rules

upvoted 4 times

Jimmy500 11 months, 1 week ago

For today answer is as below:
I think this question now looks like an outdated questions, because now we do not have custom Alert rules in Defender for Cloud we can create it from Azure Monitor but those would be metrics, logs, activity logs, resource health or service health. We can create Security Alerts from Defender for Cloud as of today , this will generate alert regarding to Workloads , such as virtual machines ,storage accounts, container registry and other workloads that can be protected by defender for cloud. This question can come exam like this , if they ask what do we need to create Custom Alerts we need log analytics workspace , if it asks what do we need first to create Security Alerts then we need to upgrade the plan of Defender of Cloud.

upvoted 6 times

Tognan 1 year, 3 months ago

Selected Answer: D

The correct action you should take to ensure custom alert rules can be created in Azure Security Center is:

D. You should make sure that Security Center has the necessary tier configured.

Here's why:

Free tier limitations: The free tier of Azure Security Center may not support creating custom alert rules. These rules allow for more granular security monitoring based on your specific needs.
Paid tiers: Upgrading Security Center to a paid tier (such as Standard or Premium) typically unlocks features like custom alert rule creation.
upvoted 3 times

Tognan 1 year, 3 months ago
The correct action you should take to ensure custom alert rules can be created in Azure Security Center is:

D. You should make sure that Security Center has the necessary tier configured.

Here's why:

Free tier limitations: The free tier of Azure Security Center may not support creating custom alert rules. These rules allow for more granular security monitoring based on your specific needs.
Paid tiers: Upgrading Security Center to a paid tier (such as Standard or Premium) typically unlocks features like custom alert rule creation.
upvoted 2 times

JunetGoyal 1 year, 8 months ago
its D, not C
upvoted 1 times

wardy1983 1 year, 8 months ago
why is it D?
upvoted 2 times

ESAJRR 1 year, 11 months ago
Selected Answer: C
C. You should create an Azure Log Analytics workspace.
upvoted 2 times

Dev1079 2 years ago
Selected Answer: C
https://learn.microsoft.com/en-us/answers/questions/1085512/azure-security-center-custom-rules?orderby=oldest
upvoted 2 times

Cock 2 years, 1 month ago
Selected Answer: D
The answer is D. Similar questions appeared before
upvoted 1 times

AlexPenev95 2 years, 1 month ago
Selected Answer: D
D seems legit to me
upvoted 1 times

majstor86 2 years, 4 months ago
Selected Answer: C
C. You should create an Azure Log Analytics workspace. Most Voted
upvoted 2 times

DESHAINEMARI 2 years, 4 months ago
D. You should make sure that Security Center has the necessary tier configured.

To create custom alert rules in Azure Security Center, you need to have the appropriate tier of Security Center enabled. The Standard tier and the Free tier of Security Center support creating custom alert rules, while the Basic tier does not.

Therefore, after creating a new Azure subscription, you should make sure that Security Center has the necessary tier configured, either Standard or Free, to enable the creation of custom alert rules. Creating an Azure Storage account, creating a DLP policy, or creating an Azure Log Analytics workspace are not directly related to enabling the creation of custom alert rules in Azure Security Center.
upvoted 3 times

azlearner001 2 years, 4 months ago

Answer should be D.

https://woivre.com/blog/2021/12/improve-your-microsoft-defender-for-cloud-with-your-custom-rules

upvoted 2 times

Question #34 *Topic 1*

Your company's Azure subscription includes an Azure Log Analytics workspace.

Your company has a hundred on-premises servers that run either Windows Server 2012 R2 or Windows Server 2016, and is linked to the Azure Log Analytics workspace. The Azure Log Analytics workspace is set up to gather performance counters associated with security from these linked servers.

You have been tasked with configuring alerts according to the information gathered by the Azure Log Analytics workspace.

You have to make sure that alert rules allow for dimensions, and that alert creation time should be kept to a minimum. Furthermore, a single alert notification must be created when the alert is created and when the alert is sorted out.

You need to make use of the necessary signal type when creating the alert rules.

Which of the following is the option you should use?

A. You should make use of the Activity log signal type.

B. You should make use of the Application Log signal type.

C. You should make use of the Metric signal type.

D. You should make use of the Audit Log signal type.

Suggested Answer: *C*

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

Community vote distribution

C (100%)

salmantarik Highly Voted 3 years, 9 months ago

Correct

There are four signal type : Metric, Activity log, Application Insights, and Log.

Guys always read the question properly and look for the key words. The key word in the question is "gather PERFORMANCE COUNTERS", the performance counter directly linked to the Metric signal type.

upvoted 61 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: C

Answer: C, You should make use of the Metric signal type.

Reason: The Metric signal type is ideal for this scenario because it allows for dimensions, enables quick alert creation, and supports single alert notifications for both alert creation and resolution.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-types#metric-alerts

upvoted 1 times

Ruffyit 8 months ago

Correct

There are four signal type : Metric, Activity log, Application Insights, and Log.

Guys always read the question properly and look for the key words. The key word in the question is "gather PERFORMANCE COUNTERS", the performance counter directly linked to the Metric signal type.

upvoted 1 times

trashbox 1 year, 8 months ago

Selected Answer: C

Infrastructure data that can be collected by Performance Counter are called Metrics. Therefore, it is a Metrics Signal Type.

upvoted 1 times

ESAJRR 1 year, 11 months ago

Selected Answer: C

C. You should make use of the Metric signal type.

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: C

The Metric signal type in Azure Log Analytics allows you to create alert rules based on performance counters and metrics collected from the linked servers. By configuring alerts using the Metric signal type, you can leverage dimensions to define specific conditions and thresholds for generating alerts. This enables you to fine-tune the alert rules based on different attributes or properties associated with the collected metrics.

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-types#metric-alerts

Metric alert rules include these features:

- You can use multiple conditions on an alert rule for a single resource.
- You can add granularity by monitoring multiple metric dimensions.
- You can use dynamic thresholds, which are driven by machine learning.
- You can configure if metric alerts are stateful or stateless. Metric alerts are stateful by default.

upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: C

C. You should make use of the Metric signal type.

upvoted 2 times

sofieejo 2 years, 5 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 1 times

blazefather 2 years, 7 months ago

In exam 31/10/2022

upvoted 1 times

somenick 2 years, 9 months ago

Confusing question. Windows Performance Counters provide a high-level abstraction layer that provides a consistent interface for collecting various kinds of system data such as CPU, memory, and disk usage. Which of those metrics are security???

upvoted 1 times

arseyam 2 years, 8 months ago

Exactly, performance counters are not related to security!

upvoted 1 times

xRiot007 11 months, 2 weeks ago

They are, Microsoft Sentinel uses metrics data and combines them with other security events using correlation.

upvoted 1 times

fonte 2 years, 6 months ago

Unusual CPU or Memory usage could be an indicator of something wrong. If you usually have the CPU at 50% and now you see it at 75% or 80% what is causing that spike? Is it a process?! What is that process doing? You see that is sending data to somewhere... boom, you've got yourself a compromised scenario.

Now, of course ideally you should have picked up that process long before detecting it by looking at the CPU, but it can happen.

upvoted 2 times

Irishtk 3 years, 2 months ago

Ans is C.

"Newer metric alerts support alerting for metrics that use dimensions. You can use dimensions to filter your metric to the right level. All supported metrics along with applicable dimensions can be explored and visualized from Azure Monitor - Metrics Explorer"

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-metric-near-real-time#metrics-and-dimensions-supported

upvoted 4 times

AKYK 3 years, 5 months ago

C is the answer

upvoted 1 times

EzeQ 3 years, 6 months ago

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-metric-logs

upvoted 2 times

sadako 3 years, 7 months ago

Alerts = Metric

upvoted 1 times

Adonist 3 years, 5 months ago

Performance = metric

upvoted 3 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 2 times

maylevi 3 years, 9 months ago

Correct.
from the given article: "In the Manage rules blade, you can view all your alert rules across subscriptions. You can further filter the rules using Resource group, Resource type, and Resource. If you want to see only metric alerts, select Signal type as Metrics."

upvoted 3 times

Question #35 *Topic 1*

Your company's Azure subscription includes a hundred virtual machines that have Azure Diagnostics enabled.
You have been tasked with retrieving the identity of the user that removed a virtual machine fifteen days ago. You have already accessed Azure Monitor.
Which of the following options should you use?

A. Application Log

B. Metrics

C. Activity Log

D. Logs

Suggested Answer: *C*
Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as ג€audit logsג€ or
ג€operational logs,ג€ because they report control-plane events for your subscriptions.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

Community vote distribution

C (100%)

orallony Highly Voted 3 years, 9 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 18 times

SecurityAnalyst Highly Voted 3 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 14 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: C

Answer: C, Activity Log

Reason: The Activity Log in Azure Monitor records all operations performed on resources at the subscription level, including resource creation, modification, and deletion.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log

upvoted 2 times

Ruffyit 8 months ago

The question asks for data 15 days old.
Activity logs are retained by default for 30 days(Basic) and 90 days (Standard), but can be setup with longer retention periods if needed.

upvoted 1 times

MeisAdriano 1 year, 8 months ago

arent Activity logs are kept only for 90 days?

upvoted 1 times

xRiot007 11 months, 2 weeks ago

The question asks for data 15 days old.
Activity logs are retained by default for 30 days(Basic) and 90 days (Standard), but can be setup with longer retention periods if needed.

upvoted 1 times

ArchitectX 1 year, 9 months ago

Selected Answer: C

Activity Log

upvoted 2 times

ESAJRR 1 year, 11 months ago

Selected Answer: C

C. Activity Log

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: C

The Activity Log in Azure Monitor provides a comprehensive record of activities performed on resources within your Azure subscription. It includes information about various operations such as creating, modifying, or deleting resources. By querying the Activity Log, you can search for events related to the removal of a virtual machine and identify the user who performed the action.

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-types#choose-the-right-alert-type

- Activity log alert

Activity logs provide auditing of all actions that occurred on resources. Use activity log alerts to be alerted when a specific event happens to a resource like a restart, a shutdown, or the creation or deletion of a resource. Service Health alerts and Resource Health alerts let you know when there's an issue with one of your services or resources.

upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: C

C. Activity Log

upvoted 1 times

Seelearndo 2 years, 5 months ago

Selected Answer: C

Use the Activity Log, to determine the what, who, and when...taken on the resources in your subscription.
https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/platform-logs-overview

upvoted 2 times

Armored5772 2 years, 9 months ago

Selected Answer: C

CORRECT

upvoted 1 times

CheesyAce101 2 years, 10 months ago

Selected Answer: C

C: Activity Log shows 'management plane' data

upvoted 1 times

Irishtk 3 years, 2 months ago

Activity logs provide " insight into the operations on each Azure resource in the subscription from the outside (the management plane) in addition to updates on Service Health events. Use the Activity Log, to determine the what, who, and when for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. There is a single Activity log for each Azure subscription.
https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/platform-logs-overview

upvoted 2 times

WMG 3 years, 2 months ago

Selected Answer: C

"Activity logs provides insight into the operations that were performed on resources in your subscription."

upvoted 5 times

Eltooth 3 years, 3 months ago

Selected Answer: C

C is correct answer

upvoted 2 times

udmraj 3 years, 4 months ago

Answer is C

upvoted 1 times

Question #36 *Topic 1*

Your company's Azure subscription includes a hundred virtual machines that have Azure Diagnostics enabled.
You have been tasked with analyzing the security events of a Windows Server 2016 virtual machine. You have already accessed Azure Monitor.
Which of the following options should you use?

A. Application Log

B. Metrics

C. Activity Log

D. Logs

Suggested Answer: *D*
Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

Community vote distribution

D (100%)

SecurityAnalyst Highly Voted 3 years, 10 months ago
# IN EXAM - 31/8/2021
upvoted 13 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: D
Answer: D, Logs

Reason: Azure Monitor Logs is the appropriate option for analyzing security events from a Windows Server 2016 virtual machine with Azure Diagnostics enabled.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs
upvoted 2 times

Ruffyit 8 months ago
D is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-types#choose-the-right-alert-type
- Log alert
You can use log alerts to perform advanced logic operations on your data. If the data you want to monitor is available in logs, or requires advanced logic, you can use the robust features of Kusto Query Language (KQL) for data manipulation by using log alerts.
upvoted 1 times

ESAJRR 1 year, 11 months ago
Selected Answer: D
D. Logs
upvoted 2 times

Andre369 2 years, 1 month ago
Selected Answer: D
Azure Monitor Logs allow you to collect and analyze log data from various sources, including Windows Event Logs. By querying the Windows Event Logs, you can access the security events generated by the Windows Server 2016 virtual machine and analyze them for security purposes.
upvoted 2 times

zellck 2 years, 1 month ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-types#choose-the-right-alert-type

- Log alert

You can use log alerts to perform advanced logic operations on your data. If the data you want to monitor is available in logs, or requires advanced logic, you can use the robust features of Kusto Query Language (KQL) for data manipulation by using log alerts.

upvoted 2 times

majstor86 2 years, 4 months ago

Selected Answer: D

D. Logs

upvoted 2 times

badaboom 2 years, 7 months ago

Selected Answer: D

D for sure

upvoted 2 times

Eltooth 3 years, 3 months ago

Selected Answer: D

D is correct answer

upvoted 3 times

udmraj 3 years, 4 months ago

D is the correct Answer

upvoted 1 times

AKYK 3 years, 5 months ago

D is Answer

upvoted 1 times

Incredible99 3 years, 6 months ago

In 12/18/21 exams

upvoted 3 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 1 times

mhzayt 3 years, 7 months ago

Correct answer

upvoted 1 times

Question #37 *Topic 1*

You have been tasked with making sure that you are able to modify the operating system security configurations via Azure Security Center.
To achieve your goal, you need to have the correct pricing tier for Azure Security Center in place.
Which of the following is the pricing tier required?

A. Advanced

B. Premium

C. Standard

D. Free

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

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

ad7399 Highly Voted 3 years, 8 months ago
This question is no longer relevant as the pricing model has changed. It's now offered in two modes: defender on or defender off.
upvoted 51 times

[Removed] 1 year, 10 months ago
good one, on and off
upvoted 1 times

Yiannisthe7th Highly Voted 3 years, 11 months ago
The Standard tier extends the capabilities of the free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The standard tier also adds threat protection capabilities, which use built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more. In addition, standard tier adds vulnerability scanning for your virtual machines.
upvoted 18 times

AdityaGupta Most Recent 3 months, 1 week ago
Selected Answer: A
This is outdated question now. Microsoft is using MS Defender for cloud which much more advance solution than Azure Security Center.

If you want OS-level security changes & enforcement, go for Microsoft Defender for Servers Plan 2.
upvoted 3 times

stonwall12 4 months, 2 weeks ago
--Question is out of date--
Azure Security Center has been rebranded to Microsoft Defender for Cloud, and the pricing tiers have changed.

Answer: Defender plans must be turned ON

Reason: Microsoft Defender for Cloud now operates in two modes: with Defender plans ON or OFF. To modify operating system security configurations, you need to have the relevant Defender plan turned ON for your resources. The "Defender OFF" mode (previously known as Free tier) provides basic security assessments but does not include advanced features like modifying OS security configurations.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
upvoted 1 times

ITFranz 6 months ago
Selected Answer: C
To support the answer:
To modify the operating system security configurations via Azure Security Center, you need the Standard tier (now called Microsoft Defender for Servers Plan 2). This tier provides advanced security features and customization options, including the ability to modify operating system security configurations.

The pricing for Microsoft Defender for Servers Plan 2 is typically around $0.02 per server per hour4. This tier includes:
Advanced threat detection capabilities
Customizable security policies
Ability to modify operating system security configurations
Continuous security assessment and recommendations
Answer = C.
upvoted 1 times

codeunit 8 months, 3 weeks ago
To modify operating system security configurations via Azure Security Center (now known as Microsoft Defender for Cloud), you need to be on the Microsoft Defender for Servers plan. This plan is part of the enhanced security features available in the Defender (formerly known as Standard) tier.

The Free tier of Azure Security Center provides basic security capabilities, but to access advanced features like modifying operating system security configurations, you need the Microsoft Defender tier. This includes access to features such as vulnerability assessments, security baselines, and just-in-time (JIT) VM access, among others.

So, the required pricing tier is the Defender for Servers (within the Microsoft Defender tier).
upvoted 1 times

KRISTINMERIEANN 1 year, 2 months ago
Selected Answer: C
C. Standard
upvoted 1 times

ESAJRR 1 year, 11 months ago
Selected Answer: C
C. Standard
upvoted 2 times

Andre369 2 years, 1 month ago
Selected Answer: B
If the question is still relavent
Premium

Azure Security Center offers different pricing tiers: Free, Standard, and Premium. While the Free and Standard tiers provide basic security capabilities, the Premium tier offers advanced features, including the ability to modify operating system security configurations.
upvoted 3 times

zellck 2 years, 1 month ago
Modifying OS security configurations should be done by Azure Automation State Configuration instead.

https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview
upvoted 1 times

majstor86 2 years, 4 months ago
Selected Answer: C
C. Standard - old question
upvoted 3 times

koreshio 2 years, 8 months ago
now you have 'Defender for Cloud' --> 'Free' tier. and the 'Defender for Cloud' -> 'Enhanced Security Features' which would be the 'Paid' tier.

therefore, this question is now obsolete.
upvoted 9 times

Eltooth 3 years, 3 months ago
No longer valid question.
https://docs.microsoft.com/en-gb/azure/defender-for-cloud/defender-for-cloud-introduction
upvoted 4 times

rohitmedi 3 years, 7 months ago
correct answer
upvoted 1 times

⊟ **Strifelife** 3 years, 8 months ago

I really hate this kind of questions, since you know that there's two tiers for security center one with defender on and other with defender off. I see no point remembering what it's actually called (they are standard and free) but in my mind standard and advanced sound more describing. Sorry I just wanted to rant how annoying some of there questions are.

upvoted 13 times

Question #38 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company's Azure subscription is linked to their Azure Active Directory (Azure AD) tenant.
After an internally developed application is registered in Azure AD, you are tasked with making sure that the application has the ability to access Azure Key Vault secrets on application the users' behalf.
Solution: You configure a delegated permission with admin consent.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

Joshing Highly Voted 👍 3 years, 5 months ago

This question is regarding compound identities (Application-plus-user) and Key Vault Authentication. Compound Identity requires the Principal (User)and Authorised Application to be used for a Key Vault Access Policy. This requires the application to be registered in Azure AD and given permission to read the key vault on behalf of the user (Delegated) a.k.a Impersonation. There is a permission for this under the Azure Key Vault permissions called "user_impersonation" with the description "Allow the application full access to the Azure Key Vault service on behalf of the signed-in user". This is a delegated permission.

Reference - https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#key-vault-authentication-options

upvoted 31 times

ravy_rv 3 years, 2 months ago

Very good explanation. thanks.
Just to clarify the process, to give an application to access secret 'on user behalf'
1- You need to create an app registration
2- In the API permission add 'Azure Key Vault' permission, select 'user_impersonation'
3- Both applicationId and objectId must be specified in the access policy. The applicationId identifies the required application and the objectId identifies the user.

In step 3, currently, this option isn't available for data plane Azure RBAC.

upvoted 7 times

shnz03 3 years, 4 months ago

Excellent explanation and reference. I see this as a similar concept to onprem ADDS compound claims and Kerberos delegation. Thanks

upvoted 1 times

Duncan Highly Voted 👍 3 years, 9 months ago

Must be 'application' type permission instead.

upvoted 10 times

amksa 3 years, 5 months ago

the question states : on application the users' behalf. so delegated permission is correct with no admin consent.

upvoted 15 times

mmmyo Most Recent 🕘 1 month, 3 weeks ago

Selected Answer: A

Delegated permissions allow an application to access resources on behalf of a signed-in user, meaning the app operates with the same permissions as the user using it.

Since Azure Key Vault secret access is a privileged operation, admin consent is required to ensure that users can authorize the application to retrieve secrets.

Once approved, the app can request an OAuth access token for Key Vault using Azure AD authentication, enabling secure access to secrets while maintaining user identity context.

upvoted 1 times

AdityaGupta 3 months, 1 week ago

Selected Answer: B

✖ Delegated Permissions in Azure AD won't work for Key Vault access because Key Vault doesn’t support delegated permissions. Azure Key Vault does not support delegated permissions in Azure AD roles & permissions. Instead, Key Vault uses Azure RBAC or Access Policies.

✅ Instead, use Azure RBAC roles (preferred) or Access Policies to control application access to Key Vault.

upvoted 1 times

Hot_156 4 months ago

Selected Answer: A

Delegated Permissions: These permissions allow an application to act on behalf of a signed-in user. In this case, the application needs to access Key Vault secrets on behalf of the users.

Admin Consent: Granting admin consent allows the application to access the specified resources (Key Vault secrets in this case) on behalf of all users in the organization.

upvoted 1 times

Ruffyit 8 months ago

This question is regarding compound identities (Application-plus-user) and Key Vault Authentication. Compound Identity requires the Principal (User)and Authorised Application to be used for a Key Vault Access Policy. This requires the application to be registered in Azure AD and given permission to read the key vault on behalf of the user (Delegated) a.k.a Impersonation. There is a permission for this under the Azure Key Vault permissions called "user_impersonation" with the description "Allow the application full access to the Azure Key Vault service on behalf of the signed-in user". This is a delegated permission.

upvoted 2 times

Jimmy500 1 year ago

The permission is delegated but not Admin consent required.

upvoted 1 times

ManiMessner 1 year, 7 months ago

Selected Answer: B

NO. answer correct

upvoted 1 times

wardy1983 1 year, 7 months ago

Answer: A

Explanation:

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

upvoted 1 times

Oyoko 1 year, 11 months ago

I believe it is delegated permission since it is on the users behalf. My only confusion is the admin consent part.

upvoted 2 times

> **Jimmy500** 1 year ago
>
> We do not need admin consent for it , but it is delegated answer is no
>
> upvoted 1 times

majstor86 2 years, 4 months ago

Selected Answer: B

B. No is correct answer

upvoted 3 times

amitdimpy 2 years, 5 months ago

Question was in 8-Jan-2023 exam. Cleared the exam successfully.

upvoted 8 times

EM1234 2 years, 7 months ago

This test bank is low quality and needs to be refreshed. A lot of old stuff need removal

upvoted 7 times

cast0r 2 years, 8 months ago

On the official practice test @ MeasureUP - given answer is incorrect - delegated permission is correct

upvoted 1 times

ChrisPinas 2 years, 7 months ago

Can you give the link for the practice test of Measure Up? Is it for free? Thanks

upvoted 1 times

arseyam 2 years, 8 months ago

Selected Answer: B

Answer should be NO because there is only one option when you assign Azure Key Vault permission which is Delegated permission WITHOUT Admin Consent

upvoted 2 times

Irishtk 3 years, 2 months ago

Ans is B

From Key Vault resource, select Access Policies, then add a Policy, then select Secret permissions and Select Principal (Application). "Use Key Vault Access Policies to add a policy for authorized application, service principal. Enable Azure RBAC permissions on existing key vault, then assign role, assign access to the current user. Key Vault access policies grant permissions separately to keys, secrets, or certificate. You can grant a user access only to keys and not to secrets."

https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal
https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#privileged-access

upvoted 1 times

CJ32 3 years, 4 months ago

Delegated permissions is selected by default. Delegated permissions are appropriate for client apps that access a web API as the signed-in user, and whose access should be restricted to the permissions you select in the next step. Leave Delegated permissions selected for this example.

Application permissions are for service- or daemon-type applications that need to access a web API as themselves, without user interaction for sign-in or consent. Unless you've defined application roles for your web API, this option is disabled.

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

upvoted 1 times

Question #39 *Topic 1*

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

Your company's Azure subscription is linked to their Azure Active Directory (Azure AD) tenant.

After an internally developed application is registered in Azure AD, you are tasked with making sure that the application has the ability to access Azure Key Vault secrets on application the users' behalf.

Solution: You configure a delegated permission with no admin consent.

Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

Community vote distribution

A (80%) B (20%)

somenick Highly Voted 1 year, 8 months ago

Selected Answer: A

Just register an Azure AD App then go to API Permissions and select Azure Key Vault, you will find a single permission to add "user_impersonation" under Delegated Permissions and Admin Consent is not required.

You will notice that Application Permissions is dimmed out

upvoted 11 times

amitdimpy Highly Voted 1 year, 5 months ago

Question was in 8-Jan-2023 exam.

upvoted 8 times

gauravwagh16193 Most Recent 2 months, 3 weeks ago

Selected Answer: B

No, the solution does not meet the goal. Configuring a delegated permission with no admin consent is not sufficient for an application to access Azure Key Vault secrets on behalf of users.

To achieve this, you need to configure application permissions and ensure that the application has the necessary Key Vault access policies12. Application permissions allow the app to access resources without user interaction, which is essential for accessing Key Vault secrets.

upvoted 1 times

AdityaGupta 3 months, 1 week ago

Selected Answer: B

Azure Key Vault does not support delegated permissions in Azure AD roles & permissions. Instead, Key Vault uses Azure RBAC or Access Policies.

upvoted 2 times

heyhey12345 4 months, 2 weeks ago

Selected Answer: B

No, the solution does not meet the goal because access to Key Vault secrets requires permissions that typically need admin consent.

upvoted 1 times

ESAJRR 11 months, 4 weeks ago

Selected Answer: A

A. YES. no admin consent.

upvoted 1 times

ESAJRR 11 months, 4 weeks ago

Selected Answer: B

B is the correct answer

upvoted 2 times

Andre369 1 year, 1 month ago

Selected Answer: B

The solution mentioned, which is to configure a delegated permission with no admin consent, does not meet the goal of allowing the application to access Azure Key Vault secrets on behalf of application users.

Delegated permissions are used when an application needs to access APIs on behalf of a user. However, in this case, the requirement is for the application to access Azure Key Vault secrets on behalf of the application users.

To achieve this, you would need to configure the application with the appropriate application permissions and assign those permissions to the application in Azure AD. Delegated permissions alone would not be sufficient, and configuring delegated permissions without admin consent would not provide the necessary access to the application.

upvoted 2 times

majstor86 1 year, 4 months ago

Selected Answer: A

A. YES. no admin consent.

upvoted 3 times

ylfr 1 year, 8 months ago

Selected Answer: A

no admin consent is the clue

upvoted 1 times

Pasapugazh 1 year, 8 months ago

One more question with properly balanced two sets of answers:). As usual not able to find relevant MS docs. Unable to replicate it in my azure lab as well. I will go with option A!!

upvoted 1 times

arseyam 1 year, 8 months ago

Just register an Azure AD App then go to API Permissions and select Azure Key Vault, you will find a single permission to add "user_impersonation" under Delegated Permissions and Admin Consent is not required.
You will notice that Application Permissions is dimmed out

upvoted 1 times

Irishtk 2 years, 2 months ago

Ans is B

upvoted 2 times

Gejlug 2 years, 2 months ago

Selected Answer: A

A.
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent
Delegated permissions are used by apps that have a signed-in user present. For these apps, either the user or an administrator consents to the permissions that the app requests. The app is delegated with the permission to act as a signed-in user when it makes calls to the target resource.

The questions clearly stated as 'on behalf', so it's delegated permissions. Next, do we need admin consent to read secret?, nope, so it's delegated without admin consent

upvoted 5 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

CaioAugusto 2 years, 5 months ago

B. No - I think that this access can be granted using RBAC after configuring Key Vault permission model to "Azure role-based access control".

upvoted 1 times

rohitmedi 2 years, 7 months ago

correct answer

upvoted 3 times

ashxos 2 years, 7 months ago

Selected Answer: B

The correct answer should be "Assign permission to AD Registered application using Access Policy of Key Vault on the Secret"

upvoted 2 times

sadako 2 years, 7 months ago

Answer should be A.

upvoted 1 times

Question #40 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
Your Azure Active Directory Azure (Azure AD) tenant has an Azure subscription linked to it.
Your developer has created a mobile application that obtains Azure AD access tokens using the OAuth 2 implicit grant type.
The mobile application must be registered in Azure AD.
You require a redirect URI from the developer for registration purposes.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required

B. a secret

C. a login hint

D. a client ID

Suggested Answer: *A*
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

Community vote distribution
A (55%) D (42%)

Rume Highly Voted 3 years, 12 months ago
given answer is correct. "No adjustment required"
upvoted 43 times

helpaws 3 years, 5 months ago
https://docs.microsoft.com/en-us/azure/active-directory/develop/reply-url
upvoted 2 times

LDodge Highly Voted 3 years, 6 months ago
Selected Answer: D
As per Microsoft's documentation, a Client ID is REQUIRED, while a Redirect URI is only RECOMMENDED https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-implicit-grant-flow
upvoted 34 times

zellck 2 years, 1 month ago
Client ID is generated when app is registered, not given by developer.

https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#register-an-application
When registration finishes, the Azure portal displays the app registration's Overview pane. You see the Application (client) ID. Also called the client ID, this value uniquely identifies your application in the Microsoft identity platform.
upvoted 9 times

xRiot007 11 months, 2 weeks ago
A client ID is required for access, not for registration.
The problem is at the step where the app needs registering.
The Client ID (or App ID) is what you get after the registration is done.
upvoted 3 times

CaioAugusto 3 years, 3 months ago
At your link the client_id is referred not to register the app, but instead after, to obtain a token from Azure AD. To register an app you just need the redirect uri. Correct response is A - No adjustment required.
upvoted 6 times

Siblark 2 years, 9 months ago
You require a client id for access purposes but need a REDIRECT URI to register an app. Sometimes, you may not enter it during registration, but you must enter it later on.
https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

upvoted 2 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: A

Answer: A, No adjustment required

Reason: The underlined segment is accurate. When registering a mobile application that uses the OAuth 2 implicit grant flow in Azure AD, a redirect URI is indeed required.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-implicit-grant-flow#send-the-sign-in-request

upvoted 2 times

Ruffyit 8 months ago

As per Microsoft's documentation, a Client ID is REQUIRED, while a Redirect URI is only RECOMMENDED https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-implicit-grant-flow

upvoted 1 times

JackGelder 8 months ago

Client ID is generated after you complete the registration. Question clearly says the you require some information from developer. Developer can't provide you client Id

upvoted 1 times

ITFranz 8 months ago

To use the OAuth 2.0 implicit grant type with a mobile application registered in Azure AD, you'll need to follow these key steps:
Register the mobile application in Azure AD:
Sign in to the Azure portal
Navigate to Azure Active Directory
Select "App registrations" and click "New registration"
Provide a name for your application
Select "Public client/native (mobile & desktop)" as the application type
Specify the redirect URI for your mobile app

Answer = A

upvoted 1 times

sudowhoami 10 months, 2 weeks ago

Selected Answer: A

You require a redirect URI from the developer for registration purposes.

Registering a mobile application that uses the OAuth 2.0 implicit grant type in Azure AD, the redirect URI is indeed required for registration. URI is where Azure AD will send the authentication response after the user logs in.

A. No adjustment required

upvoted 2 times

JaridB 1 year, 2 months ago

The underlined segment regarding the requirement for a redirect URI from the developer for Azure AD app registration is accurate. In the context of Azure Active Directory (Azure AD), when registering a mobile application that obtains Azure AD access tokens using the OAuth 2.0 implicit grant type, it is indeed necessary to provide a redirect URI. This redirect URI is where the Microsoft identity platform sends the user after authentication, and it is crucial for the correct operation of the application, as it receives the authentication response from Azure AD at this URI (MS Learn).

Thus, the correct choice based on the information is:
A. No adjustment required

This choice is supported by the official Azure documentation, which explains the importance of specifying a redirect URI during the app registration process. The redirect URI is a fundamental part of setting up authentication flows within Azure AD (MS Learn).

upvoted 3 times

khaled_razouk 1 year, 3 months ago

Selected Answer: A

A
you can do it from the app registration

upvoted 1 times

[Removed] 1 year, 6 months ago

The Redirect URI is where Azure AD will send the user after they have authenticated. This is a security measure to ensure that the authentication response is sent only to the authorized location specified by the application.

upvoted 1 times

wardy1983 1 year, 7 months ago

Answer: D

Explanation:

1. As per Microsoft's documentation, a Client ID is REQUIRED, while a Redirect URI is only RECOMMENDED https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-implicit-grant-flow

2. CLIENT ID

upvoted 1 times

flafernan 1 year, 8 months ago

Selected Answer: A

The client ID is required to register the mobile application with Azure AD and ensure that it can obtain access tokens using the OAuth 2 implicit flow. The "client ID" is a unique identifier for the application in Azure AD.

Redirect URI: This is equally necessary as it defines where the authorization server should redirect the user after authentication is complete. This redirection is essential so that the server knows where to send the access token.

upvoted 1 times

flafernan 1 year, 8 months ago

Selected Answer: D

The client ID is required to register the mobile application with Azure AD and ensure that it can obtain access tokens using the OAuth 2 implicit flow. The "Client ID" is a unique identifier for the application in Azure AD.

URI redirection is also required, but is not in the list of options offered. Therefore, the "D. a customer ID" option is the most accurate answer available.

upvoted 1 times

ArchitectX 1 year, 9 months ago

Selected Answer: D

"No adjustment required"

upvoted 2 times

timHAG 1 year, 11 months ago

Selected Answer: D

agree its d

upvoted 1 times

Ario 1 year, 12 months ago

Selected Answer: D

require a client ID

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: D

When registering a mobile application in Azure AD, you would require a redirect URI for registration purposes. The redirect URI is used to redirect the user back to the application after authentication. However, the redirect URI is not mentioned in the underlined segment.

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#add-a-redirect-uri

A redirect URI is the location where the Microsoft identity platform redirects a user's client and sends security tokens after authentication.

upvoted 1 times

> **Holii** 2 years, 1 month ago
>
> Correct. Redirect URI is optional in the app registration...but nothing is 'required' for entry when registering an application. These values are all generated for you...so not sure what this question is asking.
>
> Redirect uri is optional: https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

upvoted 1 times

Question #41 *Topic 1*

You are in the process of configuring an Azure policy via the Azure portal.
Your policy will include an effect that will need a managed identity for it to be assigned.
Which of the following is the effect in question?

A. AuditIfNotExist

B. Disabled

C. DeployIfNotExist

D. EnforceOPAConstraint

Suggested Answer: *C*
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

Community vote distribution
C (100%)

AKYK Highly Voted 3 years, 9 months ago
correct answer C
upvoted 11 times

SecurityAnalyst Highly Voted 3 years, 10 months ago
# IN EXAM - 31/8/2021
upvoted 10 times

Sabr_ Most Recent 2 months, 3 weeks ago
Selected Answer: C
Exam question 6th April 2025
upvoted 2 times

stonwall12 4 months, 2 weeks ago
Selected Answer: C
Answer: C, DeployIfNotExist

Reason: The DeployIfNotExist effect in Azure Policy requires a managed identity to be assigned when the policy is created.

Reference: https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists
upvoted 2 times

Ruffyit 8 months ago
Correct answer C. DeployIfNotExist
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure
Azure Policy supports the following types of effect:
Append: adds the defined set of fields to the request
Audit: generates a warning event in activity log but doesn't fail the request
AuditIfNotExists: generates a warning event in activity log if a related resource doesn't exist
Deny: generates an event in the activity log and fails the request
DeployIfNotExists: deploys a related resource if it doesn't already exist
Disabled: doesn't evaluate resources for compliance to the policy rule
Modify: adds, updates, or removes the defined set of fields in the request
EnforceOPAConstraint (deprecated): configures the Open Policy Agent admissions controller with Gatekeeper v3 for self-managed Kubernetes clusters on Azure
EnforceRegoPolicy (deprecated): configures the Open Policy Agent admissions controller with Gatekeeper v2 in Azure Kubernetes Service
upvoted 3 times

Jimmy500 1 year ago
2 policy effects needs managed identity. 1 DeployIFNotExist second one is Manage

upvoted 1 times

meeko86 1 year, 10 months ago

Correct answer C. DeployIfNotExist

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy supports the following types of effect:

Append: adds the defined set of fields to the request

Audit: generates a warning event in activity log but doesn't fail the request

AuditIfNotExists: generates a warning event in activity log if a related resource doesn't exist

Deny: generates an event in the activity log and fails the request

DeployIfNotExists: deploys a related resource if it doesn't already exist

Disabled: doesn't evaluate resources for compliance to the policy rule

Modify: adds, updates, or removes the defined set of fields in the request

EnforceOPAConstraint (deprecated): configures the Open Policy Agent admissions controller with Gatekeeper v3 for self-managed Kubernetes clusters on Azure

EnforceRegoPolicy (deprecated): configures the Open Policy Agent admissions controller with Gatekeeper v2 in Azure Kubernetes Service

upvoted 3 times

AzureAdventure 1 year, 11 months ago

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists:~:text=Similar%20to%20AuditIfNotExists%2C%20a%20DeployIfNotExists%20policy%20defir

upvoted 1 times

ESAJRR 1 year, 11 months ago

Selected Answer: C

C. DeployIfNotExist

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: C

The DeployIfNotExist effect in Azure policy allows you to automatically deploy and configure resources if they do not exist. When using this effect, a managed identity is required to perform the necessary deployment actions on behalf of the policy.

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists

Similar to AuditIfNotExists, a DeployIfNotExists policy definition executes a template deployment when the condition is met. Policy assignments with effect set as DeployIfNotExists require a managed identity to do remediation.

upvoted 2 times

ETV 2 years, 2 months ago

Passed exam today some questions were present 24/04/23

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: C

C. DeployIfNotExist

upvoted 2 times

amitdimpy 2 years, 5 months ago

Question was in 8-Jan-2023 exam.

upvoted 2 times

Amit3 2 years, 9 months ago

# In EXAM - 01-Oct-2022

upvoted 2 times

Eltooth 3 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 3 times

Cessyd 3 years, 5 months ago

On today's exam 06/01/22 (question was asked in a slightly different way though)

upvoted 3 times

Question #42 *Topic 1*

You have been tasked with creating an Azure key vault using PowerShell. You have been informed that objects deleted from the key vault must be kept for a set period of 90 days.
Which two of the following parameters must be used in conjunction to meet the requirement? (Choose two.)

A. EnabledForDeployment

B. EnablePurgeProtection

C. EnabledForTemplateDeployment

D. EnableSoftDelete

Suggested Answer: *BD*
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault https://docs.microsoft.com/en-us/azure/key-vault/key-vault-ovw-soft-delete

Community vote distribution

BD (100%)

rawrkadia Highly Voted 3 years, 10 months ago
Correct, but soft-delete is now enabled by default. :)
upvoted 7 times

Rume Highly Voted 4 years ago
repeted question - and the answers are correct
upvoted 7 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: BD
Answer:
1. B, EnablePurgeProtection
2. D, EnableSoftDelete

Reason: To keep deleted objects in an Azure Key Vault for a set period of 90 days, you need to use both EnableSoftDelete and EnablePurgeProtection parameters.
1. EnablePurgeProtection prevents the permanent deletion of these objects before the retention period expires.
2. EnableSoftDelete allows for the recovery of deleted objects within a specified retention period.

Reference: https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview
upvoted 2 times

Ruffyit 8 months ago
Here you have a fantastic video-training in which you'll be able to deeply learn about KeyVault:
upvoted 1 times

STC007 1 year, 9 months ago
Here you have a fantastic video-training in which you'll be able to deeply learn about KeyVault:
https://www.youtube.com/results?search_query=john+savill+key+vault
upvoted 2 times

ArchitectX 1 year, 9 months ago
Selected Answer: BD
B & D are the right answers
upvoted 1 times

ESAJRR 1 year, 12 months ago
Selected Answer: BD
B. EnablePurgeProtection
D. EnableSoftDelete

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: BD

To meet the requirement of keeping deleted objects in the Azure key vault for a set period of 90 days, you need to use the following two parameters together:

B. EnablePurgeProtection: This parameter enables purge protection, which prevents permanent deletion of objects from the key vault. When purge protection is enabled, deleted objects are retained for a specified period and can be recovered within that timeframe.

D. EnableSoftDelete: This parameter enables soft delete functionality for the key vault, which allows for the recovery of deleted objects. Soft deleted objects are retained for a specified retention period, during which they can be restored.

By using both EnablePurgeProtection and EnableSoftDelete parameters in your PowerShell script, you can ensure that deleted objects in the key vault are protected from permanent deletion and kept for the required period of 90 days.

upvoted 4 times

zellck 2 years, 1 month ago

Selected Answer: BD

BD is the asnwer.

https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview
When soft-delete is enabled, resources marked as deleted resources are retained for a specified period (90 days by default). The service further provides a mechanism for recovering the deleted object, essentially undoing the deletion.

upvoted 2 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview#purge-protection
Purge protection is an optional Key Vault behavior and is not enabled by default. Purge protection can only be enabled once soft-delete is enabled. It can be turned on via CLI or PowerShell. Purge protection is recommended when using keys for encryption to prevent data loss. Most Azure services that integrate with Azure Key Vault, such as Storage, require purge protection to prevent data loss.

When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed.

The default retention period is 90 days, but it is possible to set the retention policy interval to a value from 7 to 90 days through the Azure portal. Once the retention policy interval is set and saved it cannot be changed for that vault.

upvoted 3 times

153a793 9 months, 2 weeks ago

In simple terms purge protection option is to protects the "soft delete" state.

upvoted 1 times

exnaniantwort 2 years, 2 months ago

Purge protection is an optional feature of Azure Key Vault which is disabled by default. Purge protection can only be enabled once soft delete is enabled for the key vault. When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed. Please note that the purge protection retention policy uses the same interval as soft delete. Once the period is set, the retention policy interval cannot be changed.

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: BD

B. EnablePurgeProtection
D. EnableSoftDelete

upvoted 2 times

blazefather 2 years, 7 months ago

In exam 31/10/2022

upvoted 2 times

Armored5772 2 years, 9 months ago

Selected Answer: BD

CORRECT

upvoted 2 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: BD

B and D are correct.

upvoted 1 times

⊟ **udmraj** 3 years, 4 months ago

Correct Answer - EnablePurgeProtection an EnableSoftDelete

upvoted 1 times

⊟ **mansc3wth1s** 3 years, 4 months ago

Just note soon SoftDelete will be enabled by DEFAULT in the coming months.

https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

upvoted 1 times

⊟ **subhuman** 3 years, 4 months ago

Correct ,

for EnablePurgeProtection to work self delete has to be enabled

upvoted 1 times

Question #43 *Topic 1*

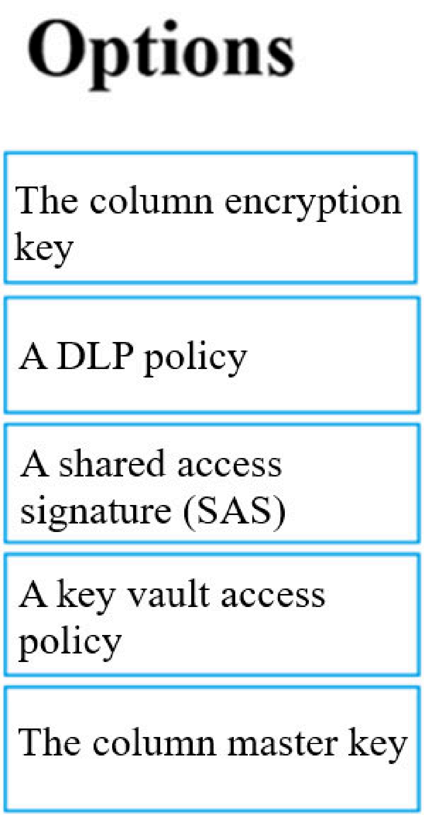
DRAG DROP -

Your company has an Azure SQL database that has Always Encrypted enabled.

You are required to make the relevant information available to application developers to allow them to access data in the database.

Which two of the following options should be made available? Answer by dragging the correct options from the list to the answer area.

Select and Place:



Options

Answer

The column encryption key

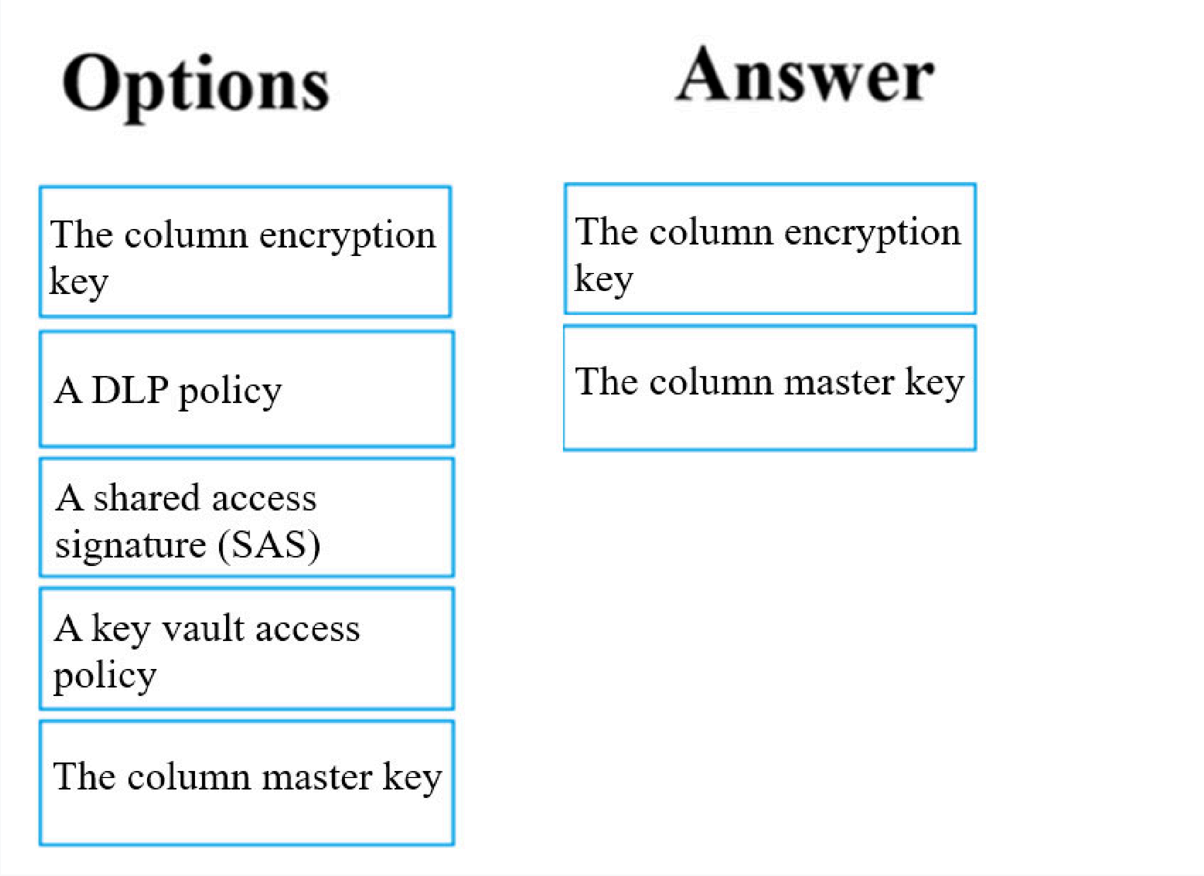
A DLP policy

A shared access signature (SAS)

A key vault access policy

The column master key

Suggested Answer:



Options

Answer

The column encryption key

A DLP policy

A shared access signature (SAS)

A key vault access policy

The column master key

The column encryption key

The column master key

Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
Reference:
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

zellck Highly Voted 👍 2 years, 1 month ago

1. column master key
2. column encryption key

https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/overview-of-key-management-for-always-encrypted
Always Encrypted uses two types of cryptographic keys to protect your data - one key to encrypt your data, and another key to encrypt the key that encrypts your data. The column encryption key encrypts your data, the column master key encrypts the column encryption key.

upvoted 9 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 6 times

majstor86 Highly Voted 👍 2 years, 3 months ago

Column Encryption Key
Column Master Key.

upvoted 6 times

ca7859c Most Recent 🕒 1 month, 1 week ago

1. column master key
2. column encryption key
A column master key is a key-protecting key that encrypts one or more column encryption keys.
A column encryption key is used to encrypt the data within an encrypted column.

upvoted 1 times

stonwall12 4 months, 2 weeks ago

Answer:
1. Column encryption key
2. Column master key

Reason:
1. Column Master Key (CMK): This is the root key used to protect the column encryption keys. It's typically stored in a secure location like Azure Key Vault. Developers need access to this key to be able to decrypt the column encryption keys.
2. Column Encryption Key (CEK): This key is used to encrypt the actual data in the database columns. It's protected by the column master key.

Reference:
https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/overview-of-key-management-for-always-encrypted
https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/overview-of-key-management-for-always-encrypted?view=sql-server-ver16

upvoted 1 times

Ruffyit 8 months ago

1. column master key
2. column encryption key

https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/overview-of-key-management-for-always-encrypted
Always Encrypted uses two types of cryptographic keys to protect your data - one key to encrypt your data, and another key to encrypt the key that encrypts your data. The column encryption key encrypts your data, the column master key encrypts the column encryption key.

upvoted 1 times

Ivan80 1 year, 5 months ago

In exam 1/28/24

upvoted 4 times

MikeScout 1 year, 6 months ago

I do not think that a policy is required as it only needs 'specific permissions'. Please see the following. To access an encrypted column, your application needs to be able to access Azure Key Vault and it also needs specific permissions on the column master key to decrypt the column encryption key protecting the column. To manage keys for Always Encrypted, you need permissions to list and create column master keys in Azure Key Vault, and to perform cryptographic operations using the keys.
https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/create-and-store-column-master-keys-always-encrypted?view=sql-server-ver16

upvoted 2 times

elster 1 year, 8 months ago

The question is which information has to be made available to the application developer. As the column master key is stored in KeyVault, shouldn't the right answer then be 'A key vault access policy' instead of 'column master key', because other than the encryption key the master key will not be handed over directly to the app developer, but the latter has to fetch it from key vault, which will work only with an appropriate key vault access policy.

upvoted 2 times

pentium75 11 months ago

Tricky, but question is "which information has to be made available to the application developer". The "key vault access policy" is NOT something that you 'make available to the developer'. The "key vault access policy" is something that you CREATE, and BY DOING SO you 'make the column master key available to the developer' (= allow him to read it from key vault).

upvoted 1 times

ESAJRR 1 year, 11 months ago

1. column master key
2. column encryption key

upvoted 5 times

Andre369 2 years, 1 month ago

A. The column encryption key: This key is used to encrypt and decrypt the sensitive columns in the database. Application developers will need access to this key to perform encryption and decryption operations.

F. The column master key: This key is used to protect the column encryption keys. It is stored in a trusted key store, such as Azure Key Vault. Application developers will need access to this key to access and manage the column encryption keys.

upvoted 5 times

003nickm 2 years, 4 months ago

On 2-March-2023, I passed AZ-500 with flying colur. This question was in exam. Some question were on Defender EASM as well.

upvoted 4 times

Diallo18 2 years, 8 months ago

In Exam 10/18/2022. One case study, no lab.

upvoted 2 times

Eltooth 3 years, 3 months ago

Answer is correct.

upvoted 1 times

Incredible99 3 years, 6 months ago

Correct answer. In 12/18/21 exams

upvoted 4 times

LDodge 3 years, 6 months ago

Correct- Column Encryption Key and Column Master Key.

upvoted 4 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 1 times

ReadyToLearn 3 years, 8 months ago

Answer is correct

upvoted 4 times

Question #1 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription named Sub1.
You have an Azure Storage account named sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to sa1.
Solution: You create a new stored access policy.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Creating a new (additional) stored access policy with have no effect on the existing policy or the SAS's linked to it.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.
Reference:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

Community vote distribution

B (100%)

JohnCrawford Highly Voted 👍 5 years, 8 months ago
I believe the correct answer to this is "No". You can up to 5 access policies on an object. Creating a new one doesn't revoke the old one. To revoke a stored access policy, you can delete it, rename it by changing the signed identifier, or change the expiry time to a value in the past. Nowhere in the documentation does it say creating a new one revokes the old one.
upvoted 73 times

awssecuritynewbie 4 years, 9 months ago
i agree, it just says create a new policy not " delete" or revoke the existing one that has caused this issue
upvoted 5 times

Globetrotter 3 years, 9 months ago
answer is no here , as creating a new access policy won't cancel existing shared access signature . we just need to update or delete existing access policy for the same.
upvoted 3 times

S_Khan Highly Voted 👍 5 years, 3 months ago
Answer "Yes" is correct. You can find explanation in the article: https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy
"A stored access policy provides an additional level of control over service-level shared access signatures (SAS) on the server side. Establishing a stored access policy serves to group shared access signatures and to provide additional restrictions for signatures that are bound by the policy. You can use a stored access policy to change the start time, expiry time, or permissions for a signature, or to revoke it after it has been issued."
upvoted 21 times

pentium75 11 months ago
Deleting the existing stored access policy would help, but just creating a new (additional) one does not.
upvoted 1 times

bxlin 1 year, 1 month ago
stored access policy is only available for blob not for file share. hence No.
upvoted 1 times

obaali1990 2 years, 2 months ago

Your explanation is not accurate. It doesnt explain the question. The answer to the question is NO

upvoted 2 times

peacegrace 4 years, 2 months ago

NO . Becaz .....Creating a new (additional) stored access policy with have no effect on the existing policy or the SASג€™s linked to it.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

upvoted 9 times

gchristina 4 years, 2 months ago

I agree:
https://docs.microsoft.com/en-us/rest/api/storageservices/create-user-delegation-sas#revoke-a-user-delegation-sas
https://docs.microsoft.com/en-us/rest/api/storageservices/create-service-sas#revocation-of-a-sas

upvoted 2 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: B

Answer: B, No

Reason: Creating a new stored access policy doesn't revoke existing SAS tokens or access. To revoke all access, you need to regenerate the storage account keys, which will invalidate all existing SAS tokens regardless of their policies.

Reference: https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage

upvoted 3 times

Ruffyit 8 months ago

I believe the correct answer to this is "No". You can up to 5 access policies on an object. Creating a new one doesn't revoke the old one. To revoke a stored access policy, you can delete it, rename it by changing the signed identifier, or change the expiry time to a value in the past. Nowhere in the documentation does it say creating a new one revokes the old one.

upvoted 1 times

codeunit 8 months, 3 weeks ago

No, creating a new stored access policy alone does not meet the goal.

To revoke all access to the storage account (sa1), you need to delete or modify the existing stored access policies associated with the shared access signatures (SAS). When you delete or change an existing stored access policy, all SAS tokens associated with that policy will be immediately invalidated, effectively revoking access.

Creating a new stored access policy does not impact existing SAS tokens, so it will not revoke access for unauthorized users who have valid SAS tokens linked to the current policies. To revoke all access effectively, you should either:

Delete the existing stored access policies linked to the SAS tokens, or
Rotate the account keys for sa1, which will invalidate all SAS tokens associated with those keys.
Therefore, the correct action would be to delete or modify the existing stored access policies or rotate the storage account keys.

upvoted 1 times

saira23 11 months ago

this question was in exam 19/07/2024

upvoted 1 times

Ivan80 1 year, 5 months ago

In exam 1/28/24

upvoted 3 times

trashbox 1 year, 8 months ago

Selected Answer: B

The question was given on the October 9, 2023 exam.

upvoted 3 times

ESAJRR 1 year, 11 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: B

No, creating a new stored access policy does not meet the goal of revoking all access to the Azure Storage account. A stored access policy is used to define a set of constraints and permissions for shared access signatures (SAS) to the resources in the storage account. Creating a new stored access policy does not automatically revoke existing access.

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy#modify-or-revoke-a-stored-access-policy
To revoke a stored access policy, you can delete it, rename it by changing the signed identifier, or change the expiry time to a value in the past. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Changing the expiry time to a value in the past causes any associated signatures to expire. Deleting or modifying the stored access policy immediately affects all of the shared access signatures associated with it.

upvoted 2 times

Johnvic 2 years, 2 months ago

Exam.6 case studies. 3 true/false questions. 47 multiple questions and no simulations. Alot of new questions thats not up here

upvoted 1 times

Gesbie 2 years, 2 months ago

In exam April 11, 2023

upvoted 4 times

majstor86 2 years, 3 months ago

Selected Answer: B

B. NO is correct answer

upvoted 2 times

Diallo18 2 years, 8 months ago

In Exam 10/18/2022. One case study, no lab.

upvoted 1 times

Amit3 2 years, 9 months ago

# In EXAM - 01-Oct-2022

upvoted 1 times

091practiceemail 2 years, 10 months ago

In Exam 08/29/22

upvoted 2 times

Question #2 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
✑ Create Azure Virtual Network.
✑ Create a custom DNS server in the Azure Virtual Network.
✑ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
✑ Configure forwarding between the custom DNS server and your on-premises DNS server.
References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

Community vote distribution

B (100%)

gfhbox0083 Highly Voted 5 years ago

B, for sure.

upvoted 16 times

codeunit Most Recent 8 months, 3 weeks ago

No, deploying the On-premises Data Gateway does not meet the goal for allowing users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

To enable Azure HDInsight to use on-premises Active Directory for authentication, you should set up Azure Active Directory Domain Services (Azure AD DS) or create a VPN or ExpressRoute connection between your on-premises network and Azure. Then, you can deploy Active Directory Domain Services (AD DS) on a virtual machine in the same virtual network as the HDInsight cluster, or use Azure AD DS to synchronize with your on-premises Active Directory.

upvoted 3 times

pentium75 11 months ago

Selected Answer: B

Data gateway has nothing to do with authentication

upvoted 1 times

ESAJRR 1 year, 11 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: B

No, deploying the On-premises data gateway does not meet the goal of configuring the environment to support user authentication to the Azure HDInsight cluster with on-premises Active Directory credentials.

upvoted 1 times

majstor86 2 years, 3 months ago

Selected Answer: B

B. NO is correct answer

upvoted 2 times

rrabeya 2 years, 9 months ago

Answer is B - On premises data gateway is used for services like Power BI, Power Apps, Power Automate, Azure Analysis Services, and Azure Logic Apps.

upvoted 3 times

Nikola112910 2 years, 10 months ago

The answer Should be B for Sure

upvoted 1 times

Alessandro365 3 years ago

Selected Answer: B

B, for sure

upvoted 1 times

Irishtk 3 years, 1 month ago

Ans B

HD Insights uses Enterprise Security Package and custom DNS to connect to on premise AD.

https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure-adds

upvoted 4 times

Eltooth 3 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 3 times

Mcgood 3 years, 11 months ago

Correct Answer Is B NO Doubts

upvoted 3 times

justinp 3 years, 11 months ago

this question was in the test today

upvoted 4 times

markozoide 3 years, 11 months ago

es B, se pasa solo

upvoted 3 times

FK2974 4 years, 3 months ago

Correct answer B!

upvoted 2 times

abilioneto 4 years, 4 months ago

Yes, my guess is B

upvoted 2 times

Question #3 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You create a site-to-site VPN between the virtual network and the on-premises network.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
✑ Create Azure Virtual Network.
✑ Create a custom DNS server in the Azure Virtual Network.
✑ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
✑ Configure forwarding between the custom DNS server and your on-premises DNS server.
References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

Community vote distribution
B (71%) A (29%)

cloudguy365 Highly Voted 5 years, 1 month ago
Here is hint in the question itself--- "You need to configure the environment to support the planned authentication"
They are asking to "configure the environment" to support the planned auth, hence VPN is one of solution
upvoted 74 times

server1 4 years, 10 months ago
excellent observation - we have to read the question carefully
upvoted 5 times

WMG 3 years, 2 months ago
This is and remains the best tip for all cert exams. Read the question carefully. You have tons of time at the exam to read and re-read every question.
upvoted 7 times

Davidf 2 years, 11 months ago
Correct answer is no - the VPN question is misleading, you need Azure AD DS for AUTHENTICATION. You can create an Azure AD DS without a VPN back to on premise.

You could then (for example) bastion into a resource in the Azure AD DS and authenticate to Insight HD from that resource, which has never seen actual on premise.
upvoted 8 times

Holii 2 years, 1 month ago
"You have a hybrid configuration of Azure Active Directory (Azure AD)" This means we already have a connected Active Directory on-premises and Azure for authentication.
S2S will provide the link between the cluster for connectivity.

This is yes.

More food for thought:

Traditionally with these sort of questions (You cannot go back) there is usually one "yes" answer.
This is the yes. It wouldn't follow their normal answer structure to have them all be "no"
upvoted 6 times

⊟ **PDR** Highly Voted 👍 5 years, 5 months ago

agree it is confusing. My reasons :
It says "You have a hybrid configuration of Azure Active Directory (Azure AD)" which suggests that AD Connect is in place , but it isnt clear plus doesnt mention what configuration it has (Hash Synch, Pass through, Federated etc).

Creating a site to site VPN will simply just enabled connectivty between the on premise network and the HDInsight cluster but not fulfil the authentifacation via on premises AD.
So without exact knowledge of the configuration of the Hybrid AD , any AD connect etc it is impossible to say for sure that would work. You could take it further and say it is impossible to know as you dont know the config of the HD cluster, any NSGs etc. I always find this ambiguous questions a bit annoying if I have the knowledge to answer them but the details are too blurry.
upvoted 33 times

⊟ **kiketxu** 4 years, 9 months ago

I agree with your point. This is the key "You have a hybrid configuration of Azure Active Directory (Azure AD)" so if ADConnect is in place it only need connectivity.
My answer in yes, it's right it this case. (Planned authentication doesn't mean plain-text auth, it is about the plan to configure authentication (just says in the above line)

Btw, this same question it is repeated without "Hybrid" AD scenario, where the S2S-VPN isn't the solution and the answer will be NO.
upvoted 6 times

⊟ **stonwall12** Most Recent ⊙ 4 months, 2 weeks ago

Selected Answer: B

Answer: B, No

Reason: While a site-to-site VPN is part of the solution, it's not sufficient alone. You also need to configure Azure AD Domain Services (AD DS) for HDInsight to enable authentication using on-premises AD credentials.

Hint: The VPN connection alone doesn't enable authentication. AD DS is an avaliable answer.

Reference: https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-introduction
upvoted 2 times

⊟ **evangelist** 5 months ago

Selected Answer: B

The solution does not meet the goal because HDInsight ESP requires Azure AD DS, not direct on-premises AD integration. A site-to-site VPN alone is insufficient.
upvoted 2 times

⊟ **codeunit** 8 months, 3 weeks ago

Yes, creating a site-to-site VPN between the virtual network and the on-premises network is part of the solution and meets the goal for allowing users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

For hybrid authentication to Azure HDInsight, the site-to-site VPN enables secure communication between Azure and the on-premises environment. This allows the HDInsight cluster to access the on-premises Active Directory for user authentication.

However, keep in mind that a site-to-site VPN alone is not sufficient; you will also need to ensure that:

Active Directory Domain Services (AD DS) is accessible over the VPN connection.
Azure HDInsight is configured to use this AD DS for Kerberos authentication.
upvoted 1 times

⊟ **Drummer** 1 year, 1 month ago

A. Yes

Creating a site-to-site VPN between the virtual network and the on-premises network would indeed meet the goal. This setup would allow the Azure HDInsight cluster on the virtual network to communicate with the on-premises network, thereby enabling users to authenticate to the cluster using their on-premises Active Directory credentials.

The option “No” would imply that creating a site-to-site VPN between the virtual network and the on-premises network would not allow users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials. However, this is not the case.A site-to-site VPN allows secure communication between resources in a virtual network and an on-premises location over the public internet. It essentially extends your on-premises network to the cloud.

upvoted 2 times

⊟ **wardy1983** 1 year, 7 months ago

Answer: B

Explanation:

AI: Creating a site-to-site VPN between the virtual network and the on-premises network will establish a secure connection between the two networks, but it alone does not enable users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

To support the planned authentication, you need to use Azure AD Domain Services to synchronize on- premises Active Directory with Azure AD. This synchronization will allow users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

Therefore, the given solution alone does not meet the goal.

upvoted 1 times

⊟ **Mnguyen0503** 1 year, 6 months ago

This is incorrect because the question has already said this is a hybrid environment, the credentials are synced at this point.

upvoted 1 times

⊟ **flafernan** 1 year, 8 months ago

Selected Answer: B

NO. Creating a site-to-site VPN between the virtual network and the on-premises network is not sufficient to allow users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials. Azure HDInsight supports integration with Azure AD and does not rely on a site-to-site VPN for integration with on-premises Active Directory.

To enable user authentication with on-premises Active Directory credentials to your Azure HDInsight cluster, you must configure Azure Active Directory Domain Integration with Azure HDInsight. This involves configuring Azure AD Connect or Azure AD DS to extend Azure AD authentication to your on-premises environment.

Therefore, creating a site-to-site VPN is not the appropriate solution for this scenario. Instead, you must configure Azure Active Directory Domain Integration as part of the solution.

upvoted 3 times

⊟ **Sujeeth** 1 year, 9 months ago

Answer is No, creating a site-to-site VPN between the virtual network and the on-premises network alone does not meet the goal of allowing users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

To achieve this goal, you should implement Azure AD Domain Services (Azure AD DS) or Azure AD Connect with Pass-Through Authentication (PTA) and Seamless Single Sign-On (SSO). These solutions enable users to use their on-premises Active Directory credentials to authenticate to Azure resources, including Azure HDInsight clusters.

upvoted 1 times

⊟ **alfaAzure** 1 year, 10 months ago

Selected Answer: B

Configuring Azure AD DS in your Azure AD tenant, not just creating a site-to-site VPN.

upvoted 1 times

⊟ **ESAJRR** 1 year, 11 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

⊟ **microsoftbyomded** 2 years ago

Ok I think I have figured out these 2 HDInsight questions. Either we need a VPN to on-prem AD to perform the authentication or we need Azure AD DS synced with Azure AD Connect (aka "a hybrid configuration"). Here is the other version of the question:
https://www.examtopics.com/discussions/microsoft/view/3791-exam-az-500-topic-2-question-3-discussion/

My answer: Go with Azure AD DS as being the "Yes" variant on this series of questions, thus making this answer "No." Proof:
https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/hdinsight-security-overview#authentication

^ This article discusses Enterprise Security Packages, but that seems to be the only method to connect Hadoop/Apache on which HDInsights is based to Active Directory (both on-prem and Azure AD DS).

upvoted 1 times

microsoftbyomded 2 years ago

Ok I think I have figured out these 2 HDInsight questions. Either we need a VPN to on-prem AD to perform the authentication or we need Azure AD DS synced with Azure AD Connect (aka "a hybrid configuration"). Here is the other version of the question: https://www.examtopics.com/discussions/microsoft/view/3791-exam-az-500-topic-2-question-3-discussion/

My answer: Go with Azure AD DS as being the "Yes" variant on this series of questions. Proof: https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/hdinsight-security-overview#authentication

^ This article discusses Enterprise Security Packages, but that seems to be the only method to connect Hadoop/Apache on which HDInsights is based to Active Directory (both on-prem and Azure AD DS).

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: B

No, creating a site-to-site VPN between the virtual network and the on-premises network does not meet the goal of configuring the environment to support user authentication to the Azure HDInsight cluster with on-premises Active Directory credentials.

To enable authentication with on-premises Active Directory credentials, you need to configure Azure AD Domain Services. Azure AD Domain Services allows you to integrate your on-premises Active Directory environment with Azure AD. This integration enables users to authenticate using their on-premises credentials to access Azure resources such as the Azure HDInsight cluster.

Creating a site-to-site VPN establishes a secure connection between the on-premises network and the Azure virtual network, allowing communication between the two environments. While it is necessary for hybrid connectivity, it does not directly enable authentication with on-premises Active Directory credentials for Azure resources.

Therefore, the correct solution would involve configuring Azure AD Domain Services, not creating a site-to-site VPN.

upvoted 3 times

billo79152718 2 years, 1 month ago

Selected Answer: B

B is correct

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: B

B. No is valid answer

upvoted 5 times

Fal991l 2 years, 4 months ago

Selected Answer: B

AI: Creating a site-to-site VPN between the virtual network and the on-premises network will establish a secure connection between the two networks, but it alone does not enable users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

To support the planned authentication, you need to use Azure AD Domain Services to synchronize on-premises Active Directory with Azure AD. This synchronization will allow users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

Therefore, the given solution alone does not meet the goal.

upvoted 3 times

Holii 2 years, 1 month ago

"You have a hybrid configuration of Azure AD." I would assume you already have an On-premises AD and Azure AD connected.

upvoted 1 times

Question #4 *Topic 2*

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.
You need to recommend an integration solution that meets the following requirements:
✑ Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
✑ Minimizes the number of servers required for the solution.
Which authentication method should you include in the recommendation?

A. federated identity with Active Directory Federation Services (AD FS)

B. password hash synchronization with seamless single sign-on (SSO)

C. pass-through authentication with seamless single sign-on (SSO)

Suggested Answer: *B*
Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.
Incorrect Answers:
A: A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.
C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.
Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests.
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Community vote distribution

C (97%)

⊟ **Ace786** Highly Voted 4 years, 10 months ago
PTA for sure as you need to enforce on prem password policies hence pass through to on prem
upvoted 109 times

⊟ **kanag1** 3 years, 5 months ago
Thank you Ace786 and those upvoted to confirm the answer !
upvoted 1 times

⊟ **rawrkadia** 3 years, 11 months ago
Agreed. The question cares about logon restrictions as well as password policies, AAD doesn't care about those. AAD also only respects enabled/disabled statuses, so with PHS an expired password still functions for cloud services.
upvoted 3 times

⊟ **rgullini** 4 years, 2 months ago
Agree with you. PTA due to the policies. Microsoft uses to create this questions which might lead to confusion with statements like "least administrative effort required" or "minimize the number of servers". These statements should be taken as "when possible" or "as much as possible"
upvoted 16 times

⊟ **rke2** 2 years, 8 months ago
C: PTA

A is out; it required more servers

B could be the answer but user logon restriction does not sync immediately

"The password expired and account locked-out states aren't currently synced to Azure AD with Azure AD Connect. When you change a user's password and set the user must change password at next logon flag, the password hash will not be synced to Azure AD with Azure AD Connect until the user changes their password."

From <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

upvoted 4 times

pentium75 11 months ago

"User logon restrictions" do not sync at all with hash sync. Users can still log on to Entra ID even if their password or accounts are expired, etc.

upvoted 1 times

Ilko Highly Voted 👍 4 years, 6 months ago

This is the breaking point, actually password policies is not like GPO(GPOs are only in AADDS and ADDS, no such thing like GPOs in AAD) ---- ✑ Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant

Also, we need to have less servers to manage ✑ Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?
A. federated identity with Active Directory Federation Services (AD FS) - completely not matching our requirements.
B. password hash synchronization with seamless single sign-on (SSO) - this is match
C. pass-through authentication with seamless single sign-on (SSO) - this is match as well.

Why B is more correct? Because both authentication methods enforce password policies, but with B we do not have to manage large on prem infrastructure in order to protect sign in process. Which meets the second requirements in the question - minimize the servers required.
At first I got confused as well, but in question they are talking about password policies not GPOs.
Which make sense why B is the correct one.

upvoted 37 times

cfsxtuv33 3 years, 6 months ago

You are absolutely correct in your explanation and answer choice...password hash synchronization is the better choice. PTA is valid but in my opinion answer B is the better of the two.

upvoted 3 times

Sajinp 3 years, 10 months ago

I think option 3 (PTA) is more appropriate because not all onpremise password policies and user login restrictions are applied with PHS.
wIth PHS, by default the cloud account password is set to Never Expire.
1) "You can continue to sign in to your cloud services by using a synchronized password that is expired in your on-premises environment. "
2) "If your organization uses the accountExpires attribute as part of user account management, this attribute is not synchronized to Azure AD. As a result, an expired Active Directory account in an environment configured for password hash synchronization will still be active in Azure AD."

upvoted 7 times

Ivanvazovv 2 years, 10 months ago

With PTA you use the GPOs on your domain controllers. So if you want to control password policies from your DCs, PTA is the way.

upvoted 1 times

ChinkSantana 3 years, 12 months ago

I Agree with you. B is correct. PHS

When password hash synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use all of the valid passwords from your on-premises Active Directory instance to access Azure AD services.

Key word here is : "Synchronized users"
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

upvoted 5 times

pentium75 Most Recent 🕘 11 months ago

Selected Answer: C

A - too many servers

B - logon restrictions etc. not synced

upvoted 2 times

QueZee 1 year, 3 months ago

C. Pass-through authentication with seamless single sign-on (SSO)

Minimizes Servers: PTA leverages a lightweight agent installed on a Windows Server in your on-premises network, reducing server requirements compared to AD FS.

Enforces Policies: During user sign-in, PTA validates user credentials directly against your on-premises AD. This ensures that on-premises password policies and logon restrictions are applied to synchronized accounts in Azure AD.

upvoted 1 times

bugger123 1 year, 4 months ago

Selected Answer: C

. .

upvoted 1 times

ManiMessner 1 year, 7 months ago

Selected Answer: C

C. password hash sync

The solution is not dependent on the type of sync, so the easier to setup is hash sync

Microsoft Entra Password Protection is designed with the following principles in mind:

The software isn't dependent on other Microsoft Entra features. For example, Microsoft Entra password hash sync (PHS) isn't related or required for Microsoft Entra Password Protection.

upvoted 1 times

wardy1983 1 year, 7 months ago

Answer: C

Explanation:

1. C. pass-through authentication with seamless single sign-on (SSO)

2. Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method (PTA).https://learn.microsoft.com/en- us/azure/active-directory/hybrid/choose-ad-authn

upvoted 1 times

Feraso 1 year, 8 months ago

Selected Answer: C

C: PTA

This feature is an alternative to Microsoft Entra Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta#what-is-microsoft-entra-pass-through-authentication

upvoted 1 times

MeisAdriano 1 year, 8 months ago

Selected Answer: C

you can't ensures that password policies and user logon restrictions appl on hashes

upvoted 1 times

BigShot0 1 year, 9 months ago

Selected Answer: C

Pass through is required to enforce on-prem login requirements

upvoted 1 times

Sujeeth 1 year, 9 months ago

C can be answrer The recommended authentication method is pass-through authentication with seamless single sign-on (SSO) because it enforces on-premises password policies and user logon restrictions, ensuring consistency with Azure AD. This approach also minimizes the need for additional servers, making the solution efficient. Seamless SSO enhances the user experience by enabling single sign-on for both on-premises and cloud resources.

upvoted 1 times

Sujeeth 1 year, 9 months ago

C is answer

upvoted 1 times

ESAJRR 1 year, 11 months ago

Selected Answer: C

C. pass-through authentication with seamless single sign-on (SSO)

upvoted 1 times

Millard90 2 years ago

Selected Answer: C

Pass-through is required for logon restrictions.

upvoted 1 times

Pupu86 2 years ago

PHA - does not fulfil the policy enforcement though password hashs are sync to AAD via AD Connect but still not sufficient to authenticate with on-perm AD credentials
Federated with/without AD DS on-premise or brand new setup in Azure - requires mice of additional servers/VMs
PTA - enables enforcement of on-prem AD policies and authentication of user accounts

So I would go with PTA since its the closest possible answer.

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: B

To meet the requirements of ensuring password policies and user logon restrictions apply to user accounts synced to the Azure AD tenant while minimizing the number of servers required, the recommended authentication method is password hash synchronization with seamless single sign-on (SSO).

With password hash synchronization, the password hashes from on-premises Active Directory are synchronized to Azure AD. This allows users to sign in to Azure AD using their on-premises passwords. By enabling seamless single sign-on (SSO), users can access Azure AD-integrated resources without needing to re-enter their credentials.

This solution ensures that the password policies and user logon restrictions defined in the on-premises Active Directory apply to the synchronized user accounts in Azure AD. Additionally, it minimizes the infrastructure requirements as it does not require additional servers, such as Active Directory Federation Services (AD FS), for federated identity.

upvoted 1 times

Amnesia 2 years, 1 month ago

Pass-through authentication with Seamless Single Sign-On requires a separate agent to be installed on-premises and as a requirement it is necessary to minimize the number of servers. the correct answer is B.

upvoted 1 times

Question #5 *Topic 2*

Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You sync all on-premises identities to Azure AD.
You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.
What should you use?

A. Synchronization Rules Editor

B. Web Service Configuration Tool

C. the Azure AD Connect wizard

D. Active Directory Users and Computers

Suggested Answer: *A*
Use the Synchronization Rules Editor and write attribute-based filtering rule.
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

Community vote distribution

A (100%)

AS007 Highly Voted 4 years, 2 months ago

Correct Answer

upvoted 28 times

mackc13 Highly Voted 4 years ago

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

Answer is correct

upvoted 9 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: A

Answer: A, Synchronization Rules Editor

Reason: The Synchronization Rules Editor is the correct tool for creating custom filtering rules based on LDAP attributes like givenName. It allows you to create a scoping filter that prevents users with specific attribute values from syncing to Azure AD without modifying the user objects themselves.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration#create-an-attribute-based-filter

upvoted 2 times

ESAJRR 11 months, 3 weeks ago

Selected Answer: A

A. Synchronization Rules Editor

upvoted 1 times

majstor86 1 year, 3 months ago

Selected Answer: A

A. Synchronization Rules Editor

upvoted 1 times

Juhee23 1 year, 6 months ago

A is correct answer

upvoted 1 times

feln 2 years ago

Selected Answer: A

Yup correct

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 3 times

udmraj 2 years, 4 months ago

Correct Answer - A

upvoted 2 times

DarkCyberGhost 2 years, 5 months ago

Selected Answer: A

Correct Answer

upvoted 2 times

DrRossmondMD 2 years, 6 months ago

Selected Answer: A

Correct Answer

upvoted 2 times

AS179 2 years, 6 months ago

A is correct

upvoted 1 times

rohitmedi 2 years, 7 months ago

correct answer repeated

upvoted 1 times

TonytheTiger 2 years, 9 months ago

## Exam Question - 17 Sept 2021 ##

upvoted 3 times

Fred64 3 years, 3 months ago

answer A

upvoted 3 times

finolweb 3 years, 4 months ago

In exam

upvoted 5 times

zic04 3 years, 5 months ago

A correct answer

upvoted 2 times

Question #6 Topic 2

DRAG DROP -

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

✑ Users with leaked credentials

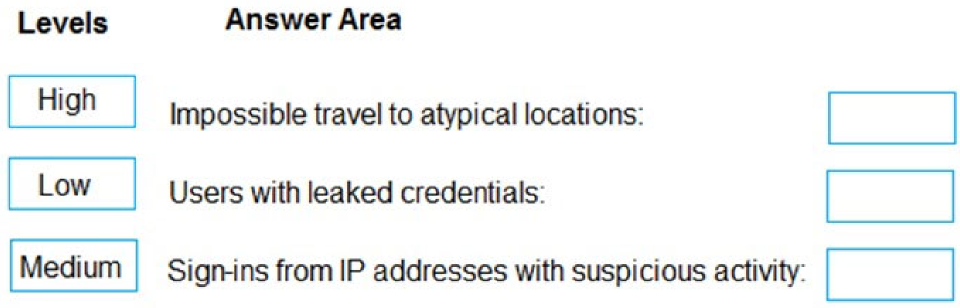
✑ Impossible travel to atypical locations

✑ Sign-ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Levels

High

Low

Medium

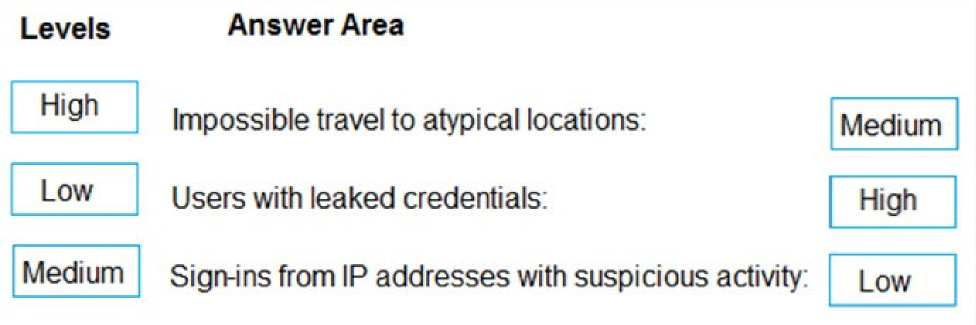
Answer Area

Impossible travel to atypical locations:

Users with leaked credentials:

Sign-ins from IP addresses with suspicious activity:

Suggested Answer:



Levels

High

Low

Medium

Answer Area

Impossible travel to atypical locations: Medium

Users with leaked credentials: High

Sign-ins from IP addresses with suspicious activity: Low

Azure AD Identity protection can detect six types of suspicious sign-in activities:

✑ Users with leaked credentials

✑ Sign-ins from anonymous IP addresses

✑ Impossible travel to atypical locations

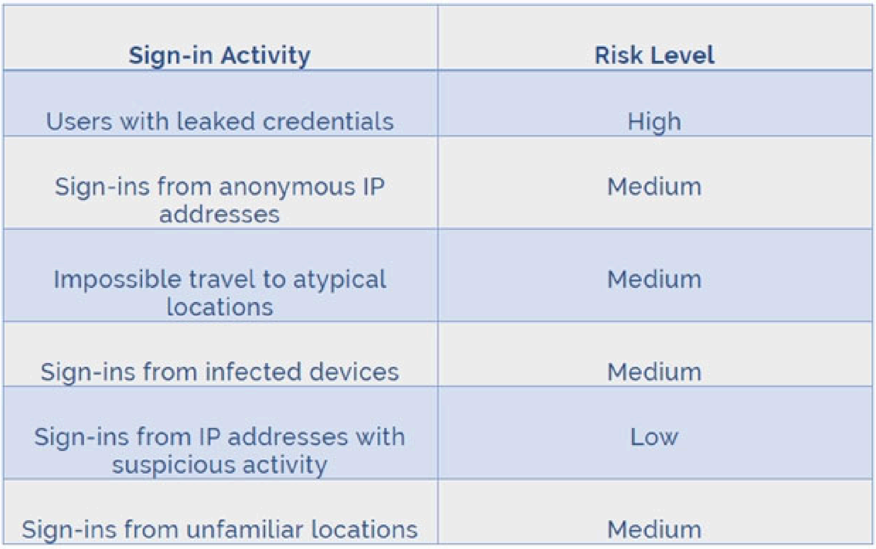
Sign-ins from infected devices -

▪

✑ Sign-ins from IP addresses with suspicious activity

✑ Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks ג€" High, Medium & Low:



Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

⊟ **majstor86** Highly Voted 👍 2 years, 3 months ago

Medium

High

Medium

The question is not valid anymore

upvoted 27 times

⊟ **Malikusmanrasheed** 2 years, 1 month ago

rebeladmin guide attached is outdated. The newer guide doesn't have any indication of the severity of each risk

upvoted 3 times

⊟ **ahorva** Highly Voted 👍 3 years, 1 month ago

This question is no longer valid. The referenced article in the explanation also mentions the same thing :
"Some time ago I wrote this article about sign-in risk-based conditional access policies. But things have been changed over time and I thought it is time to update it with new content. The updated post can access using https://www.rebeladmin.com/2020/11/step-by-step-guide-how-to-configure-sign-in-risk-based-azure-conditional-access-policies/ "

upvoted 5 times

⊟ **PowerBIAddict** 3 years, 1 month ago

Agreed. Trying to confirm the impossible travel in Microsoft docs it is clear that Azure has changed since this question was originally included. Amusingly the official practice exam has a very similar question.

upvoted 3 times

⊟ **stonwall12** Most Recent 🕘 4 months, 2 weeks ago

Answer:

1. Impossible travel to atypical location: Medium
2. Users with leaked credential: High
3. Sign-ins from IP addresses with suspicious activity: Medium

Reason: Impossible travel to atypical locations: Medium

- This is considered a high-risk event because it indicates potentially impossible geographic movements that could signal account compromise

Users with leaked credentials: High

- This represents a medium risk as the credentials are known to be compromised but haven't necessarily been used maliciously yet

Sign-ins from IP addresses with suspicious activity: Medium

- This is also classified as medium risk since suspicious IP addresses might indicate potential attack attempts but aren't definitive proof of compromise

Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

upvoted 2 times

⊟ **trashbox** 1 year, 8 months ago

Impossible travel: Medium

Leaked credentials: High

IP addresses with suspicious activity: Medium

upvoted 1 times

⊟ **Andre369** 2 years, 1 month ago

Users with leaked credentials - Low

Impossible travel to atypical location - High

Sign-ins from IP addresses with suspicious activity - Medium

The rationale behind these choices is as follows:

Users with leaked credentials are typically considered to have a lower risk level because it indicates a potential compromise of user credentials but may not necessarily imply immediate unauthorized access to sensitive resources.

Impossible travel to atypical location suggests a high risk level because it indicates a significant deviation from the user's typical travel patterns, which can be indicative of account compromise or misuse.

Sign-ins from IP addresses with suspicious activity indicate a medium risk level because it suggests potential suspicious behavior but may require further investigation to determine the severity and intent of the activity.

upvoted 1 times

xRiot007 11 months, 2 weeks ago

"Users with leaked credentials - Low" - Really ? I suggest using Chat GPT less.

upvoted 1 times

IvanIco 1 year, 9 months ago

what are u high on bro, it must be some good sh**, i don't know how can someone say the leaked credentials is low risk... but it is high just like you are high on some good stuff

upvoted 8 times

FonKeel 2 years, 5 months ago

I doubt such question would appear in exams as the Risk level differ based on organization's risk definitions, Microsoft can only recommend but can't bind such levels.

upvoted 3 times

awfnewf1q243 2 years, 8 months ago

Note: It is very unlikely the Microsoft will require the memorization of specific risk levels given that they have changed the documentation.

Previously the risk levels were very well defined, however they now provide this very vague paragraph:

"Microsoft doesn't provide specific details about how risk is calculated. Each level of risk brings higher confidence that the user or sign-in is compromised. For example, something like one instance of unfamiliar sign-in properties for a user might not be as threatening as leaked credentials for another user."

Modern Documentation: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#investigate-risk

Legacy Documentation: https://web.archive.org/web/20190419234045/https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events

upvoted 4 times

the_flow88 2 years, 11 months ago

question no longer valid - you can now assign your own "score" to any item based on your companies needs. Which makes more sense anyway...

upvoted 2 times

phi3nix 3 years, 1 month ago

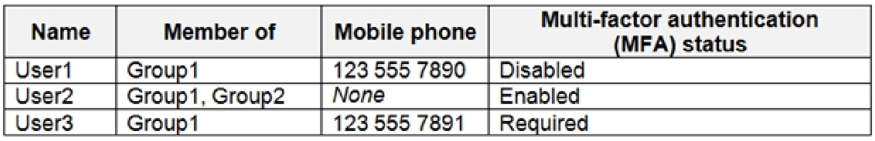
Sign-ins from IP addresses with suspicious activity is Medium now.
https://github.com/toddkitta/azure-content/blob/master/articles/active-directory/active-directory-identityprotection-risk-events-types.md#sign-ins-from-ip-addresses-with-suspicious-activity

upvoted 4 times

Question #7 *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	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	*None*	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

✑ Assignment: Include Group1, Exclude Group2

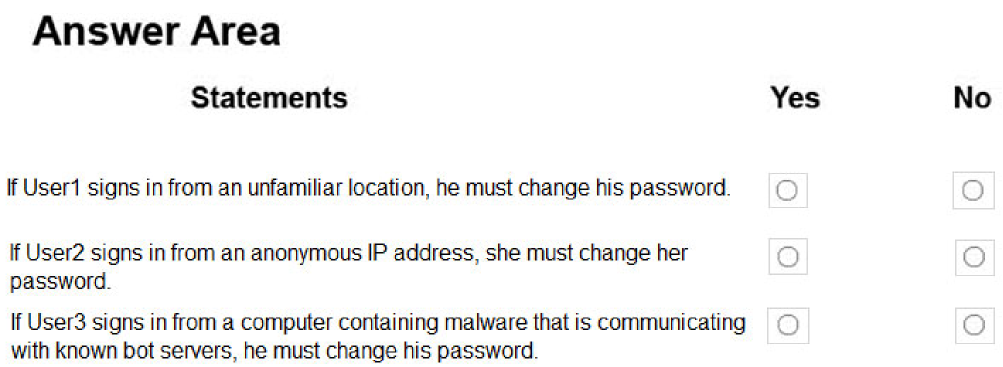
✑ Conditions: Sign-in risk of Medium and above

✑ Access: Allow access, Require password change

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

NOTE: Each correct selection is worth one point.

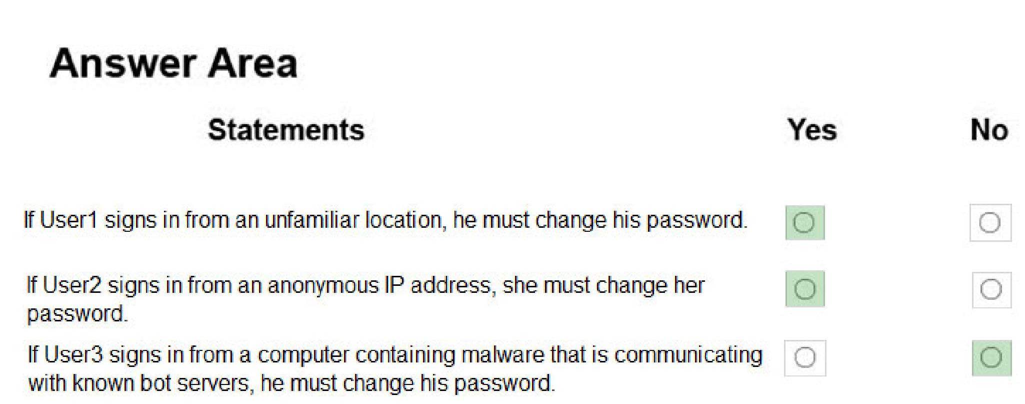
Hot Area:



Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	[✓ ○]	○
If User2 signs in from an anonymous IP address, she must change her password.	[✓ ○]	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	[✓ ○]

Box 1: Yes -

User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

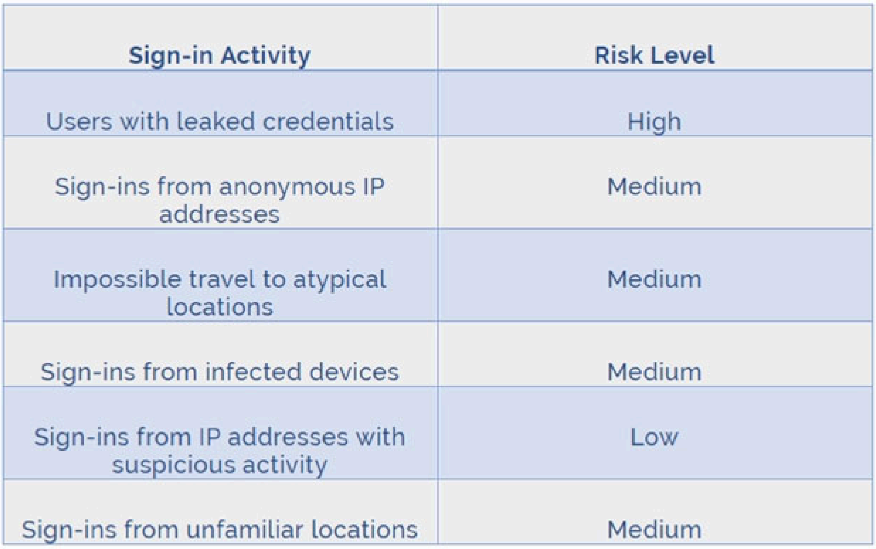
Box 2: Yes -

User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.

Box 3: No -

Sign-ins from IP addresses with suspicious activity is low.

Note:



Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Azure AD Identity protection can detect six types of suspicious sign-in activities:
✑ Users with leaked credentials
✑ Sign-ins from anonymous IP addresses
✑ Impossible travel to atypical locations
✑ Sign-ins from infected devices
✑ Sign-ins from IP addresses with suspicious activity
✑ Sign-ins from unfamiliar locations
These six types of events are categorized in to 3 levels of risks ɿ€" High, Medium & Low:
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

⊟ **Geeky93** Highly Voted 4 years, 3 months ago
Wrong answer.

Should be :

YES, NO, NO
"When organizations both include and exclude a user or group the user or group is excluded from the policy, as an exclude action overrides an include in policy. "
Source :
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups
upvoted 165 times

⊟ **kitus** 1 year ago
shouldn't it be YES, NO, YES? the third use case is Medium sign-in risk because the authentication comes from an infected device
upvoted 5 times

⊟ **ITFranz** 6 months ago
To support the third answer.
Yes, if a user signs in from a computer containing malware that is communicating with bot servers, the user should change their password.
This is an important security measure for several reasons:
Malware on the computer may include keyloggers or other tools that can capture passwords as they are entered1.
The malware communicating with bot servers indicates an active security breach, which could potentially expose sensitive information including login credentials2.
Changing passwords is a crucial step in securing accounts after a potential compromise3.
User3 = Yes
upvoted 2 times

⊟ **Patchfox** 3 years, 6 months ago
Correct answer
upvoted 2 times

⊟ **vtoroynah** 3 years, 5 months ago

"##Sign-ins from infected devices
This risk event type identifies sign-ins from devices infected with malware, that are known to actively communicate with a bot server. This is determined by correlating IP addresses of the user's device against IP addresses that were in contact with a bot server.

This risk event identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is the reason for classifying this risk event as "Low"."

https://github.com/toddkitta/azure-content/blob/master/articles/active-directory/active-directory-identityprotection-risk-events-types.md
upvoted 4 times

⊟ **rctm_bm** Highly Voted 4 years, 3 months ago
Agree with Geeky93, but not sure with 3rd answer. Given question with malware refers to infected device wich is Medium Risk Level, so the answer should be YES.
YES,NO,YES
upvoted 134 times

⊟ **Vikku30** 3 years, 6 months ago
Yes it should : Yes, No & Yes as in option 3 the device is compromised/infected so access from infected device is medium level severity and as per question any sign in above medium risk level, password should be changed
upvoted 4 times

⊟ **rgullini** 4 years, 2 months ago
totally agree with rctm_bm
upvoted 5 times

⊟ **udmraj** 3 years, 4 months ago
It should be Yes, No, Yes

Number 3 is a Malware infected System, which is Infected system
upvoted 13 times

⊟ **JCWF** 4 years, 3 months ago
Device containing malware refers to infected device which is Low Risk Level,
upvoted 9 times

⊟ **cannibalcorpse** 4 years, 2 months ago
Exactly,any event not related to credentials leakage, we may say as Low Risk Level.
upvoted 3 times

⊟ **cfsxtuv33** 3 years, 6 months ago
Infected Devices: Medium Risk
upvoted 3 times

⊟ **rctm_bm** 3 years, 11 months ago
No. The only Low Risk Level is Sign-ins from IP addresses with suspicious activity. Everything else is medium\high
upvoted 15 times

⊟ **Knighthell** Most Recent 3 weeks, 2 days ago
yes-no-yes

Unfamiliar location -> risk high or Medium -> YES
User2 signs in from an anonymous IP address --> policy exclusions
User 3 malware --> risk high yes
upvoted 2 times

⊟ **Knighthell** 3 weeks, 3 days ago
Risk detection Risk level (as used by Identity Protection)
Leaked credentials High
Anonymous IP address Medium
Password spray High
Unfamiliar sign-in properties Low
Malware linked IP address High
Impossible travel Medium

NO-NO-YES

Risk detection Risk level (as used by Identity Protection)
Leaked credentials High
Anonymous IP address Medium
Password spray High
Unfamiliar sign-in properties Low
Malware linked IP address High
Impossible travel Medium
upvoted 1 times

SofiaLorean 3 months, 3 weeks ago
Yes No Yes
upvoted 1 times

MarcoHurry 7 months, 3 weeks ago
Me too: YES, NO, YES for the same reasons discussed here
upvoted 1 times

pentium75 11 months ago
YES, NO, YES.
User 2 is excluded
Other risks are medium or higher
upvoted 1 times

ShambhuSNair 11 months, 1 week ago
Answer: Yes No Yes
1. Risk rating for User1 is medium and User1 is part of Group1 where Risk policy applies, So User1 will be allowed to sign-in after changing the password.
2. Risk rating for User 2 is medium, but the risk policy is not applied as User2 is part of Group2 which is excluded from the assignment. Hence User2 wont be allowed to sign-in, and won't be prompted to change the password.
3. Risk rating for User3 is medium and User3 is part of Group1 where Risk policy applies, So User3 will be allowed to sign-in after changing the password.
upvoted 2 times

Jkayx94 1 year, 4 months ago
Yes, No Yes.

B - Exclusion takes precedence of Inclusion

C - Device is Infected with Malware, regardless if it's communicating with a botnet, it's detected as Malware = Medium Risk = Included in CAP.
upvoted 3 times

ABIYGK 1 year, 7 months ago
Explanation:
Box 1: Yes - User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.
Box 2. No - "When organizations both include and exclude a user or group the user or group is excluded from the policy, as an exclude action overrides an include in policy. "

Box 3: Yes - Sign-ins from infected device is Medium.
upvoted 6 times

xRiot007 11 months, 2 weeks ago
Sign-ins from infected device is LOW
https://github.com/toddkitta/azure-content/blob/master/articles/active-directory/active-directory-identityprotection-risk-events-types.md
upvoted 1 times

wardy1983 1 year, 7 months ago
Explanation:
Box 1: Yes -
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.
Box 2 no
"When organizations both include and exclude a user or group the user or group is excluded from the policy, as an exclude action overrides an include

in policy. "

Box 3: No -

Sign-ins from IP addresses with suspicious activity is low.

upvoted 1 times

⊟ **jimmyjose** 1 year, 7 months ago

The answer to Box 3 is 'YES' because it talks about a computer containing malware communicating with bots. There is a difference between malware (MEDIUM) and suspicious activity (LOW).

upvoted 1 times

⊟ **MeisAdriano** 1 year, 8 months ago

NO: unfamiliar location i think is similar to IP suspected, so low level not medium level risk.

NO: "anonymous" IP address is the same of "unfamiliar location", similar to suspicious IP address, so the risk is low

YES: because infected device is medium risk (not IP suspected that is low rish). The question says on medium and above sign-in risk you have to require password change.

upvoted 1 times

⊟ **GaryKing123** 1 year, 8 months ago

So having MFA enabled, disabled or even required doesn't impact the answer here I believe. In Entra under CA, now when you Grant access you can either have "require MFA" or "require authentication strength" or "require password change" among various options

upvoted 1 times

⊟ **JunetGoyal** 1 year, 8 months ago

Yes NoYes

upvoted 1 times

⊟ **fireb** 1 year, 9 months ago

Based on changes on Azure over the years, the answer should be:

Yes, Yes, Yes.

upvoted 4 times

⊟ **xRiot007** 11 months, 2 weeks ago

No. Anon IP login should require at most MFA, not a password change.

upvoted 1 times

⊟ **ArchitectX** 1 year, 9 months ago

It should be Yes No No

upvoted 1 times

⊟ **heatfan900** 1 year, 10 months ago

Y, N, N.

USER 1 belongs to GROUP 1 and meet the Medium or Higher Conditions

USER 2 belong to GROUP 1 and 2. Since Group 2 is excluded, the user will then be excluded even though he belongs to GROUP 1. When a user is in two different groups and one is excluded, they are excluded, even if the other group they belong to is included in the RISK POLICY.

USER 3 is signing in from an infected device. This risk event identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is the reason for classifying this risk event as “Low”.

upvoted 3 times

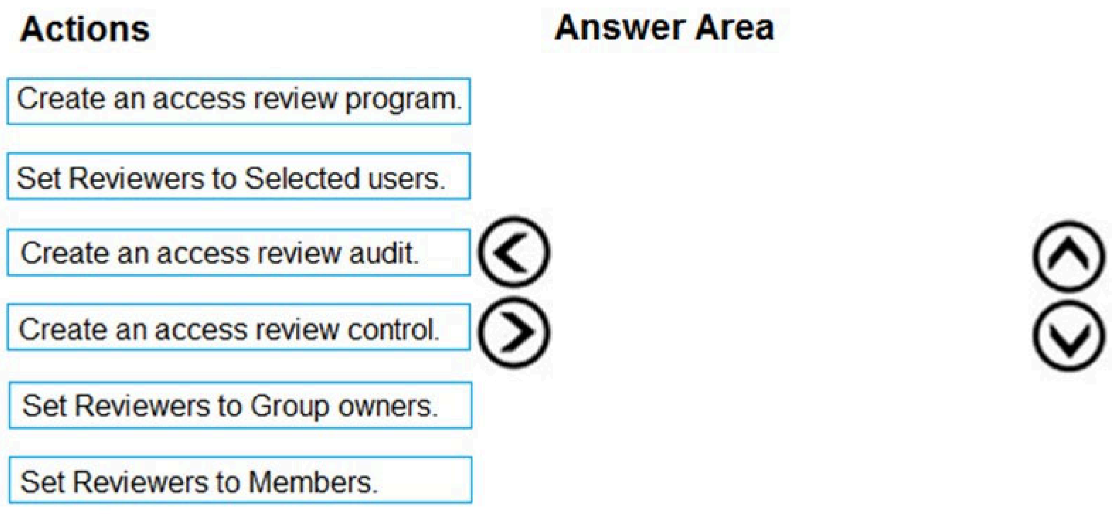
Question #8 *Topic 2*

DRAG DROP -

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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

Select and Place:

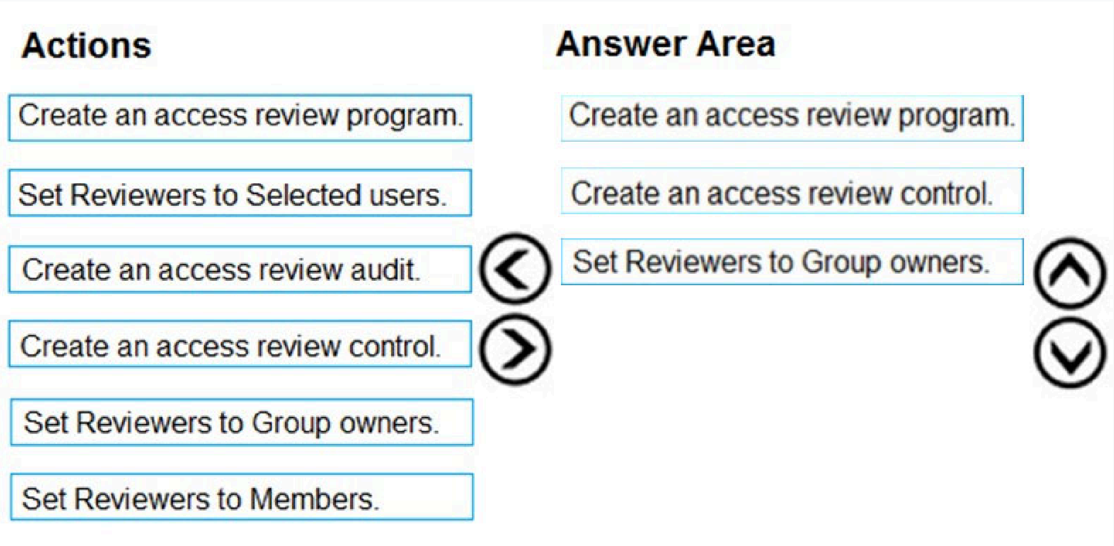


Actions

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

Suggested Answer:



Actions

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

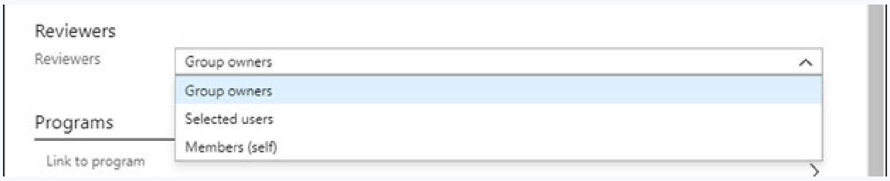
- Create an access review program.
- Create an access review control.
- Set Reviewers to Group owners.

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reviewers

Reviewers: Group owners

- Group owners
- Selected users
- Members (self)

Programs

Link to program

References:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

PDR Highly Voted 5 years, 4 months ago

The answer is correct. The question itself refers to assigning a "collection of reviews" which means a access review program. In order to assign a program to a access review it must first be created , otherwise only the default program can be assigned. So that is why it is first step.

upvoted 46 times

BobIsSearchingForTheMoon 5 years, 4 months ago

I agree with PDR, and notice that it says "The review will be assigned to a NEW collection of reviews". So new collection means the collection "program" needs to be created first.

upvoted 6 times

FK2974 Highly Voted 4 years, 3 months ago

correct ! Program/Control/Owner

upvoted 16 times

SofiaLorean Most Recent 3 months, 3 weeks ago

The answer is correct!

upvoted 1 times

stonwall12 4 months, 2 weeks ago

Answer: The correct sequence is:

1. Create an access review program
2. Create an access review control
3. Set Reviewers to Group owners

Reason: When configuring access reviews in Azure AD:

1. Create an access review program which serves as the container for your reviews
2. Create an access review control which defines the scope and settings of the review
3. Set the reviewers to Group owners since the requirement states it should be reviewed by resource owners

Reference: https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review

upvoted 1 times

bob_sez 1 year, 7 months ago

I just took my exam on 25th Nov 2023 and I wasnt aware that this is an open book exam. I am not sure if this comment will be approved, but you can open Learn.microsoft.com during the exam and do your research for any question.

upvoted 6 times

MPB 1 year, 1 month ago

https://techcommunity.microsoft.com/t5/microsoft-learn-blog/introducing-a-new-resource-for-all-role-based-microsoft/ba-p/3500870
That's
Hilarious guys)))

upvoted 1 times

dc864d4 1 year, 1 month ago

Open book not in the traditional sense. It's timed, proctored and the only resource is Microsoft Learn.....but that does help. Right now the test would be pretty difficult to pass without a resource as they are in process of making major changes.

upvoted 1 times

UjunwaRejoice 1 year, 5 months ago

RAEALLY?, YOU WONT BE PENALISED FOR IT?

upvoted 2 times

yonie 1 year, 6 months ago

You just blew my mind

upvoted 1 times

ArchitectX 1 year, 9 months ago

right answer

upvoted 2 times

Andre369 2 years, 1 month ago

To configure an access review assigned to a new collection of reviews and reviewed by resource owners, you should perform the following three actions in sequence:

Create an access review program
Set Reviewers to selected users
Set Reviewers to Group owners
These actions ensure that an access review program is created, reviewers are specified as selected users, and the reviewers are set to the owners of the relevant groups.

upvoted 1 times

xRiot007 11 months, 2 weeks ago

Inside a program you need a Control.

upvoted 1 times

majstor86 2 years, 3 months ago

1. Create program
2. Create control
3. Set reviewers to Group owners

upvoted 4 times

ltjones12 2 years, 5 months ago

Really disappointed with how nobody in exam topics seems to be cleaning up or upgrading their deprecated questions

upvoted 9 times

mung 2 years, 7 months ago

Damn why there are so many deprecated question on AZ-500?
Az-104 was fine..

upvoted 2 times

D3D1997 2 years, 5 months ago

coz AZ-500 had never its number changed;
AZ-104 is newer, AZ-305 is the sequel to AZ-300/301 (2018/2019) AZ-303/304 (2020/2021)...
so should be a AZ-503 by now...

upvoted 3 times

JohnBentass 2 years, 7 months ago

The answer is correct

upvoted 1 times

OpsecDude 2 years, 9 months ago

Hey guys.

I just created an access review and all I did was:

1_Create the Access review from Identity Governance (no longer on "Access Review" plus no onboarding needed)

2_ Set reviewers.

Then off course I set up what happens with reviewees if reviewers don't respond, durations, etc, but no access review control

upvoted 4 times

Patchfox 3 years, 6 months ago

Is this question up to date?
I can't find any documentation about programs. The added links forword me to the documentation of access review, not programs.
I saw in the Identity Governance the Program section. Is this still a recommended feature or near to the end of life?

upvoted 2 times

Joshing 3 years, 4 months ago

I believe this is deprecated. I found a link to the Microsoft Graph API beta where it shows the Access Review Program and it's under the deprecated section. With the new api for Access Reviews as showing V2 in the url.

https://docs.microsoft.com/en-us/graph/api/resources/program?view=graph-rest-beta

upvoted 5 times

Joshing 3 years, 4 months ago

I was wrong this completely exists...

If anyone else is looking for the location of this, it is found here -
https://portal.azure.com/#blade/Microsoft_AAD_ERM/DashboardBlade/Programs

There is basically no documentation on it but it is similar to Catalogs for access packages. Just a logical container for storing access reviews.

upvoted 2 times

Joshing 3 years, 4 months ago

My brain is like mush from studying this exam. Apologies.

upvoted 6 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 3 times

justinp 3 years, 11 months ago

this question is present in test today

upvoted 4 times

milind8451 4 years, 4 months ago

Right ans.

upvoted 1 times

sureshatt 4 years, 4 months ago

With the new UI (2021.02.12) it is very hard to answer this question since the terms are not 100% aligning with the terms in the new UI. But still the answer provided here is correct.

1. Since the question talks about creating a collection of access reviews, we first need to create an access review programme.

2. Then we have to create an access review (here I have to assume 'access review control' = 'access review').

3. Question says the "resource owners" should perform the review. Here the owners can be Group owner role. Therefore assignment should be to group owners. (I honestly thinks that the word "resource" was used just to confuse us)

upvoted 8 times

sureshatt 4 years, 3 months ago

as of today, 2021.03.28, access review programs and access review controls do not exists. Only access reviews exists.

upvoted 6 times

WMG 3 years, 2 months ago

Wrong. Programs exists under Home>Identity Governance>Programs. We use this regularly.

upvoted 1 times

micofucho 3 years, 11 months ago

What if the review is for Applications??, the questions says anything about if the review is on Teams and Groups or Applications. Then, who is the owner?? The question is rubbish, like a lot of questions in the exam: ambiguous, mal formed and with thousands of interpretations. It's not a problem of trying to confuse, it's a problem of a stupid person formulating the questions for the exam.

upvoted 1 times

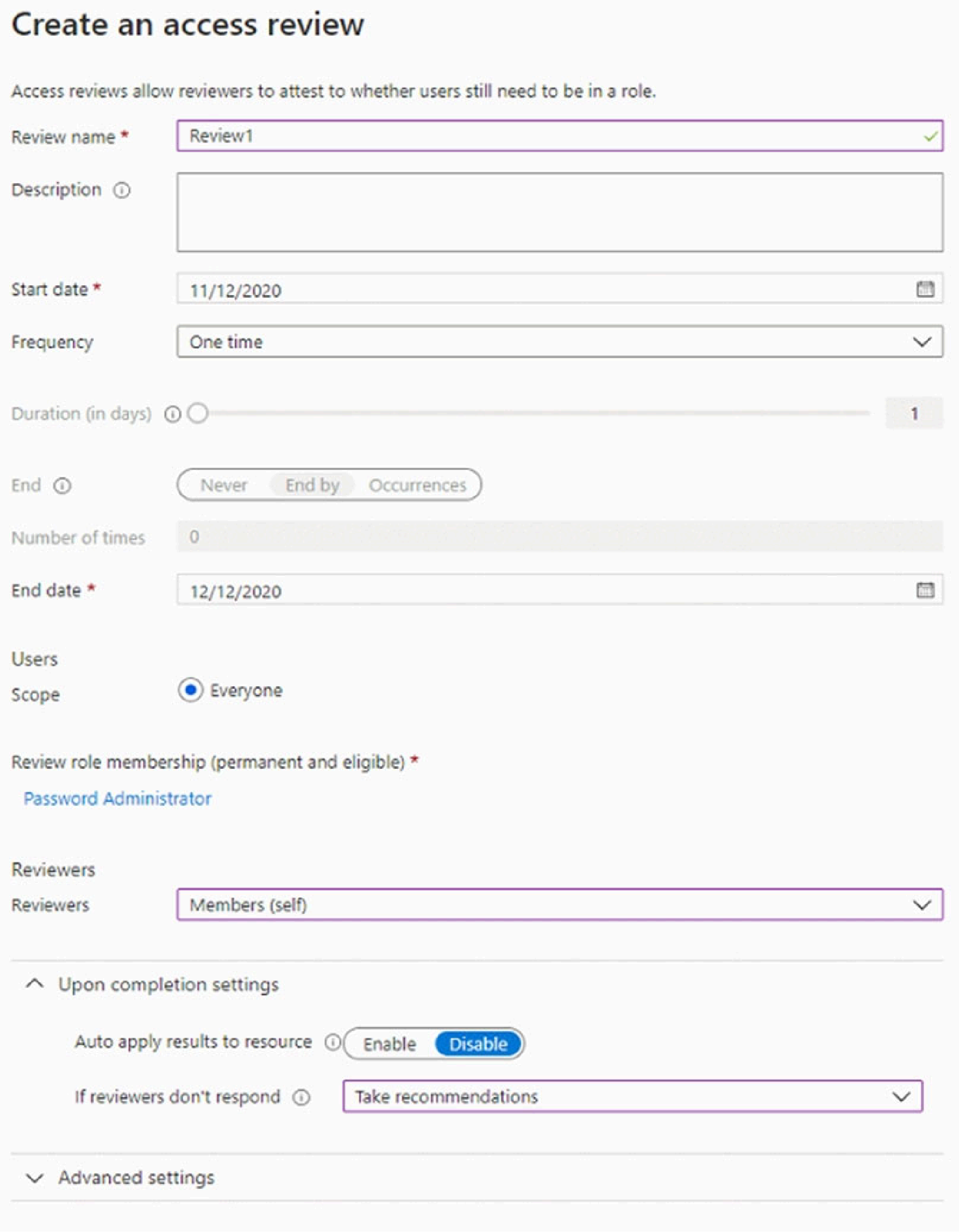
Question #9 *Topic 2*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Sign in frequency
User1	Password administrator	Signs in every work day
User2	Password administrator	Signs in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.



Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *: Review1

Description ⓘ:

Start date *: 11/12/2020

Frequency: One time

Duration (in days) ⓘ: 1

End ⓘ: Never | End by | Occurrences

Number of times: 0

End date *: 12/12/2020

Users

Scope: ● Everyone

Review role membership (permanent and eligible) *

Password Administrator

Reviewers

Reviewers: Members (self)

Upon completion settings

Auto apply results to resource ⓘ: Enable [✓ Disable]

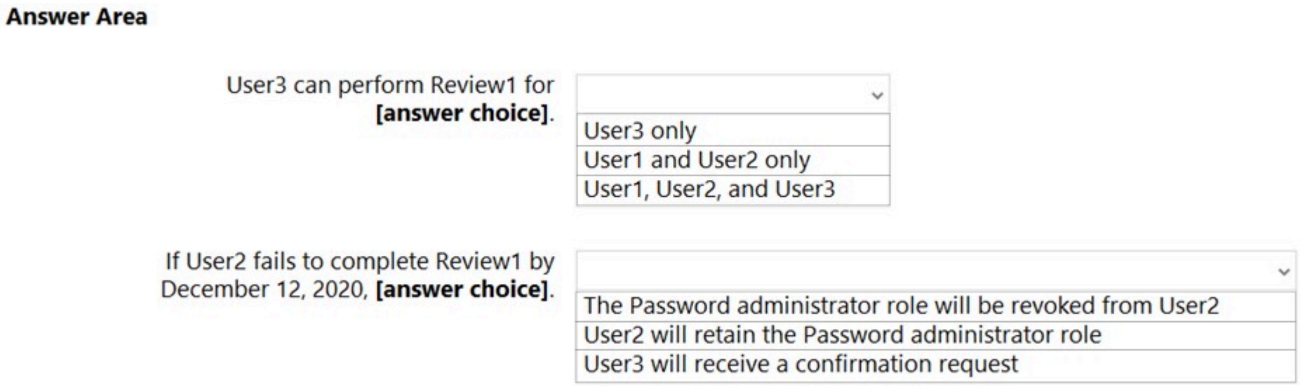
If reviewers don't respond ⓘ: Take recommendations

Advanced settings

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

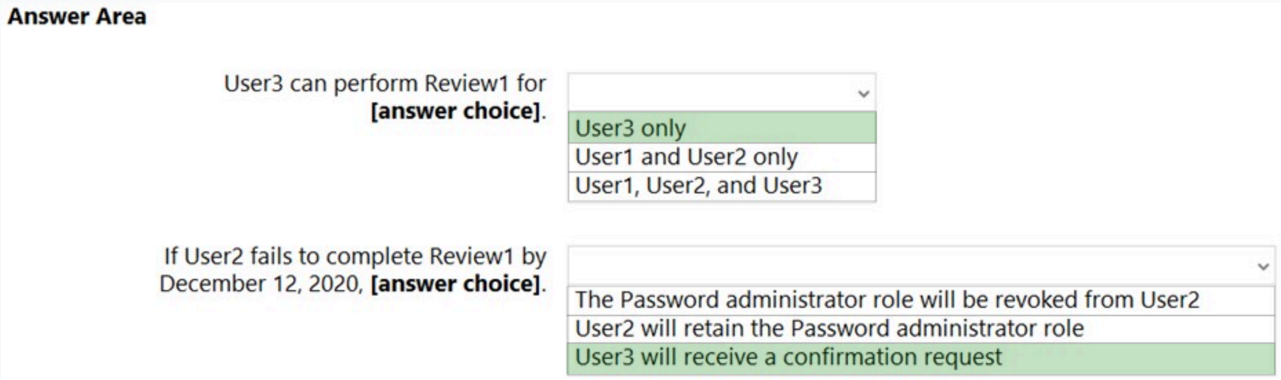
User3 can perform Review1 for **[answer choice]**.

- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by December 12, 2020, **[answer choice]**.

- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Suggested Answer:



Answer Area

User3 can perform Review1 for **[answer choice]**.

- [✓ User3 only]
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by December 12, 2020, **[answer choice]**.

- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- [✓ User3 will receive a confirmation request]

Box 1: User3 only -

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

Reference:

https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review

jantoniocesargatica Highly Voted 3 years, 3 months ago

Hi all. The picture has got some information missing and it is creating a big confusion. The picture is not displaying "The Advanced Settings" where you can decide between retain the passowrd or receive a confirmation. I saw that part of the picture is displayed in older exams. The Advanced Settings has got the option "Email Notification" marked as Enabled, so the answer is "Receive a confirmation request". I saw rhe same question in other webs with the missing information, even in the following link from examtopics where you can see part of the picture:

https://www.examtopics.com/discussions/microsoft/view/46524-exam-az-500-topic-2-question-9-discussion/

upvoted 38 times

fokher 1 year, 5 months ago

thank for this information sir

upvoted 2 times

majstor86 2 years, 3 months ago

exactly

upvoted 1 times

[Removed] Highly Voted 3 years, 6 months ago

1- Correct

2- User2 will retain Password Admin role as it takes system recommendation

upvoted 28 times

siecz 3 years, 3 months ago

"auto apply results to resource" is disabled, so even if the recommendation is to retain password, I believe User3 will get confirmation request

upvoted 8 times

Knighthell Most Recent 3 weeks, 2 days ago

1 correct

2 User2 will retain the Password administrator role

upvoted 1 times

Nhadipour 4 months, 3 weeks ago

As the reviewers set on (self), user 3 has nothing to do with user 2 approval!

So: user 2 will retain the Password administrator role.

upvoted 1 times

saira23 11 months ago

this question was in exam 19/07/2024

upvoted 4 times

sudowhoami 10 months, 3 weeks ago

What's the answer?

upvoted 1 times

maden 10 months, 3 weeks ago

Iam absoulately confused

upvoted 1 times

AZ5002023 1 year, 6 months ago

1- Correct : member itself

2- User2 will retain Password Admin role as it takes system recommendation : because the take recommandations verify the user's sign in in the last 30 days : if the user is innactive since 30 days it will be disabled from his role : so in this case the user is already active because he make authentication bi weekly

upvoted 5 times

wardy1983 1 year, 7 months ago

Explanation:

Box 1: User3 only -

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

Reference:

https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-st art-security-review

upvoted 1 times

wardy1983 1 year, 7 months ago

Box 1: User3 only -

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

upvoted 1 times

⊟ **FedericoBellotti** 2 years, 1 month ago

No words about the money that you ask for this .... incomplete documentation

upvoted 5 times

⊟ **Johnvic** 2 years, 2 months ago

Exam.6 case studies. 3 true/false questions. 47 multiple questions and no simulations. Alot of new questions thats not up here

upvoted 4 times

⊟ **patilsnehal9625** 2 years, 6 months ago

1- Correct

2- User2 will retain Password Admin role as it takes system recommendation

upvoted 2 times

⊟ **blazefather** 2 years, 7 months ago

In exam 31/10/2022

upvoted 6 times

⊟ **Diallo18** 2 years, 8 months ago

In Exam 10/18/2022. One case study, no lab.

upvoted 5 times

⊟ **BlackZeros** 2 years, 9 months ago

User scope is everyone (that includes all password admins)

Reviewer is SELF, user3 with GA access will be able to review

first answer should be user 1, 2 and 3

upvoted 5 times

⊟ **Fal991l** 2 years, 7 months ago

"auto-reply to resource: disable", which means User2 will retain the Password administrator role

upvoted 1 times

⊟ **timHAG** 1 year, 11 months ago

agree, any thoughts, first answer should be all, second answer, missing advance tap details. and should be GA to recive notification

upvoted 1 times

⊟ **vecajif5812k** 3 years, 4 months ago

in exam 01/03/22

upvoted 3 times

⊟ **khengoolman** 3 years, 4 months ago

1-User 3 only

2-User 2 will retain access, since they login every 2 weeks, this is because system recommendation is as follows:

If enabled, system recommends reviewers to deny users who have not signed-in within 30 days. Recommendation accounts for both interactive and non-interactive sign-ins.

This is directly from Access Reviews section in PIM.

upvoted 4 times

⊟ **rodrigo_alx** 3 years, 5 months ago

I agree with Vikku30, anyone have any thoughts?

upvoted 1 times

Question #10 *Topic 2*

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
An administrator named Admin1 has access to the following identities:
✑ An OpenID-enabled user account
✑ A Hotmail account
✑ An account in contoso.com
✑ An account in an Azure AD tenant named fabrikam.com
You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.
To which accounts can you transfer the ownership of Sub1?

A. contoso.com only

B. contoso.com, fabrikam.com, and Hotmail only

C. contoso.com and fabrikam.com only

D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

Suggested Answer: *C*
When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant

Community vote distribution
A (57%) C (43%)

gfhbox0083 Highly Voted 4 years, 12 months ago
C, for sure.
contoso.com and fabrikam.com only
upvoted 46 times

fireb 1 year, 9 months ago
I agree.
upvoted 3 times

milind8451 Highly Voted 4 years, 4 months ago
When you create a new subscription, it's hosted in your account's Azure AD tenant. If you want to give others access to your subscription or its resources, you need to invite them to join your tenant. Hotmail or OpenID are not part of your tenant so these won't get transferred the rights to subscription. Given ans is correct.
upvoted 14 times

Sabr_ Most Recent 2 months, 3 weeks ago
Selected Answer: A
Exam question 6th April 2025
upvoted 2 times

Nhadipour 4 months, 3 weeks ago
Selected Answer: A
Azure subscriptions can only be transferred to an account within the same Azure AD tenant as the subscription. In this case, Sub1 is associated with contoso.com, so the ownership can only be transferred to an account within contoso.com. Even though Admin1 has other accounts, they are irrelevant for the purpose of transferring ownership of Sub1.
upvoted 2 times

Arve 5 months ago
Selected Answer: A
To transfer the ownership of the Azure subscription named Sub1, you can only transfer it to an account that is within the same Azure AD tenant as the subscription. In this case, you can transfer the ownership of Sub1 to the account in contoso.com.

The other accounts (OpenID-enabled user account, Hotmail account, and the account in fabrikam.com) are not eligible for the transfer because they are not within the same Azure AD tenant as Sub1

upvoted 2 times

waqqy 5 months, 1 week ago

Selected Answer: C

C. An account in contoso.com and an account in fabrikam.com.
These are the valid accounts to which ownership of the subscription can be transferred.

upvoted 1 times

TinyTrexArmz 8 months, 3 weeks ago

Selected Answer: C

Azure Account Center has been retired so this question is old. You can transfer subs between two azure tenants though. You do have invite the billing owner to the source tenant and then transfer it to the new account.

upvoted 1 times

Pavel019846457 11 months ago

Selected Answer: C

When you transfer billing ownership of your subscription to an account in another Microsoft Entra tenant, you can move the subscription to the new account's tenant.

https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer#transfer-a-subscription-to-another-microsoft-entra-tenant-account

upvoted 1 times

Jimmy500 11 months, 3 weeks ago

Selected Answer: A

Please always make sure that you have read the condition of the question carefully. In this question, questions asks from us to which account can we transfer the ownership of Subscription-1, it does not tell to where can we transfer the subscription, It asks about changing the ownership of subscription within the Entra ID (now called) this case we need to use contonso only.
A lot of guys say answer is C, please not that it does not asks about transferring subscription to another tenant it just asks about transferring subscription withing existing tenant that is why answer here is A.
Regards,

upvoted 13 times

Jimmy500 1 year ago

I think this is old question

upvoted 1 times

QueZee 1 year, 3 months ago

A. contoso.com only

Here's why:

Azure Account Center Restrictions: Azure Account Center enforces limitations on who can be assigned ownership of Azure resources.

Supported Accounts: Only accounts within the same Azure AD tenant as the subscription can be used for ownership transfer. In this scenario, the relevant tenant is contoso.com (matching Sub1).

upvoted 5 times

> **dc864d4** 1 year, 1 month ago
>
> To clarify: when you say Azure AD, you mean Entra ID, right?
>
> upvoted 1 times

Jkayx94 1 year, 4 months ago

Selected Answer: C

It is possible to move subscription to an account in another tenant:
https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer#transfer-a-subscription-to-another-microsoft-entra-tenant-account

upvoted 2 times

> **Jimmy500** 11 months, 3 weeks ago
>
> Please always make sure that you have read the condition of the question carefully. In this question, questions asks from us to which account can we transfer the ownership of Subscription-1, it does not tell to where can we transfer the subscription, It asks about changing the ownership of

subscription within the Entra ID (now called) this case we need to use contonso only.

A lot of guys say answer is C, please not that it does not asks about transferring subscription to another tenant it just asks about transferring subscription withing existing tenant that is why answer here is A.

Regards,

upvoted 2 times

gen33 1 year, 6 months ago

answer is C YES

upvoted 2 times

yonie 1 year, 6 months ago

Selected Answer: C

The question is to what accounts can it be transferred? Subscription ownership transfer is supported to also other tenants.

upvoted 2 times

Jimmy500 11 months, 3 weeks ago

Please always make sure that you have read the condition of the question carefully. In this question, questions asks from us to which account can we transfer the ownership of Subscription-1, it does not tell to where can we transfer the subscription, It asks about changing the ownership of subscription within the Entra ID (now called) this case we need to use contonso only.

A lot of guys say answer is C, please not that it does not asks about transferring subscription to another tenant it just asks about transferring subscription withing existing tenant that is why answer here is A.

Regards,

upvoted 1 times

flafernan 1 year, 6 months ago

Selected Answer: A

"A "- The ability to transfer ownership is restricted to accounts in the same Azure AD inquiry. Therefore, the transfer of ownership can only be performed for the account associated with contoso.com. So, the correct answer is "A".

upvoted 4 times

flafernan 1 year, 8 months ago

Selected Answer: C

You can transfer ownership of Sub1 to an account in the same Azure AD domain (contoso.com), as well as to an account in another Azure AD domain (fabrikam.com) that is associated with the contoso.com tenant.

Therefore, the correct answer is:

C. contoso.com and fabrikam.com only

You cannot transfer ownership to Hotmail accounts or OpenID accounts.

upvoted 2 times

trashbox 1 year, 8 months ago

Selected Answer: C

Transfer of Subscription to a different MEID Directory is possible.

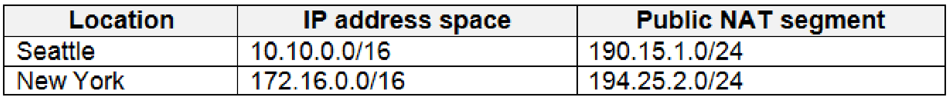
”To make management easier, you might want to transfer a subscription to a different Azure AD directory.”
https://learn.microsoft.com/en-us/azure/role-based-access-control/transfer-subscription

upvoted 2 times

Question #11 *Topic 2*

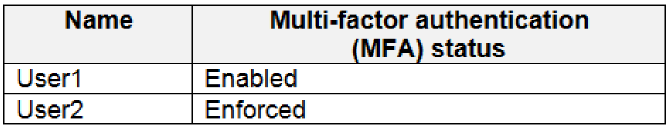
HOTSPOT -

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.



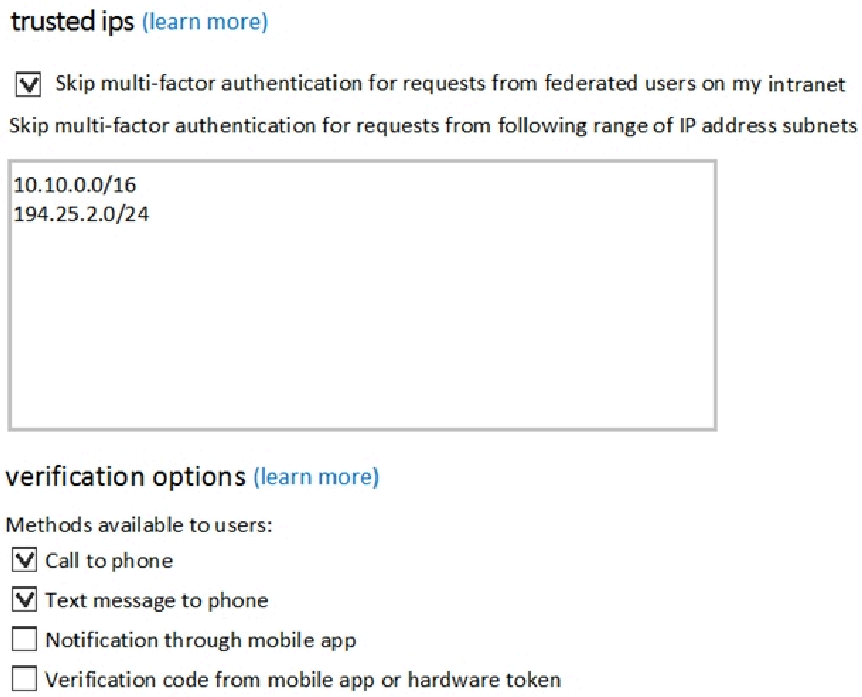
Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)



trusted ips (learn more)

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

```
10.10.0.0/16
194.25.2.0/24
```

verification options (learn more)

Methods available to users:

☑ Call to phone

☑ Text message to phone

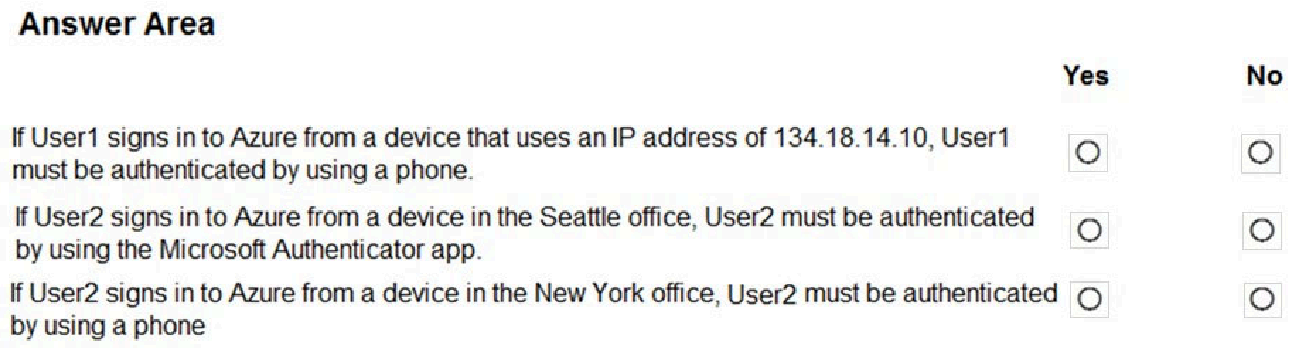
□ Notification through mobile app

□ Verification code from mobile app or hardware token

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

NOTE: Each correct selection is worth one point.

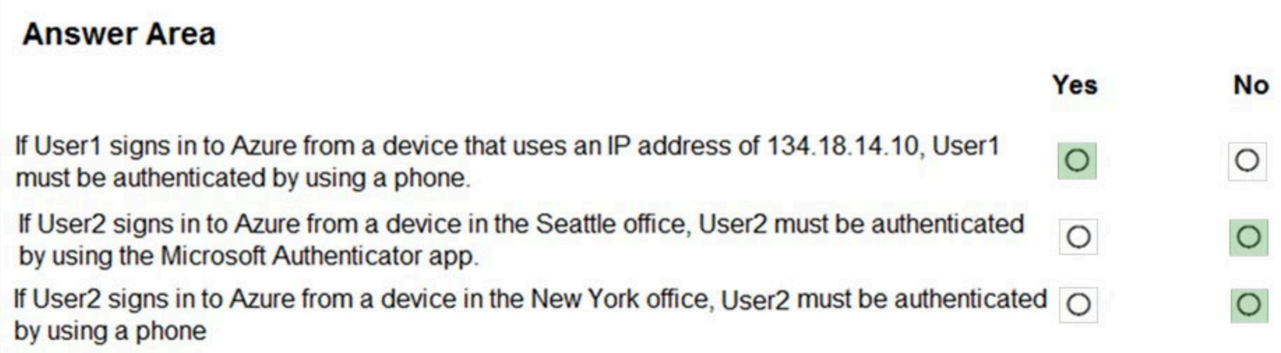
Hot Area:



Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure from a device in the New York office, User2 must be authenticated by using a phone	○	○

Suggested Answer:



Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	●	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	●
If User2 signs in to Azure from a device in the New York office, User2 must be authenticated by using a phone	○	●

Box 1: Yes -

Box 2: No -

Use of Microsoft Authenticator is not required. Either a text or phone call is required for MFA.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No -

The New York IP address subnet is included in the "skip multi-factor authentication for request.

Reference:

https://www.cayosoft.com/difference-enabling-enforcing-mfa/

[Removed] Highly Voted 5 years, 2 months ago

Yes

No

No

right ones

upvoted 90 times

Mea988 2 years, 10 months ago

The first one is a NO: user is enabled for MFA, which means that on next login it will be authenticated using only password, and then he can register its phone for MFA. Hence, NO

upvoted 15 times

Holii 2 years, 1 month ago

This. They wouldn't have listed the MFA status of each user if that didn't have an impact on the answer.

upvoted 2 times

xRiot007 11 months, 2 weeks ago

The question is not talking about subsequent logins, so you don't know if this is the first sign in or not, in which case, you must presume based on the principles of zero trust : device must go through MFA, so the answer is Yes.

upvoted 1 times

chzon 2 years, 4 months ago

you are right. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

upvoted 2 times

durak 3 years, 1 month ago

MFA is not enforced

upvoted 3 times

Aston1818 5 years, 1 month ago

I think its no for the last question as the ip given in the exception is the public NAT one!

upvoted 9 times

gboyega Highly Voted 4 years, 11 months ago

THE CORRECT ANSWER IS

YES

NO

NO

Because in the docs it is stated that
" The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure Multi-Factor Authentication, you can only use public IP address ranges"

In this case the public Ip address is already added to the excluded ips
upvoted 43 times

TheProfessor 1 year, 9 months ago
Why the first one is Yes?

It's MFA is enabled, not enforced.
upvoted 1 times

xRiot007 11 months, 2 weeks ago
Enabled means that legacy authentication is not affected until you finish up registration.
When MFA registration is done, it switches to Enforced.
You can also set Enforced directly.
The end result will always be Enforced MFA.
upvoted 1 times

GaryKing123 1 year, 8 months ago
Because even for user who is in enabled state, when user attempts to sign in next it will require user to complete MFA registration. So they still need to use mobile device to sign in even when enabled. Once they complete registration, MFA becomes enforced

"The user is enrolled per-user in Microsoft Entra multifactor authentication. If the user hasn't yet registered authentication methods, they receive a prompt to register the next time they sign in using modern authentication (such as via a web browser). Users who complete registration while in the Enabled state are automatically moved to the Enforced state"
upvoted 4 times

OpsecDude 2 years, 9 months ago
Yes that is true, but notice that Seattle Office subnet was not included in the list of Whitelisted IP's, although MS Authenticator App was unchecked in the menu so the correct answer is NO. If it had been "User must authenticate using their phone" then it would have been a yes.
upvoted 4 times

wannasruls 1 year, 5 months ago
but the first question is asking "user to authenticate using phone". So you're saying it's a yes?
upvoted 1 times

Knighthell Most Recent 3 weeks, 2 days ago
No
No
YES

"Skip MFA for trusted IPs applies only to users with MFA status 'Enabled'. Users with MFA status 'Enforced' will always be prompted for MFA even when connecting from trusted IPs."
upvoted 1 times

Yvesk 3 months ago
YNY - Trusted IPs do not override an enforced MFA requirement.
upvoted 1 times

qwerjj 11 months ago
Could I know why the question#2 is No? I guess only the NAT IP is approved now, so it means the NAT access from Seattle has not been approved.
upvoted 1 times

in_da_cloud 1 year, 4 months ago
no no no: Mea988 is right!
The first one is a NO: user is enabled for MFA, which means that on next login it will be authenticated using only password, and then he can register its phone for MFA. Hence, NO
upvoted 1 times

xRiot007 11 months, 2 weeks ago

There is no such thing as a "next" login nowhere in that question. Answer is Yes

upvoted 2 times

Ivan80 1 year, 5 months ago

In exam 1/28/24

upvoted 5 times

ITSystem 1 year, 3 months ago

what is your answer ?

upvoted 2 times

AZ5002023 1 year, 6 months ago

No : mfa enabled not enforced

No : MS authent not autorised : only phone mfa

No : the ip is bypassed

upvoted 2 times

JunetGoyal 1 year, 8 months ago

Yes, 134.x.x.x is not trusted ip

no. Ms app is not a checked option in mfa option, only phonw is listed

No. As New york location is not a trusted ip

upvoted 2 times

trashbox 1 year, 8 months ago

1. "No": User 1's MFA status is Enabled, so the use of MFA is not enforced
2. "No": MS Authenticator app is not included in the available MFA options
3. "No": MFA is skipped because New York's Public NAT segment is included in Trusted IPs

upvoted 5 times

Rachy 1 year, 10 months ago

This is current. 28/08/23

upvoted 4 times

ESAJRR 1 year, 11 months ago

Yes

No

No

upvoted 1 times

Qadour 2 years ago

Yes - No - Yes !

Why 3 = Yes ? because we have User2 trying to connect from New York OFFICE !

In the table of Whitelisted IP's we have the public IP of the NY Office

upvoted 4 times

zellck 2 years, 1 month ago

YNN is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#azure-ad-multi-factor-authentication-user-states

- Enabled

The user is enrolled in per-user Azure AD Multi-Factor Authentication, but can still use their password for legacy authentication. If the user hasn't yet registered MFA authentication methods, they receive a prompt to register the next time they sign in using modern authentication (such as via a web browser).

upvoted 7 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 3 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips

The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Azure AD Multi-Factor Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

upvoted 1 times

⊟ **Gesbie** 2 years, 2 months ago

In Exam April 11, 2023

upvoted 4 times

⊟ **majstor86** 2 years, 3 months ago

Yes

No

No

upvoted 3 times

⊟ **stepman** 2 years, 2 months ago

On exam Apr 27, 2023

upvoted 2 times

⊟ **003nickm** 2 years, 4 months ago

On 2-March-2023, I passed AZ-500 with flying color. This question was in the exam. Some question was on Defender EASM as well.

upvoted 3 times

Question #12 *Topic 2*

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments.
What should you use?

A. Azure Security Center

B. Azure Policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure Blueprints

Suggested Answer: *D*
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
✑ Role Assignments
✑ Policy Assignments
✑ Azure Resource Manager templates
✑ Resource Groups
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

Community vote distribution

D (100%)

⊟ **Prash85** Highly Voted 4 years, 1 month ago
Azure Blueprint is the correct answer
upvoted 17 times

⊟ **Atanu** Highly Voted 4 years, 5 months ago
Conflict with Question 13. Same question .. but two different answers...Which one to go with?
upvoted 7 times

> ⊟ **DA0410** 3 years, 7 months ago
> Good observation. If I am not wrong , Q13 answer should be blueprint.
> upvoted 2 times
>
> ⊟ **P4YDAY** 4 years, 5 months ago
> Azure Blueprint is the correct answer for both question.
> upvoted 33 times

⊟ **ESAJRR** Most Recent 11 months, 1 week ago
Selected Answer: D
D. Azure Blueprints
upvoted 1 times

⊟ **majstor86** 1 year, 3 months ago
Selected Answer: D
D. Azure Blueprints
upvoted 1 times

⊟ **F117A_Stealth** 1 year, 7 months ago
Selected Answer: D
Azure Blueprint is the correct answer
upvoted 1 times

⊟ **OpsecDude** 1 year, 9 months ago
Selected Answer: D

Blueprints all the way

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

Blueprints set policy at root mgmt level, which manages subscriptions.

upvoted 1 times

AS179 2 years, 6 months ago

D is correct

upvoted 1 times

rohitmedi 2 years, 7 months ago

correct answer

upvoted 1 times

justinp 2 years, 11 months ago

this question is present in test today

upvoted 1 times

Deepmindx 3 years ago

### IN EXAM ### 29/6/2021

upvoted 4 times

teehex 3 years, 1 month ago

Correct Answer is D - Azure Blueprints. You can create a blueprint at Management Group which contains two subscriptions and deploy it to both.

upvoted 3 times

bimbokeem 3 years, 1 month ago

question 12 is not conflicting with question 13 please. not in anyway that i know

upvoted 2 times

teamaws 3 years, 2 months ago

for sure, D

upvoted 2 times

seconazure 3 years, 4 months ago

Absolutely D.

Azure Blueprint

upvoted 4 times

milind8451 3 years, 4 months ago

Blueprint is right ans.

upvoted 1 times

zic04 3 years, 5 months ago

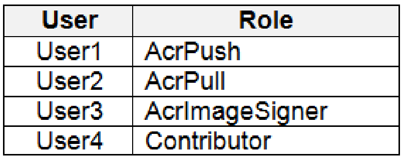
Blueprint good

upvoted 1 times

HOTSPOT -

You have an Azure Container Registry named Registry1.

You add role assignments for Registry1 as shown in the following table.

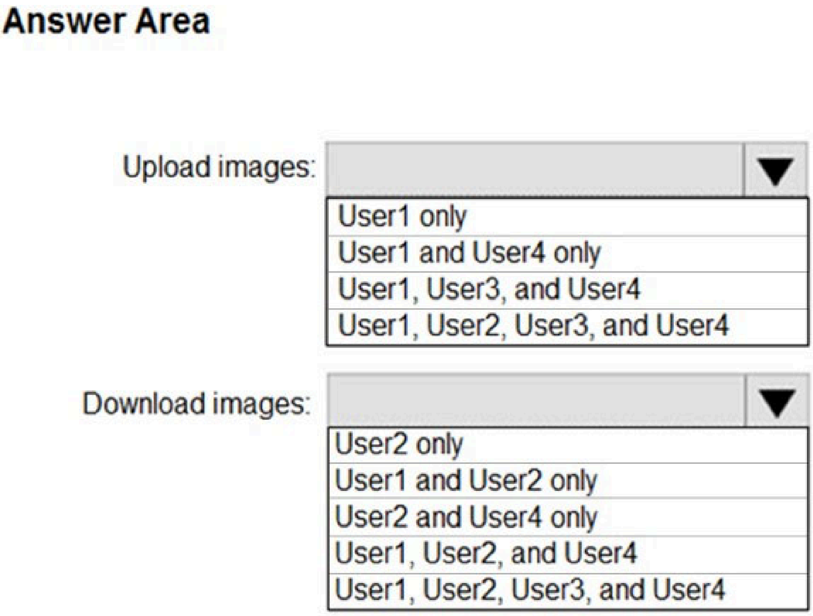


User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

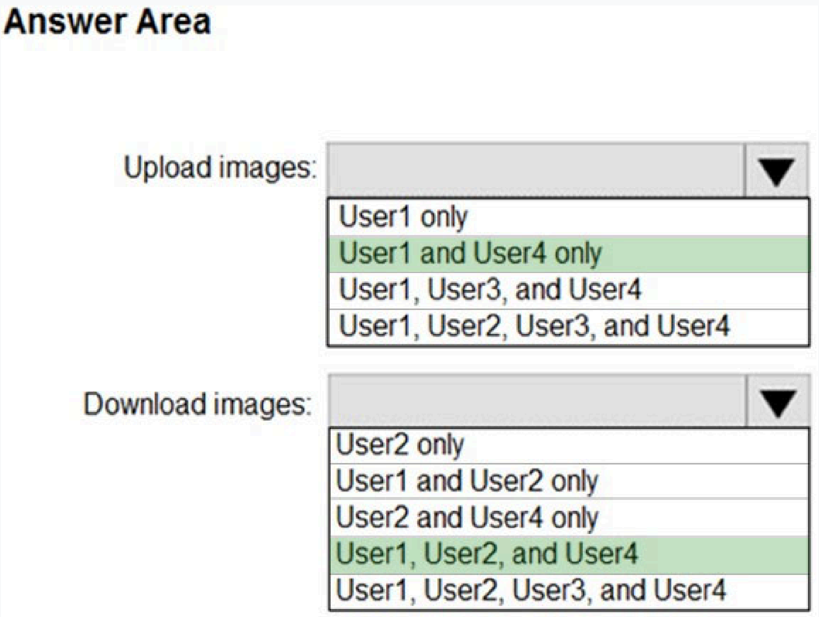


Answer Area

Upload images: ▼
- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

Download images: ▼
- User2 only
- User1 and User2 only
- User2 and User4 only
- User1, User2, and User4
- User1, User2, User3, and User4

Suggested Answer:



Answer Area

Upload images: ▼
- User1 only
- [✓ User1 and User4 only]
- User1, User3, and User4
- User1, User2, User3, and User4

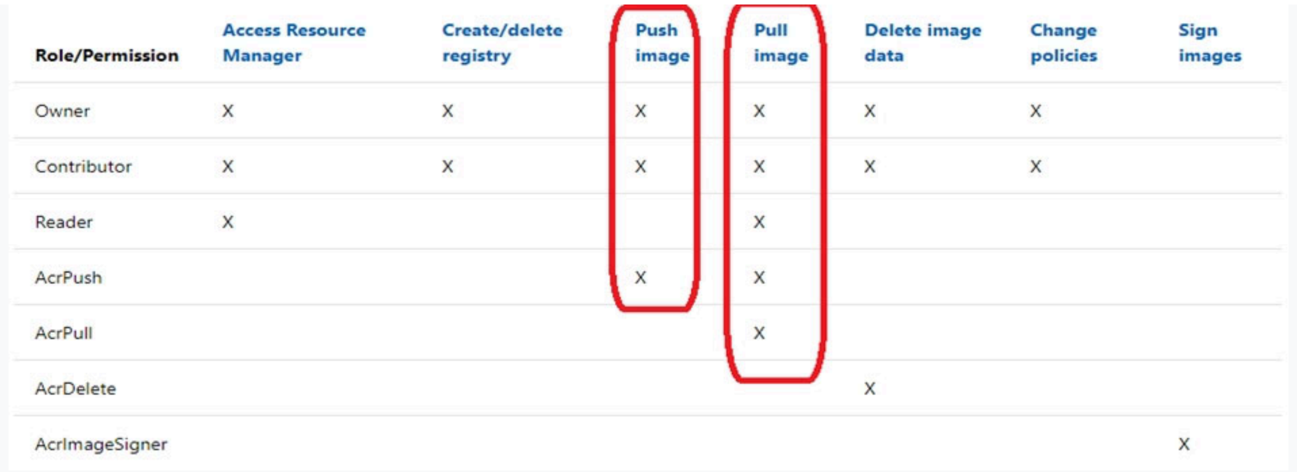
Download images: ▼
- User2 only
- User1 and User2 only
- User2 and User4 only
- [✓ User1, User2, and User4]
- User1, User2, User3, and User4

Box 1: User1 and User4 only -

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4 -

All, except AcrImagineSigner, can download/pull images.



Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

Reference:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

rawrkadia Highly Voted 3 years, 4 months ago

Listed is clearly correct per documentation.

1: User 1/4

2: User 1/2/4

upvoted 30 times

Giritharram Highly Voted 3 years, 5 months ago

Arcpush and contributor can Upload and download

Arcpull can only download

Arcimagesigner can only sign the images

upvoted 22 times

ITFranz Most Recent 7 months, 2 weeks ago

Here the support link for the answer:

https://learn.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli

Box 1. user 1-4

Box 2. user 1-2-4

upvoted 1 times

khaled_razouk 9 months ago

Q1: user 1 & user 4

Q2: user 2 & user 4

upvoted 2 times

khaled_razouk 9 months ago

after going to the Microsoft documentation the answer on the question is correct so it's

1/4

1/2/4

upvoted 2 times

Obama_boy 1 year ago

in exam 08/12/2023

upvoted 2 times

wardy1983 1 year, 1 month ago

Explanation:

Box 1: User1 and User4 only -

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4 -

All, except AcrImagineSigner, can download/pull images.

upvoted 1 times

trashbox 1 year, 2 months ago

Upload: AcrPush & Contributor

Download: AcrPush, AcrPull, & Contributor

The question was given on the October 9, 2023 exam.

upvoted 3 times

alfaAzure 1 year, 4 months ago

I believe it is.

1. User 1&4
2. User 2&4

upvoted 3 times

zellck 1 year, 7 months ago

1. User1 and User4 only
2. User1, User2, and User4

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles

upvoted 3 times

Gesbie 1 year, 8 months ago

In Exam April 11, 2023

upvoted 7 times

majstor86 1 year, 10 months ago

1: Users 1 & 4 can upload

2: Users 1, 2 & 4 can download.

upvoted 2 times

F117A_Stealth 2 years, 1 month ago

Answers are correct.

User 1 & 4 can upload

User 1, 2 & 4 can download.

upvoted 2 times

mickie2 2 years, 2 months ago

In EXAM today, I think the premium file was worth it after all. Correct Answer.

upvoted 2 times

> **bibhu14** 2 years, 2 months ago
>
> Hi , Could you please help me with the premium file
>
> upvoted 1 times

Eltooth 2 years, 9 months ago

Answers are correct.

User 1 & 4 can upload

User 1, 2 & 4 can download.

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli

upvoted 1 times

TJ001 2 years, 11 months ago

correct answer

upvoted 1 times

LDodge 3 years ago

Correct.

Upload images= User 1, User 4.

Download images= User 1, User 2, User 4

upvoted 2 times

rohitmedi 3 years, 1 month ago

correct answer

upvoted 2 times

Question #14 Topic 2

You have an Azure subscription.
You create an Azure web app named Contoso1812 that uses an S1 App Service plan.

You plan to -
create a CNAME DNS record for www.contoso.com that points to Contoso1812.
You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Turn on the system-assigned managed identity for Contoso1812.

B. Add a hostname to Contoso1812.

C. Scale out the App Service plan of Contoso1812.

D. Add a deployment slot to Contoso1812.

E. Scale up the App Service plan of Contoso1812.

F. Upload a PFX file to Contoso1812.

Suggested Answer: *BF*
B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).
To do this, you have to create three records:
A root "A" record pointing to contoso.com
A root "TXT" record for verification
A "CNAME" record for the www name that points to the A record
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
Reference:
https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

Community vote distribution
BF (100%)

⊟ **Orel123** Highly Voted 2 years, 3 months ago
B. Add a hostname to Contoso1812.
F. Upload a PFX file to Contoso1812.

Explanation:
B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it
using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN). To do this, you have to create three records:
A root "A" record pointing to contoso.com
A root "TXT" record for verification
A "CNAME" record for the www name that points to the A record
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
References: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-
domain
upvoted 49 times

⊟ **cfsxtuv33** 2 years ago
Great explanation...thank you!
upvoted 5 times

⊟ **sieira** 1 year, 11 months ago
Yes. Great explanation. Thanks
upvoted 2 times

FelipeBarbosa Highly Voted 2 years, 9 months ago

In the exam, correct answer.

upvoted 18 times

Andre369 Most Recent 7 months, 1 week ago

Selected Answer: BF

B. Add a hostname to Contoso1812: This involves adding the hostname "www.contoso.com" to the web app's custom domains. This can be done through the Azure portal or via PowerShell/CLI commands.

F. Upload a PFX file to Contoso1812: To enable HTTPS for the custom domain, you need to upload a PFX certificate to the web app. This certificate will be used to secure the HTTPS connection for the www.contoso.com URL.

upvoted 3 times

majstor86 10 months ago

Selected Answer: BF

B. Add a hostname to Contoso1812.

F. Upload a PFX file to Contoso1812.

upvoted 2 times

sofieejo 11 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 1 times

edurakhan 1 year, 1 month ago

On exam today - 11/19/22 - passed

A lot of questions about Sentinel

upvoted 2 times

VaishaliJ 1 year, 1 month ago

#Exam Question# 8th Nov 2022

upvoted 1 times

Mea988 1 year, 4 months ago

Selected Answer: BF

Correct

upvoted 1 times

Sweet_co 1 year, 5 months ago

On the exam: 20/7/2022

upvoted 1 times

acexyz 1 year, 6 months ago

# IN EXAM - 30/6/2022

upvoted 1 times

luupux 1 year, 6 months ago

Selected Answer: BF

B. Add a hostname to Contoso1812.

F. Upload a PFX file to Contoso1812

upvoted 1 times

alou333 1 year, 6 months ago

# IN EXAM - 3/6/2022 (online).

Lot of new questions. Good luck !

upvoted 2 times

Eltooth 1 year, 9 months ago

Selected Answer: BF

B and F are correct.

upvoted 1 times

LDodge 2 years ago

Selected Answer: BF

Correct- B and F

upvoted 3 times

⊟ **rohitmedi** 2 years, 1 month ago

correct answer

upvoted 2 times

⊟ **orallony** 2 years, 3 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 5 times

⊟ **Mcgood** 2 years, 5 months ago

B and F are Correct

upvoted 1 times

Question #15 *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 named Sub1.
You have an Azure Storage account named sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to sa1.
Solution: You create a lock on sa1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
Reference:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

Community vote distribution

B (100%)

kristiann21 Highly Voted 5 years ago
Correct Answer.
upvoted 18 times

gfhbox0083 Highly Voted 4 years, 12 months ago
B, for sure
upvoted 9 times

kiketxu 4 years, 9 months ago
Agree with you. it must be a NO, because any lock doesn't revoke the access.
upvoted 3 times

saira23 Most Recent 11 months ago
this question was in exam 19/07/2024
upvoted 1 times

Ivan80 1 year, 5 months ago
In exam 1/28/24
upvoted 2 times

trashbox 1 year, 8 months ago
Selected Answer: B
The question was given on the October 9, 2023 exam.
upvoted 3 times

Andre369 2 years, 1 month ago
Selected Answer: B
No, creating a lock on the Azure Storage account (sa1) will not revoke access to the blob service and file service. Locks in Azure are used to prevent accidental deletion or modification of resources, but they do not control access to the services or resources within a storage account. To revoke access to the blob service and file service, you would need to invalidate or delete the shared access signatures (SASs) and stored access policies that grant access to unauthorized users.
upvoted 7 times

Bennour 2 years, 1 month ago

Lock allows users to lock an Azure resource to prevent accidental deletion or modification of the resource. It does not prevent users from accessing the resource. A is a bad answer

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy#modify-or-revoke-a-stored-access-policy
To revoke a stored access policy, you can delete it, rename it by changing the signed identifier, or change the expiry time to a value in the past. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Changing the expiry time to a value in the past causes any associated signatures to expire. Deleting or modifying the stored access policy immediately affects all of the shared access signatures associated with it.

upvoted 4 times

Gesbie 2 years, 2 months ago

In Exam April 11, 2023

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: B

B: NO is correct answer.

upvoted 1 times

003nickm 2 years, 4 months ago

On 2-March-2023, I passed AZ-500 with flying color. This question was in the exam. Some question was on Defender EASM as well.

upvoted 2 times

F117A_Stealth 2 years, 7 months ago

Selected Answer: B

A lock wont work.

No is correct

upvoted 1 times

Diallo18 2 years, 8 months ago

In Exam 10/18/2022. One case study, no lab.

upvoted 1 times

Exams_Prep_2021 3 years ago

In Exam - 20/6/2022 - 1 Case Study (6) - Lab (10 Tasks)

upvoted 2 times

luupux 3 years ago

Selected Answer: B

Correct Answer.

upvoted 1 times

NobleVarghese 3 years ago

Selected Answer: B

Lock doesn't remove access. Lock prevents delete

upvoted 3 times

NobleVarghese 3 years ago

In exam June 09 2022

upvoted 2 times

Question #16 *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 a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
✑ Create Azure Virtual Network.
✑ Create a custom DNS server in the Azure Virtual Network.
✑ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
✑ Configure forwarding between the custom DNS server and your on-premises DNS server.
Reference:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

Community vote distribution

A (62%) B (38%)

Adamasbue Highly Voted 5 years, 1 month ago
Wrong: https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture
upvoted 36 times

PlasticMind 5 years ago
Azure AD domain Services is the only supported way for HD Insight cluster integration integration with active directory. so AAD connect to synchronise identities from an on-premises active directory to Azure AD and then Azure AD domain services for the HD Insights integration
upvoted 20 times

ochiwi 4 years, 8 months ago
i agree since there's indication that a setup of an Azure AD exists which is a requirement for HD insight, should work...
upvoted 2 times

MKnight25 1 year, 12 months ago
I agree a well, becaus:
!Using on-premises Active Directory or Active Directory on IaaS VMs alone, without Azure AD and Azure AD DS, isn't a supported configuration for HDInsight clusters with ESP.
https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture#on-premises-active-directory-or-active-directory-on-iaas-vms
upvoted 3 times

BTAB 3 years ago
@Adamasbue is correct. From that URL it states: If HDInsight and Azure AD DS are deployed in the same virtual network, the connectivity is automatically provided, and no further action is needed.

The question details that AADDS will be deployed to the Azure subscription. There is still ambiguity in the question, because it doesn't say that AADDS is deployed within the same virtual network of HDInsight.

These questions kill me.
upvoted 15 times

Hemn1990 Highly Voted 4 years, 5 months ago

You have hybrid enviroment so AD DS is alredy in place, you would need site to site vpn so the answer is no.

upvoted 29 times

TJ001 2 years, 11 months ago

Hybrid does not mean AADDS is in place .. it could be just AD connect + hash synch is always have to be separately enable based on the sync method

upvoted 13 times

Lucabrazi999 1 year, 3 months ago

and where would the hash be originally gotten from?

upvoted 2 times

ITFranz Most Recent 6 months ago

Selected Answer: A

To support the answer:

Yes, deploying Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription can be a solution to allow users to authenticate to the HDInsight cluster using their on-premises Active Directory credentials. Here's why:

1. Azure AD DS provides a managed domain service that is compatible with traditional Active Directory Domain Services
2. It enables one-way synchronization from Azure AD to the managed domain, allowing access to a central set of users, groups, and credentials
3. For hybrid environments with on-premises AD, Azure AD Connect can be used to synchronize identity information with Azure AD, which then synchronizes with Azure AD DS
4. This setup allows users to log in to services and applications connected to the managed domain using their existing credentials

Set up different domain controllers

Answer = A

upvoted 2 times

JaridB 7 months ago

Selected Answer: B

Answer: No

According to the Microsoft documentation you referenced, connecting an Azure HDInsight cluster directly to an on-premises Active Directory (AD) domain is not supported.

Therefore, the correct answer to the question "You need to configure the environment to support the planned authentication." is No. Deploying Azure Active Directory Domain Services (Azure AD DS) does not directly meet the goal of allowing users to authenticate to the HDInsight cluster using their on-premises AD credentials.

upvoted 2 times

Jarid 9 months, 1 week ago

Yes, deploying Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription meets the goal of allowing users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials in a hybrid Azure AD configuration.

Azure AD DS provides managed domain services such as domain join, group policy, LDAP, and Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory. By integrating Azure AD DS with your Azure HDInsight cluster on a virtual network, you can leverage these domain services to enable seamless authentication using on-premises Active Directory credentials. This setup allows users to access the HDInsight cluster with their existing credentials, facilitating a smoother and more secure integration between on-premises and cloud resources.

This approach is particularly effective in hybrid environments where organizations wish to extend their on-premises identity infrastructure to Azure services, ensuring that authentication and access control are centrally managed.

upvoted 3 times

flafernan 1 year ago

Selected Answer: A

Currently, HDInsight only supports Microsoft Entra Domain Services as the primary domain controller that the cluster uses for Kerberos communication. But other complex Active Directory configurations are possible, as long as such configuration leads to enabling Microsoft Entra Domain Services for access to HDInsight.

upvoted 1 times

Jkayx94 1 year, 1 month ago

A VPN is required. By Using AD DS, this will convert the AAD Synced (or now Entra ID) synced entities into a one-way sync to AAD DS. But this isn't using the local on-prem account. This is using the Microsoft Hybrid Section of the account. (i.e. AD DS maybe contoso.local, but Entra ID will be contoso.com. AD DS will be Contoso.com (or whatever domain you select when you set it up). It's asking to use the on-prem account (contoso.local), not a converted Microsoft account.

upvoted 2 times

Jkayx94 1 year, 1 month ago

I suspect the Answer is B, but the question is worded incorrect. The answer suggests the HDInsight is on-Prem rather than the original question reporting it's in cloud.

upvoted 1 times

wardy1983 1 year, 1 month ago

Answer: A

Explanation:

Azure Active Directory Domain Services

Azure AD DS provides a managed domain that's fully compatible with Windows Server Active Directory. Microsoft takes care of managing, patching, and monitoring the domain in a highly available (HA) setup. You can deploy your cluster without worrying about maintaining domain controllers. Users, groups, and passwords are synchronized from Azure AD. The one-way sync from your Azure AD instance to Azure AD DS enables users to sign in to the cluster by using the same corporate credentials.

upvoted 1 times

Sujeeth 1 year, 3 months ago

Yes is answer, deploying Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription can meet the goal of allowing users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials. Azure AD DS provides the capability to extend your on-premises Active Directory to Azure, allowing seamless authentication for resources hosted in Azure, including HDInsight clusters

upvoted 3 times

_fvt 1 year, 5 months ago

Selected Answer: A

Correct answer is A - YES.

You don't need a VPN with OnPrem to connect to HDInsights. It would be relevant if you need connection between HDInsights and onPrem servers and/or want to remove/restric public traffic.

HDIsights can be accessed from internet no matters of the authentication method.

https://learn.microsoft.com/en-us/azure/hdinsight/hdinsight-virtual-network-architecture

Now you want to connects HDI with on-prem AD DS identities.

The only supported way is to use Azure AD DS (An Azure Service, different from your onprem AD DS).

Azure AD DS needs AD connect with PHS from On-Prem AD DS to Azure AD. You are in Hybrid config so already setup AD Connects.

Azure AD DS is deplpoyed in a VNEt and needs to be Perred with HDInsights VNet. That's it.

https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-create-configure-enterprise-security-cluster

upvoted 2 times

> **_fvt** 1 year, 5 months ago
>
> The the peering to relevant VNets is a part of the Azure AD DS Deployment.
>
> upvoted 1 times

kieli 1 year, 6 months ago

https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture If PHS is confirmed to be configured and Azure ADDS can be reached it will do the work. So I would go for NO on these basis and not that it needs to be connected via VPN.

upvoted 1 times

Dev1079 1 year, 6 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure-adds

upvoted 2 times

Andre369 1 year, 7 months ago

Selected Answer: A

Yes, deploying Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription would meet the goal of allowing users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials. Azure AD DS provides managed domain services that can be used to join HDInsight clusters to an Azure AD DS-managed domain. This allows users to authenticate using their on-premises AD credentials seamlessly. Therefore, the solution meets the goal.

upvoted 2 times

⊟ **billo79152718** 1 year, 7 months ago

A: YES

upvoted 2 times

⊟ **majstor86** 1 year, 9 months ago

Selected Answer: A

A. Yes

upvoted 3 times

⊟ **yassou_123** 2 years ago

Selected Answer: B

answer should be No, it must use VPN

source:https://learn.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

upvoted 5 times

Question #17 *Topic 2*

Your network contains an Active Directory forest named contoso.com. You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.
You need to identify which roles and groups are required to perform the planned configuration. The solution must use the principle of least privilege.
Which two roles and groups should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Domain Admins group in Active Directory

B. the Security administrator role in Azure AD

C. the Global administrator role in Azure AD

D. the User administrator role in Azure AD

E. the Enterprise Admins group in Active Directory

Suggested Answer: *CE*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

Community vote distribution
CE (85%) CD (15%)

Solanki Highly Voted 5 years, 1 month ago
Correct Answer as per provided link.
In Express settings, the installation wizard asks for the following:

AD DS Enterprise Administrator credentials
Azure AD Global Administrator credentials
upvoted 44 times

gfhbox0083 Highly Voted 5 years ago
C, E, for sure.
Role ==> Global administrator
Group ==> Enterprise Admins
upvoted 16 times

TinyTrexArmz Most Recent 8 months, 3 weeks ago
Selected Answer: CE
You must have a Microsoft Entra Global Administrator account or Hybrid Identity Administrator account for the Microsoft Entra tenant you want to integrate with. This account must be a school or organization account and can't be a Microsoft account.

If you use express settings or upgrade from DirSync, you must have an Enterprise Administrator account for your on-premises Active Directory.

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-install-prerequisites
upvoted 2 times

pentium75 11 months ago
Selected Answer: CE
Global Administrator and Enterprise Admin are required FOR THE SETUP. For operation it will use less-privileged accounts.
upvoted 1 times

f82411e 1 year, 4 months ago
Correct
upvoted 1 times

d3N 1 year, 10 months ago
Answers are correct.
Note that with version 2.X of AD Connect, Global administrator can be replaced with Hybrid Identity Administrator role.

upvoted 3 times

ESAJRR 1 year, 11 months ago

Selected Answer: CE

C. the Global administrator role in Azure AD

E. the Enterprise Admins group in Active Directory

upvoted 1 times

Andre369 2 years, 1 month ago

Selected Answer: CD

To perform the planned configuration using the Express Settings installation option in Azure AD Connect, you should identify the following roles and groups:

C. The Global administrator role in Azure AD: This role is required to perform the initial configuration of Azure AD Connect and manage the synchronization process between on-premises Active Directory and Azure AD.

D. The User administrator role in Azure AD: This role is required to manage user accounts and their attributes in Azure AD. It is necessary for the synchronization process to create and update user accounts in Azure AD based on the on-premises Active Directory.

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: CE

C. the Global administrator role in Azure AD

E. the Enterprise Admins group in Active Directory

upvoted 2 times

F117A_Stealth 2 years, 7 months ago

Selected Answer: CE

CE without any doubts

upvoted 1 times

feln 3 years, 1 month ago

Selected Answer: CE

correct

upvoted 1 times

Eltooth 3 years, 3 months ago

Selected Answer: CE

C and E are correct.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions#express-settings-installation

upvoted 2 times

Patchfox 3 years, 6 months ago

This question is no longer valid when you use Azure ADConnect Version 1.4 or above: As of build 1.4.###.# it is no longer supported to use an enterprise admin or a domain admin account as the AD DS Connector account.

upvoted 5 times

> **WMG** 3 years, 2 months ago
>
> That is not what the question is asking. The question and answers are still correct as of March 2022.
>
> upvoted 2 times
>
> **BTAB** 3 years, 6 months ago
>
> Agreed, this question is outdated. I found the *Important Note below at the same URL listed in the answer: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions
>
> As of build 1.4.###.# it is no longer supported to use an enterprise admin or a domain admin account as the AD DS Connector account. If you attempt to enter an account that is an enterprise admin or domain admin when specifying use existing account, you will receive an error.
>
> upvoted 2 times
>
> > **Daan14** 3 years, 5 months ago
> >
> > True but you still need it for the setup
> >
> > upvoted 4 times

AS179 3 years, 6 months ago

Selected Answer: CE

correct

upvoted 3 times

⊟ **rohitmedi** 3 years, 7 months ago

correct answer

upvoted 1 times

⊟ **orallony** 3 years, 9 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 5 times

⊟ **Sandomj55** 3 years, 10 months ago

In Exam 8/4/2021

upvoted 3 times

Question #18 *Topic 2*

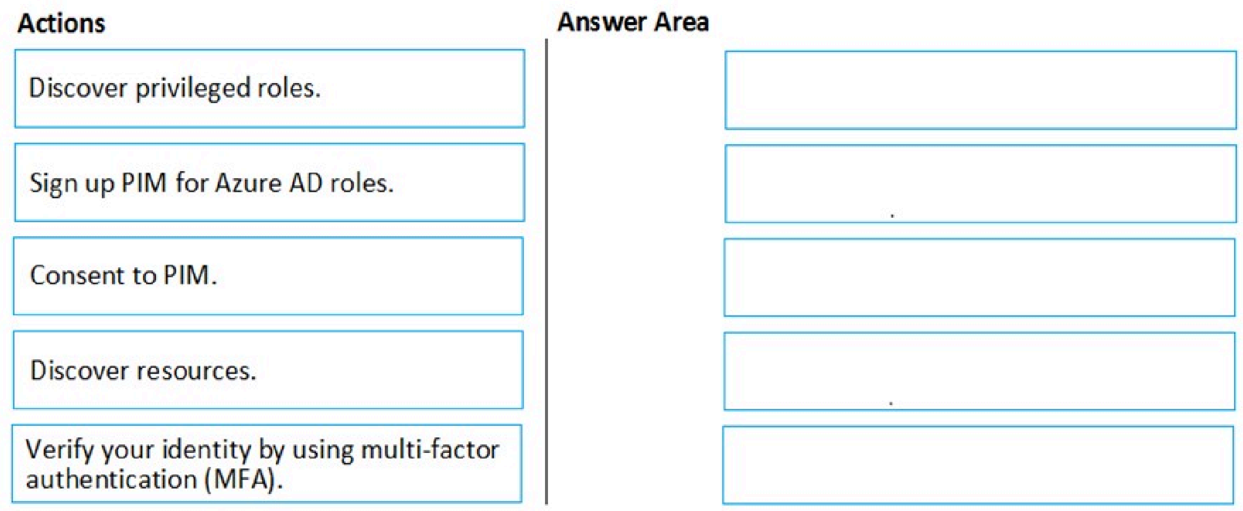
DRAG DROP -

You create an Azure subscription with Azure AD Premium P2.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

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:

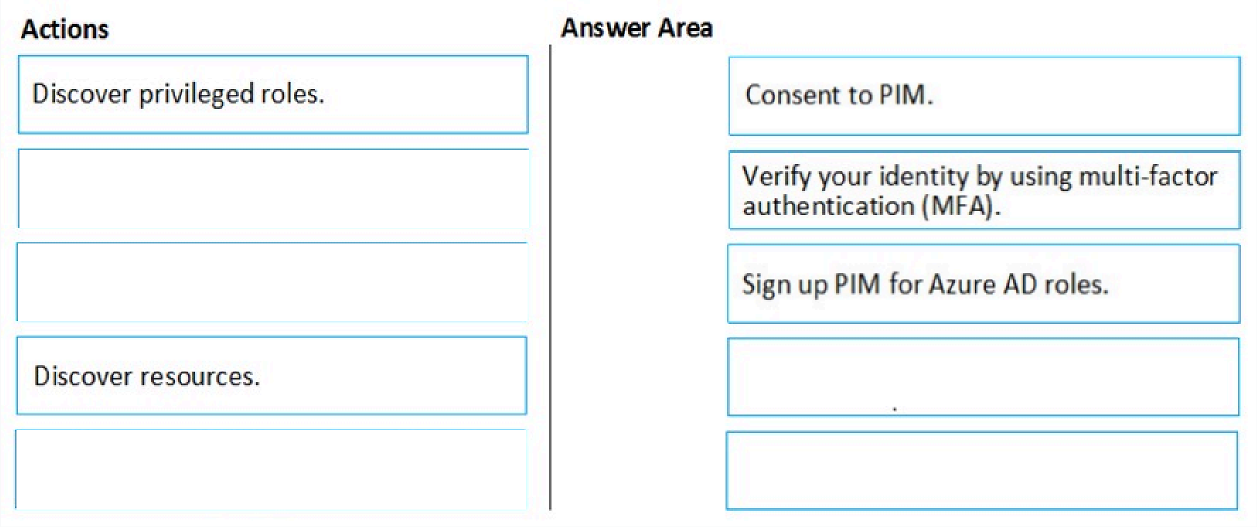


Actions

- Discover privileged roles.
- Sign up PIM for Azure AD roles.
- Consent to PIM.
- Discover resources.
- Verify your identity by using multi-factor authentication (MFA).

Answer Area

Suggested Answer:

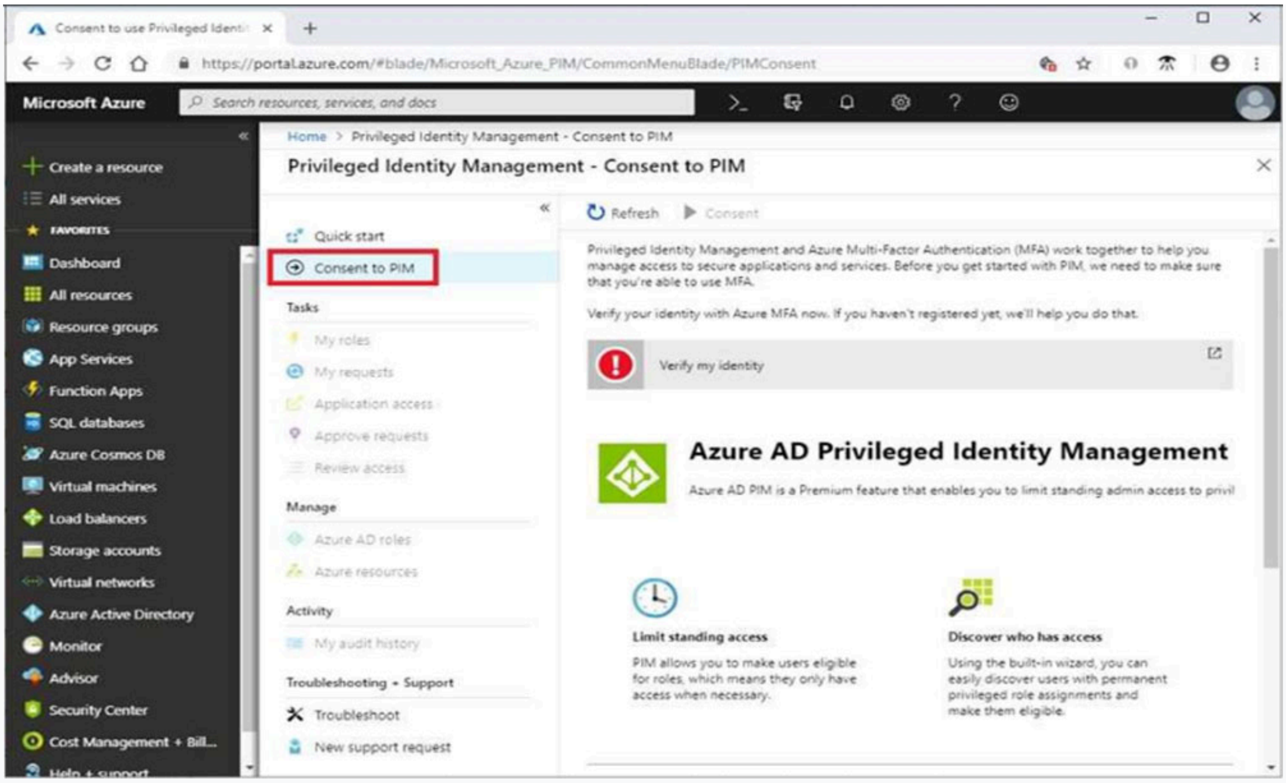


Actions

- Discover privileged roles.
- Discover resources.

Answer Area

- Consent to PIM.
- Verify your identity by using multi-factor authentication (MFA).
- Sign up PIM for Azure AD roles.



Privileged Identity Management and Azure Multi-Factor Authentication (MFA) work together to help you manage access to secure applications and services. Before you get started with PIM, we need to make sure that you're able to use MFA.

Verify your identity with Azure MFA now. If you haven't registered yet, we'll help you do that.

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privil

PIM allows you to make users eligible for roles, which means they only have access when necessary.

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.

Step: 2 Verify your identity by using multi-factor authentication (MFA)

Click Verify my identity to verify your identity with Azure MF

You'll be asked to pick an account.

Step 3: Sign up PIM for Azure AD roles

Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.

⊟ **somenick** Highly Voted 2 years, 9 months ago

Admins, I know that 20$ for this content is much less than 120$ for Test King answers, but you are not removing outdated questions even after 1 year. WTF?!

upvoted 37 times

⊟ **Malikusmanrasheed** 2 years, 1 month ago

Does the paid pdf version contain less and more relevant questions?

upvoted 3 times

⊟ **jessicamendez10** Highly Voted 4 years, 3 months ago

In exam 20/03/2021

upvoted 22 times

⊟ **sureshatt** 4 years, 3 months ago

strange that this is in a recent exam because now PIM is automatically enabled.

upvoted 9 times

⊟ **aaronkho** 4 years ago

yup PIM is already automatically enabled

upvoted 5 times

⊟ **Hot_156** Most Recent 4 months ago

OUTDATED

Prepare PIM for Microsoft Entra roles

Here are the tasks we recommend for you to prepare Privileged Identity Management to manage Microsoft Entra roles:

Configure Microsoft Entra role settings

Give eligible assignments

Allow eligible users to activate their Microsoft Entra role just-in-time

Prepare PIM for Azure roles

Here are the tasks we recommend for you to prepare Privileged Identity Management to manage Azure roles for a subscription:

Discover Azure resources

Configure Azure role settings

Give eligible assignments

Allow eligible users to activate their Azure roles just-in-time

upvoted 3 times

Srirupam 7 months, 3 weeks ago

1.Sign-up

2. Discover privileged role.

3.use MFA

upvoted 2 times

ITFranz 8 months ago

Outdate question.

To secure Azure AD roles using Azure Active Directory (Azure AD) Privileged Identity Management (PIM), you need to perform the following three actions in sequence:

Configure PIM for Azure AD roles

Assign eligible roles

Activate roles when needed

upvoted 4 times

schpeter_091 7 months ago

correct, maybe there should be something like: get the GA role. (ok..we are creating a new question now:))

upvoted 1 times

JaridB 1 year, 2 months ago

To secure Azure AD roles using Azure Active Directory (Azure AD) Privileged Identity Management (PIM), you need to perform a series of actions. Here are the recommended steps in sequence:

1. Discover Privileged Roles: Before you can manage access with PIM, you need to discover who has privileged roles within your organization. You can use access reviews to automate the discovery and subsequent approval or removal of privileged role assignments.
2. Sign up PIM for Azure AD Roles: After discovering which privileged roles exist, the next step is to sign up for PIM. This involves configuring PIM settings for each role to establish the policies that govern their activation and use, like requiring multi-factor authentication (MFA), setting activation durations, and determining the need for approval from designated approvers.
3. Consent to PIM: The final step involves giving consent to PIM. This step is about acknowledging and accepting the responsibility that comes with using PIM to manage and secure privileged access within your organization.

upvoted 10 times

alfaAzure 1 year, 9 months ago

Sign up for Azure AD roles

Discover privileged roles

Consent to PIM

upvoted 8 times

BMF 1 year, 10 months ago

Admins , can you please update the answer to this question. I just bought the Contributer accsess but the reviews here are quite negative.

upvoted 4 times

Andre369 2 years, 1 month ago

To ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles, you should perform the following actions in sequence:

Sign up for Azure AD roles: This action involves enabling Azure AD PIM for your subscription and assigning users to the appropriate Azure AD roles that will have access to privileged operations.

Discover privileged roles: After signing up for Azure AD roles, you need to identify the roles in Azure AD that are considered privileged. This step involves identifying the roles that require additional security and oversight.

Consent to PIM: Once the privileged roles are discovered, you need to provide consent to enable PIM for these roles. This step ensures that PIM can manage and enforce the security controls for these roles.

upvoted 12 times

EM1234 2 years, 7 months ago

another outdated question

upvoted 10 times

geuser 2 years, 9 months ago

https://learn.microsoft.com/en-gb/azure/active-directory/privileged-identity-management/pim-getting-started

upvoted 1 times

Vikku30 3 years, 6 months ago

Consent to PIM is decomissioned now, it is enabled by default

upvoted 12 times

ashxos 3 years, 7 months ago

Answers are not relevant today as full PIM process is changed. Options have been removed and renamed.

upvoted 4 times

PBA1211 3 years, 9 months ago

weird answer

First youy consent...?

Looks to me that you cannot consent before you sign in to AZ (with MFA)

Anny way it's outdated .. so..

upvoted 1 times

justinp 3 years, 11 months ago

In exam, today

upvoted 3 times

Rume 3 years, 12 months ago

Out dated - old question

upvoted 3 times

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 a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy an Azure AD Application Proxy.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
✑ Create Azure Virtual Network.
✑ Create a custom DNS server in the Azure Virtual Network.
✑ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
✑ Configure forwarding between the custom DNS server and your on-premises DNS server.
Reference:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

Community vote distribution

B (100%)

gfhbox0083 Highly Voted 4 years, 12 months ago

B, for sure.

upvoted 18 times

orekz Highly Voted 4 years, 11 months ago

Definitely, B is the correct answer

upvoted 5 times

ITFranz Most Recent 8 months ago

An Azure Application Proxy is a feature of Azure Active Directory that allows you to securely publish on-premises web applications for external access without opening up your firewall or setting up a DMZ. Here are the key points about Azure Application Proxy:
Purpose:
Provides remote access to on-premises web applications
Enables single sign-on (SSO) for these applications
Eliminates the need for a VPN or reverse proxy
Answer = B

upvoted 2 times

Andre369 2 years, 1 month ago

Selected Answer: B

Deploying Azure AD Application Proxy does not meet the goal of allowing users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials. Azure AD Application Proxy is used for securely publishing on-premises web applications to users outside the organization's network. It does not provide the necessary integration between Azure HDInsight and on-premises Active Directory for user authentication

upvoted 5 times

majstor86 2 years, 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

F117A_Stealth 2 years, 7 months ago

Selected Answer: B

B is correct

upvoted 1 times

abelchior 2 years, 9 months ago

Selected Answer: B

B is correct

upvoted 1 times

netapp3 2 years, 11 months ago

B, App proxy is to connect on-prem applications to public users securely. Not the other way around as questions suggest.

upvoted 1 times

Eltooth 3 years, 3 months ago

Selected Answer: B

B is correct.

AAD DS is required.

https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture#integrate-hdinsight-with-active-directory

upvoted 3 times

> **OpsecDude** 2 years, 9 months ago
>
> Still in the previous page, they show using a site to site vpn as the correct one, but after doing some reading on HDInsights and AADDS I agree with you
>
> upvoted 1 times

udmraj 3 years, 4 months ago

B is the correct answer

upvoted 1 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 1 times

sandeepsw 3 years, 10 months ago

b for sure

upvoted 1 times

Mcgood 3 years, 11 months ago

True its a NO, Proxy has to do with way outs of traffic like internet and the likes

upvoted 1 times

ManOnTheMoon 4 years ago

B, fo shizzle

upvoted 2 times

Sjn9 4 years, 2 months ago

B is the correct answer

upvoted 1 times

swati17 4 years, 2 months ago

B is correct

upvoted 1 times

teamaws 4 years, 2 months ago

B for shore

upvoted 1 times

Question #20 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription named Sub1.
You have an Azure Storage account named sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to sa1.
Solution: You regenerate the Azure storage account access keys.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

Community vote distribution
A (100%)

francis6170 Highly Voted 3 years, 3 months ago
Got this in the AZ-500 exam (Sept 2021)! A: Yes
upvoted 11 times

Squaiyumi Highly Voted 3 years, 8 months ago
In the exam 6 April
upvoted 11 times

Knighthell Most Recent 3 weeks, 2 days ago
Selected Answer: A
yes but only if

BUT: access is through SAS tokens → these tokens can be based on:

Account SAS (tied to the storage account key → regenerating the keys will invalidate these SAS tokens)

Service SAS or User Delegation SAS → regenerating the keys may not be sufficient if there are SAS tokens signed with user delegation keys.

Stored Access Policies → if the token was issued using a stored access policy, you also need to revoke or update the policy.
upvoted 1 times

brooklyn510 11 months, 4 weeks ago
On exam 1/2/24
upvoted 5 times

flafernan 1 year ago
Selected Answer: A
Yes, regenerating Azure storage account access keys is an effective way to revoke all existing access to the storage account. When you regenerate access keys, the old keys become invalid, which effectively denies access to all services associated with the account, including the blob service and file service.
upvoted 3 times

JunetGoyal 1 year, 2 months ago
yes, As SAS are built on top of access key!
upvoted 1 times

Andre369 1 year, 7 months ago

Selected Answer: A

Regenerating the Azure storage account access keys will revoke all access to the storage account, including the blob service and the file service. By regenerating the access keys, the existing SAS tokens and stored access policies will become invalid, preventing unauthorized access to the storage account.

upvoted 2 times

Gesbie 1 year, 8 months ago

In Exam April 11, 2023

upvoted 5 times

majstor86 1 year, 10 months ago

Selected Answer: A

A: Correct answer is Yes.

upvoted 1 times

003nickm 1 year, 10 months ago

On 2-March-2023, I passed AZ-500 with flying color. This question was in the exam. Some question was on Defender EASM a well.

upvoted 6 times

Diallo18 2 years, 2 months ago

In Exam 10/18/2022. One case study, no lab.

upvoted 2 times

Amit3 2 years, 3 months ago

# In EXAM - 01-Oct-2022

upvoted 2 times

Eltooth 2 years, 9 months ago

Selected Answer: A

Correct answer is Yes.

upvoted 4 times

rohitmedi 3 years, 1 month ago

correct answer

upvoted 1 times

Jco 3 years, 3 months ago

#exam question # 29 Sep

upvoted 4 times

> **Armanas** 2 years, 2 months ago
>
> So .... what is the Selected Answer?? A or B?
>
> upvoted 1 times

SecurityAnalyst 3 years, 4 months ago

# IN EXAM - 31/8/2021

upvoted 3 times

Socgen1 3 years, 4 months ago

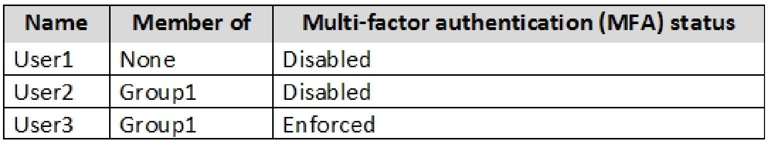
in exam on 31/08/2021

upvoted 2 times

Question #21 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	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
User3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is used in contoso.com.

In PIM, the Password Administrator role has the following settings:

✑ Maximum activation duration (hours): 2

✑ Send email notifying admins of activation: Disable

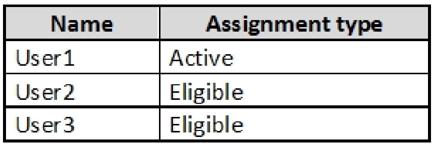
✑ Require incident/request ticket number during activation: Disable

✑ Require Azure Multi-Factor Authentication for activation: Enable

✑ Require approval to activate this role: Enable

✑ Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

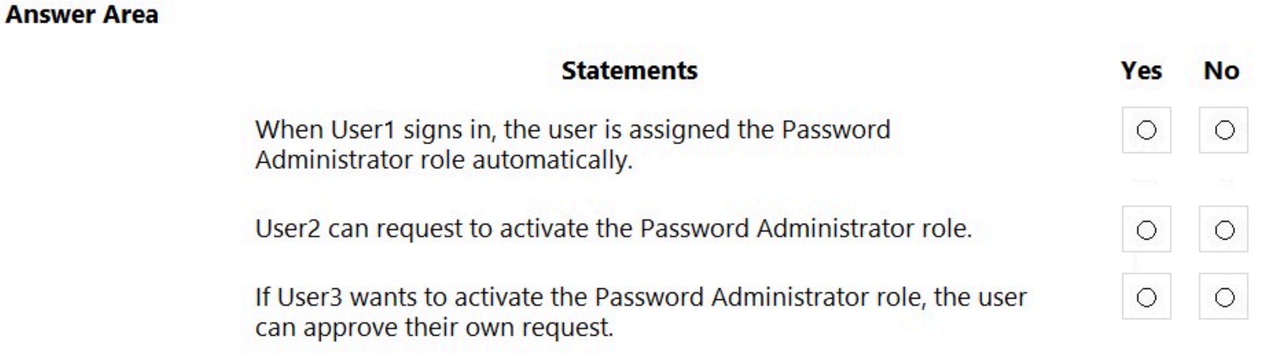


Name	Assignment type
User1	Active
User2	Eligible
User3	Eligible

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

NOTE: Each correct selection is worth one point.

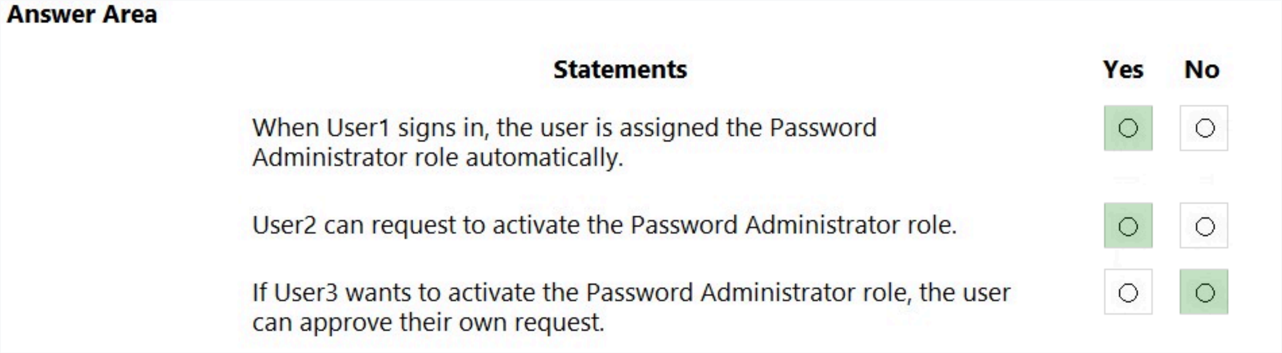
Hot Area:



Answer Area

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	[✓ ○]	○
User2 can request to activate the Password Administrator role.	[✓ ○]	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	[✓ ○]

Box 1: Yes -

Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.

Box 2: Yes -

While Multi-Factor Authentication is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled, User2 can request the role but will need to enable MFA to use the role.

Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication

(MFA) check, providing a business justification, or requesting approval from designated approvers.

Box 3: No -
User3 is Group1, which is a Selected Approver Group, however, self-approval is not allowed and someone else from group is required to approve the request.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

zellck Highly Voted 👍 2 years, 1 month ago
YYN is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles#assign-a-role
Azure AD PIM for Azure resources provides two distinct assignment types:
- Eligible assignments require the member to activate the role before using it. Administrator may require role member to perform certain actions before role activation which might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
- Active assignments don't require the member to activate the role before usage. Members assigned as active have the privileges assigned ready to use. This type of assignment is also available to customers that don't use Azure AD PIM.
upvoted 12 times

RickySmith 9 months, 1 week ago
YYN
Link for 3rd one only.
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-approval-workflow
upvoted 2 times

zellck 2 years, 1 month ago
Gotten this in May 2023 exam.
upvoted 6 times

Lidiatuke_ 1 year, 11 months ago
Was there any of the simulator questions on the exam?
upvoted 1 times

IvanIco 1 year, 9 months ago
User1 cant get the role he is not in Grp1
upvoted 1 times

pentium75 11 months ago
The group has nothing to do with the role.
upvoted 1 times

zellck 2 years, 1 month ago
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow#approve-requests
Approvers are not able to approve their own role activation requests.
upvoted 5 times

[Removed] Highly Voted 👍 3 years, 5 months ago
YES - Active assignment
NO - User 2 has MFA disabled which is a requirement
NO - You cannot self approve/activate
upvoted 9 times

helpaws 3 years, 5 months ago
box 2. Yes, you can still request it.
upvoted 17 times

Yswar Most Recent 🕘 2 months, 3 weeks ago
Yes- Active assignment requires no further action
Yes - Yes, user 2 can still request to activate a privileged role via Azure AD Privileged Identity Management (PIM), even if MFA is disabled. However, the activation process will not complete successfully unless MFA is enabled
No- self approval doesn't work
upvoted 1 times

Jimmy500 1 year ago

Here is one tricky part for the second option as it seems it asks User2 can request to activate but since MFA disabled will not be able to activate (If this ask can User2 request then it seems Yes but even request will not be able to have role at MFA disabled needs to enable MFA as well).
As documentation says before activate - You can require users who are eligible for a role to prove who they are by using the multifactor authentication feature in Microsoft Entra ID before they can activate

upvoted 2 times

Ivan80 1 year, 5 months ago

In exam 1/28/24

upvoted 7 times

Shackman66 1 year, 5 months ago

3 - shouldnt the User-3 be yes the self approver is Group1. and User-3 is member of Group1?

upvoted 1 times

wardy1983 1 year, 7 months ago

Box 1: Yes -
Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.
Box 2: Yes -
While Multi-Factor Authentication is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled, User2 can request the role but will need to enable MFA to use the role.
Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication
(MFA) check, providing a business justification, or requesting approval from designated approvers.
Box 3: No -
User3 is Group1, which is a Selected Approver Group, however, self-approval is not allowed and someone else from group is required to approve the request.

upvoted 5 times

Andre369 2 years, 1 month ago

1. When User1 signs in, the user is assigned the Password Administrator role automatically.-No.
Reason:
User1 is not a member of any group that has the Password Administrator role assigned, and User1 is not eligible for the role. Therefore, User1 will not be assigned the Password Administrator role automatically
2. User2 can request to activate the Password Administrator role.--Yes.
Reason:
User2 is eligible for the Password Administrator role, and the role requires approval for activation. User2 can request to activate the role, and the request will be sent to the assigned approver (Group1) for approval.
3. If User3 wants to activate the Password Administrator role, the user can approve their own request.-No.
Reason:
User3 is eligible for the Password Administrator role, but the role requires approval for activation. User3 cannot approve their own request. The request will be sent to the assigned approver (Group1) for approval.

upvoted 1 times

Holii 2 years, 1 month ago

User1 is already 'Active' on the Password Administrator role. He has it assigned to him automatically. YYN

upvoted 8 times

massnonn 2 years ago

No for me Y-N-N
user1 is active while user2 is eligible but mfa is disable and option for request is enable

upvoted 2 times

massnonn 2 years ago

For activation is enable user2 can request but for active use mfa

upvoted 2 times

icebw22 2 years, 3 months ago

Correct, yes, yes, no.

Cannot self approve your own request

upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

Yes

Yes

No

upvoted 4 times

⊟ **stepman** 2 years, 2 months ago

I chose this and this was On exam 4/27 with the new exam experience. No Sim or lab.

upvoted 4 times

⊟ **Ajdlfasudfo0** 2 years, 6 months ago

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow#approve-requests

"Approvers are not able to approve their own role activation requests."

upvoted 3 times

⊟ **Muaamar_Alsayyad** 2 years, 8 months ago

Answer is correct

Approvers can't approve their own role activation request , check the note section in this link

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow

upvoted 4 times

⊟ **Diallo18** 2 years, 8 months ago

In Exam 10/18/2022. One case study, no lab.

upvoted 1 times

⊟ **Amit3** 2 years, 9 months ago

# In EXAM - 01-Oct-2022

upvoted 3 times

⊟ **Didib** 3 years, 2 months ago

Tested this in the lab and User 3 was able to activate the Password Admin role himself by going to Assigned roles in AD -> Eligible assignments -> Update.

upvoted 3 times

⊟ **somenick** 2 years, 9 months ago

Agree. The message about self-assignment does not appear now.

upvoted 1 times

⊟ **Siblark** 2 years, 9 months ago

I disagree. You cannot self-approve yourself for an eligible role

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow

upvoted 3 times

⊟ **somenick** 2 years, 8 months ago

While in reality it can be different for the sake of exam I'd select No for item 3. These dumb marketing guys who creates these exams are using documentation and not the lab...

upvoted 4 times

⊟ **CJ32** 3 years, 4 months ago

Answers are correct based on the ET explanation and link. YES YES NO

upvoted 4 times

⊟ **amksa** 3 years, 5 months ago

in selected approver there's group1, why user3 can't approve its request?

User3 is in group1.

upvoted 2 times

⊟ **amksa** 3 years, 5 months ago

I see why, self approval is no allowed

upvoted 2 times

Question #22 *Topic 2*

You have a hybrid configuration of Azure Active Directory (Azure AD) that has Single Sign-On (SSO) enabled. You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance from the domain joined device and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

A. Active Directory - Password

B. Active Directory - Universal with MFA support

C. SQL Server Authentication

D. Active Directory - Integrated

Suggested Answer: *D*

Active Directory - Integrated -

Azure Active Directory Authentication is a mechanism of connecting to Microsoft Azure SQL Database by using identities in Azure Active Directory (Azure AD).

Use this method for connecting to SQL Database if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

Reference:

https://docs.microsoft.com/en-us/sql/ssms/f1-help/connect-to-server-database-engine?view=sql-server-2017 https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

Community vote distribution

D (100%)

cannibalcorpse Highly Voted 3 years, 8 months ago

Azure Active Directory - Password ---> Use this method for connecting to SQL Database if you are logged in to Windows using credentials from a domain that is not federated with Azure

Active Directory - Integrated ---> Use this method for connecting to SQL Database if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

Our keyword is "SSO" so option D should be the answer

upvoted 44 times

teehex Highly Voted 3 years, 7 months ago

The hint of this question is "You have a hybrid configuration of Azure Active Directory (Azure AD) that has Single Sign-On (SSO) enabled". So basically when SSO, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

And Microsoft already recommends to use Integrated Authentication if you are logged into Windows using your Azure Active Directory credentials from a federated domain, or a managed domain that is configured for seamless single sign-on for pass-through and password hash authentication (https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell#active-directory-integrated-authentication)

Option A (AD - Password) sounds like a correct answer if you set Remember password. However the most correct answer is Option D as it minimizes authentication prompt.

upvoted 8 times

brooklyn510 Most Recent 11 months, 4 weeks ago

On exam 1/2/24

upvoted 3 times

Obama_boy 1 year ago

Selected Answer: D

in exam 08/12/2023

upvoted 3 times

KikoTeijeiro 1 year, 2 months ago

Az-500 today on exam. Passed 826/1000. No labs on the online exam. One Case Study with 5 questions.

upvoted 2 times

tweleve 1 year, 2 months ago

In exam 13 Oct

upvoted 1 times

trashbox 1 year, 2 months ago

Selected Answer: D

The question was given on the October 9, 2023 exam.

upvoted 1 times

ESAJRR 1 year, 5 months ago

Selected Answer: D

D. Active Directory - Integrated

upvoted 1 times

Andre369 1 year, 7 months ago

Selected Answer: D

To allow database developers to connect to the Azure SQL Database instance from their domain-joined devices and authenticate using their on-premises Active Directory account with minimum authentication prompts, you should recommend the "Active Directory - Integrated" authentication method.

The "Active Directory - Integrated" authentication method enables seamless authentication using the current user's Active Directory credentials without requiring an additional prompt for authentication. It leverages the domain-joined device's established trust relationship with Azure AD to authenticate the user.

By using this authentication method, developers can connect to the Azure SQL Database instance using Microsoft SQL Server Management Studio without the need to enter separate credentials, providing a more streamlined and user-friendly experience.

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/azure-ad-authentication-sql-server-overview?view=sql-server-ver16#azure-active-directory-integrated

When the Windows domain is synchronized with Azure AD, and a user is logged into the Windows domain, the user's Windows credentials are used for Azure AD authentication.

upvoted 1 times

Gesbie 1 year, 8 months ago

In Exam April 11, 2023

upvoted 3 times

majstor86 1 year, 10 months ago

Selected Answer: D

D. Active Directory - Integrated

upvoted 1 times

F117A_Stealth 2 years, 1 month ago

Selected Answer: D

D. Active Directory - Integrated

upvoted 1 times

Amit3 2 years, 3 months ago

# In EXAM - 01-Oct-2022

upvoted 3 times

Eltooth 2 years, 9 months ago

Selected Answer: D

D is correct answer.

upvoted 2 times

⊟ **Cessyd** 2 years, 11 months ago

On today's exam 06/01/22

upvoted 5 times

⊟ **rohitmedi** 3 years, 1 month ago

correct answer

upvoted 2 times

Question #23 *Topic 2*

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.

The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

A. a key vault access policy

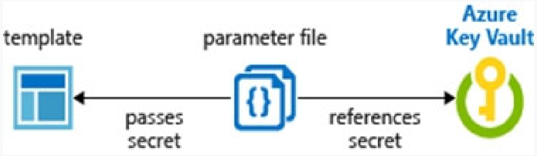
B. a linked template

C. a parameters file

D. an automation account

Suggested Answer: *C*

You reference the key vault in the parameter file, not the template. The following image shows how the parameter file references the secret and passes that value to the template.



Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter

Community vote distribution

B (93%) 7%

rharbeg Highly Voted 5 years, 7 months ago

The correct answer should be B

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter#reference-secrets-with-dynamic-id

upvoted 106 times

ExamUser 5 years, 2 months ago

You're correct. The question states the need to retrieve credentials for different deployments, and linked template's the only mechanism for it.

upvoted 4 times

vlq 5 years, 2 months ago

Yep, you are absolutely right!

upvoted 1 times

sureshatt 4 years, 4 months ago

100% correct. Answer should be B.

upvoted 11 times

kanag1 3 years, 5 months ago

You can't dynamically generate the resource ID in the parameters file because template expressions aren't allowed in the parameters file.Hence the answer is Template.

upvoted 3 times

shaheer1991 Highly Voted 5 years, 1 month ago

The correct answer is B "a linked template" and I'm backing this up by the below link:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

in the question it says:

You need to identify a method to dynamically construct a resource ID that will designate the key vault
containing the appropriate secret during each deployment. The name of the key vault and the name of the
secret will be provided as inline parameters.

----

if you check the pictures in the link, you'll find that answer B, supports the dynamic solution and the picture used to describe it contains "inline parameter" unlike the answer in the solution.

case closed

upvoted 24 times

⊟ **ExamStudy68** 2 years, 3 months ago

If you use the link Shaheer gave, it explains the dynamic versus static ID clearly - so if you are confused like I was, it is a great explanation. In the link "You can't dynamically generate the resource ID in the parameters file because template expressions aren't allowed in the parameters file." As well as "Reference secrets with static ID - With this approach, you reference the key vault in the parameter file, not the template. " Question states DYNAMIC so it would be "a linked template"

upvoted 1 times

⊟ **AZ500Xmen** Most Recent 9 months, 1 week ago

Read here: https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

you may want to pass parameter values to the template rather than create a reference parameter in the parameter file. The solution is to dynamically generate the resource ID for a key vault secret by using a linked template.

You can't dynamically generate the resource ID in the parameters file because template expressions aren't allowed in the parameters file.

In your parent template, you add the nested template and pass in a parameter that contains the dynamically generated resource ID.

upvoted 1 times

⊟ **Ivan80** 1 year, 5 months ago

In exam 1/28/24

upvoted 4 times

⊟ **yonie** 1 year, 6 months ago

Selected Answer: B

Answer is B.

Use case is dynamic vs static deployment.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#reference-secrets-with-dynamic-id

upvoted 1 times

⊟ **wardy1983** 1 year, 8 months ago

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

upvoted 1 times

⊟ **[Removed]** 1 year, 11 months ago

according to the reference article, the answer is right!

In the following parameter file, the key vault secret must already exist, and you provide a static value for its resource ID.

upvoted 1 times

⊟ **ESAJRR** 1 year, 11 months ago

Selected Answer: B

B. a linked template

upvoted 1 times

⊟ **d365ppp** 2 years, 2 months ago

Selected Answer: B

The solution is to dynamically generate the resource ID for a key vault secret by using a linked template.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

upvoted 2 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: B

B. a linked template

upvoted 2 times

⊟ **sofieejo** 2 years, 5 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 3 times

fonte 2 years, 5 months ago

Hi all,

Passed my exam (13JAN2023) with 918.

50 questions (45 + 5 of a case study).

Around 95% of the questions are here.

I've compiled the questions and my answers in a ppt, feel free to check it out and hope it helps.

https://www.dropbox.com/s/ay00xp2fnloq1ex/AZ%20500%20-%20Exam%20Topics.pptx?dl=0

Use pass az500prep to open the file.

Thanks to all the people that comment on questions, I wouldn't have passed without them :)

upvoted 7 times

shuklabond007 8 months, 2 weeks ago

File got deleted, can get new link?

upvoted 1 times

Sakkie02 2 years, 5 months ago

@fonte i downloaded your file and would like to know if i can mail you on some questions about the AZ-500 exam i will writing the exam this week and want to ask you about the file and the exam please?

upvoted 2 times

choy1977 1 year, 7 months ago

file has been deleted can you reshare? Thanks

upvoted 2 times

deepaksks 2 years, 5 months ago

The file has been deleted, please share it again.

upvoted 2 times

KaleMu92 2 years, 7 months ago

In Exam 02/12/2022

upvoted 1 times

edurakhan 2 years, 7 months ago

On exam today - 11/19/22 - pass

A lot of sentinel questions

upvoted 1 times

F117A_Stealth 2 years, 7 months ago

Selected Answer: B

B. a linked template

upvoted 1 times

Muaamar_Alsayyad 2 years, 8 months ago

Selected Answer: B

he question states the need to retrieve credentials for different deployments, and linked template's the only mechanism for it.

Reference secrets with static ID: we use only paramater

Reference secrets with dynamic ID: we use nested deployment (linked template)

upvoted 2 times

ArunRavilla 2 years, 11 months ago

Damn! Which is the right answer? :D

upvoted 3 times

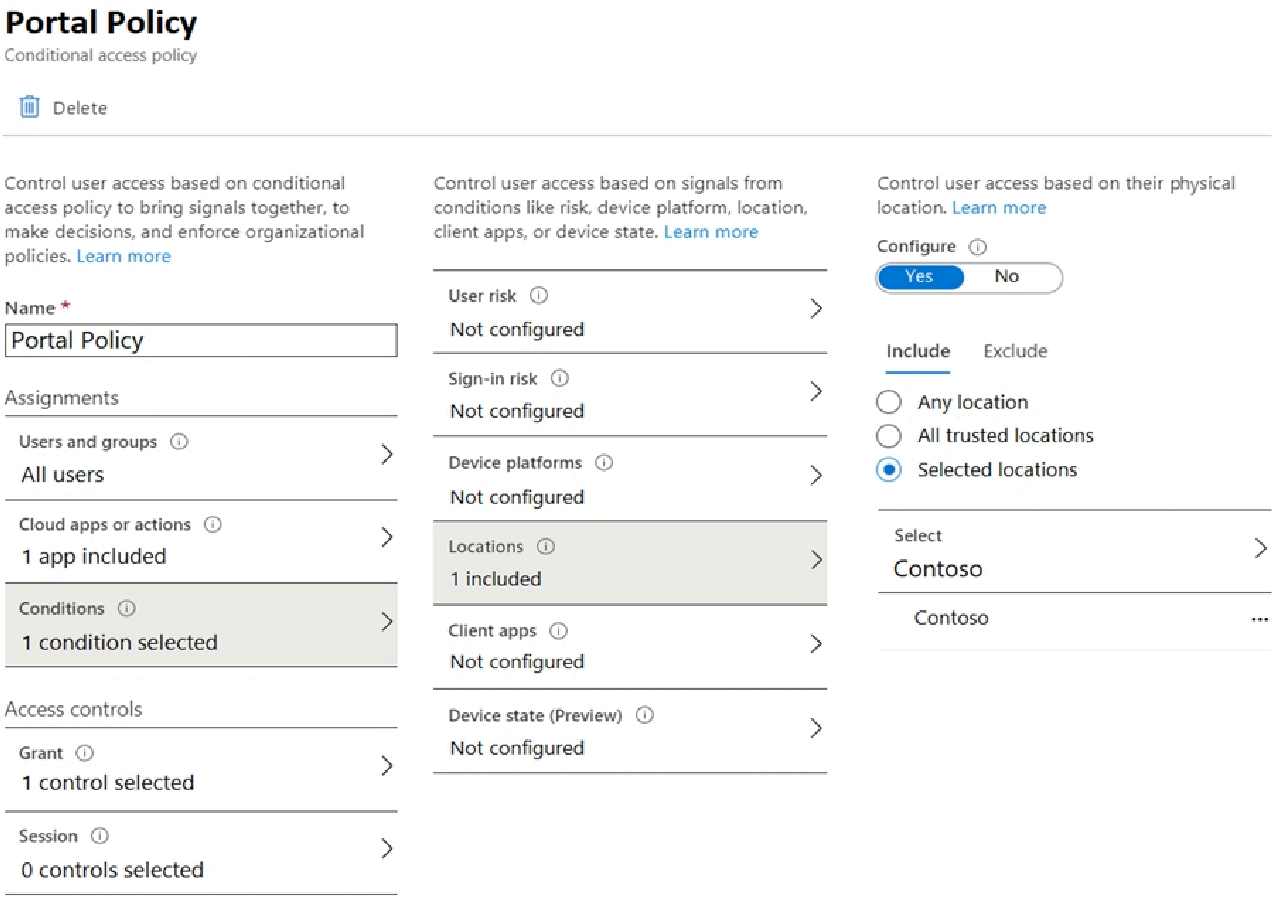
Question #24 *Topic 2*

HOTSPOT -

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



Portal Policy

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Portal Policy

Assignments

Users and groups: All users

Cloud apps or actions: 1 app included

Conditions: 1 condition selected

Access controls

Grant: 1 control selected

Session: 0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk: Not configured

Sign-in risk: Not configured

Device platforms: Not configured

Locations: 1 included

Client apps: Not configured

Device state (Preview): Not configured

Control user access based on their physical location. Learn more

Configure: [✓ Yes] No

Include | Exclude

○ Any location

○ All trusted locations

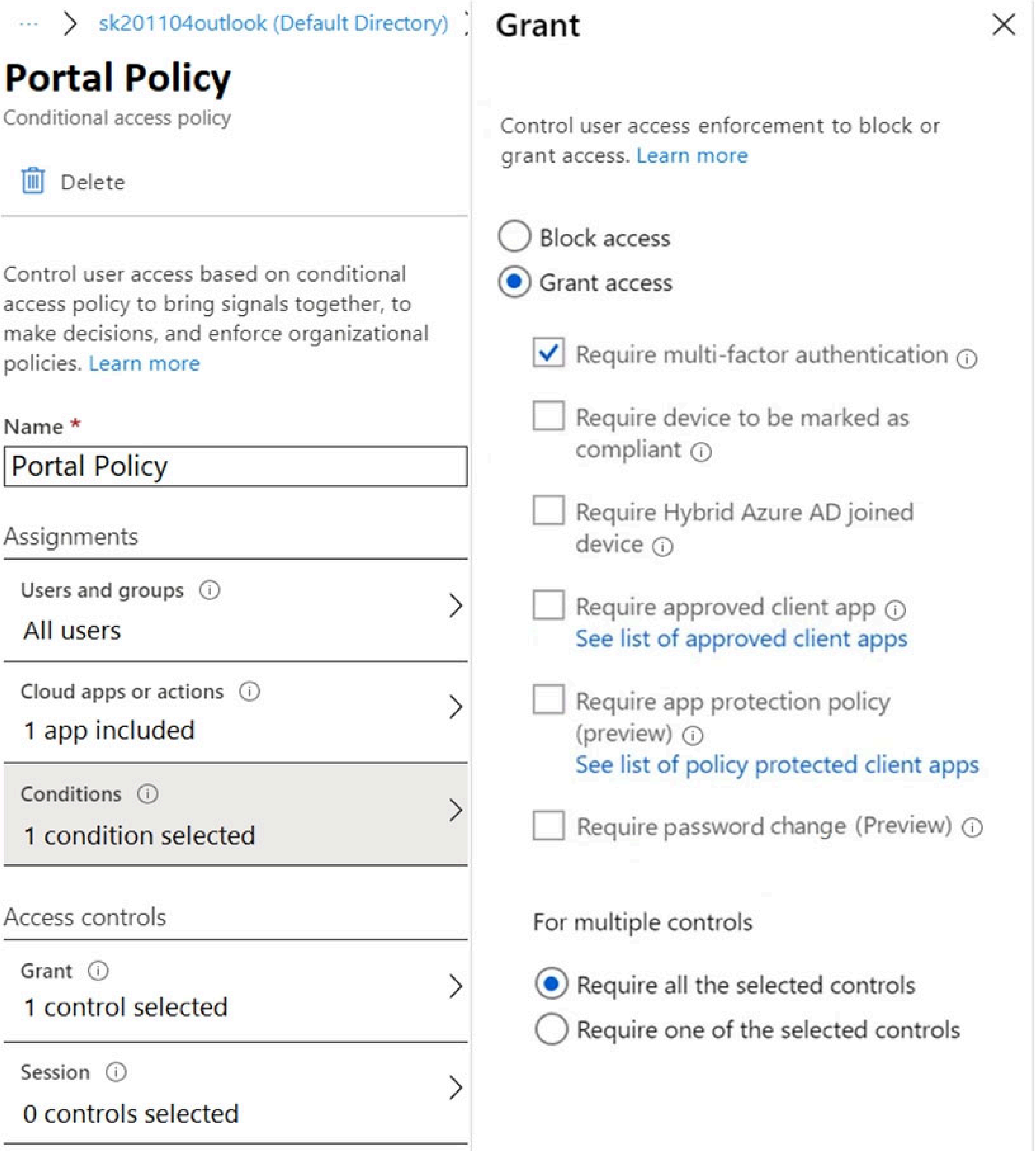
● Selected locations

Select

Contoso

Contoso ...

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



··· > sk201104outlook (Default Directory) >

Portal Policy

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Portal Policy

Assignments

Users and groups ⓘ
All users >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
1 condition selected >

Access controls

Grant ⓘ
1 control selected >

Session ⓘ
0 controls selected >

Grant

Control user access enforcement to block or grant access. Learn more

○ Block access
● Grant access

☑ Require multi-factor authentication ⓘ

□ Require device to be marked as compliant ⓘ

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

□ Require app protection policy (preview) ⓘ
See list of policy protected client apps

□ Require password change (Preview) ⓘ

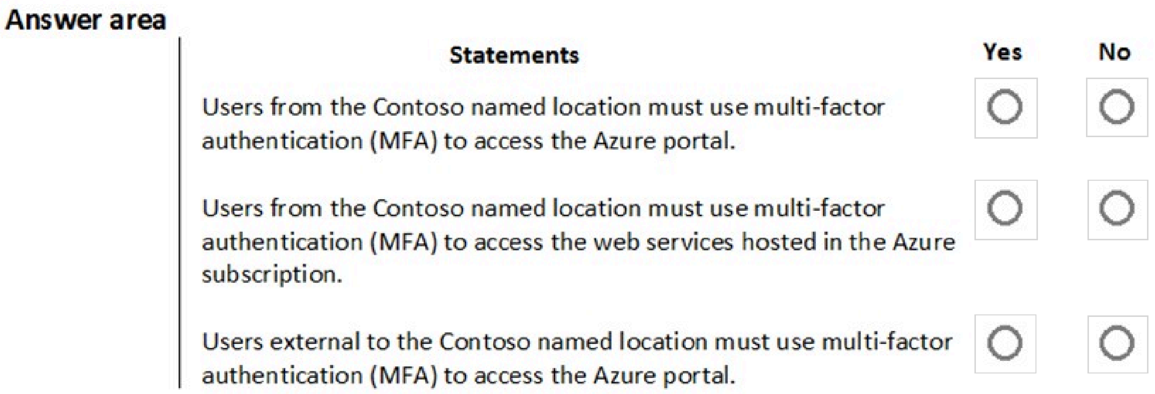
For multiple controls

● Require all the selected controls
○ Require one of the selected controls

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

NOTE: Each correct selection is worth one point.

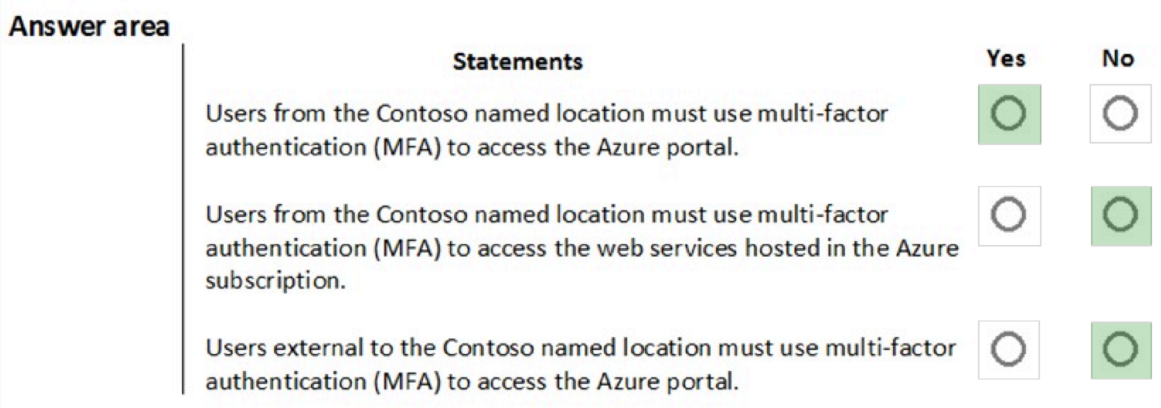
Hot Area:



Answer area

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

Suggested Answer:



Answer area

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	[✓ ○]	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	[✓ ○]
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	[✓ ○]

Box 1: Yes -

The Contoso location is included in the policy and MFA is required.

Box 2: No -

The policy applies to the Azure portal and Azure management endpoints. The policy does not apply to web services host in Azure.

Box 3: No -

The policy applies only to users in the Contoso location. The policy does not apply to users external to the Contoso location.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Orel123 Highly Voted 2 years, 3 months ago

YES - Contoso location requires MFA to use AZ Portal

NO - Contoso location does not require MFA to use web

NO - External users from Contoso location are not required to use MFA for AZ portal

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa?toc=/azure/active-directory/conditional-access/toc.json&bc=/azure/active-directory/conditional-access/breadcrumb/toc.json#configure-the-conditions-for-multi-factor-authentication

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#microsoft-cloud-applications

upvoted 24 times

Dushank Highly Voted 2 years, 5 months ago

Given answer is correct.

1) Yes - B'cos the users are accessing from Contoso location and it's included in the condition.

2) No - The cloud App is selected as "Microsoft Azure Management cloud app" . The question asks when users are accessing "Web services hosted in Azure subscription"

3) No - No other location other than "Contoso" location is selected. So when users connect from other locations, it will not prompt for MFA.

upvoted 11 times

tutonata Most Recent 9 months, 2 weeks ago

We don't know whether Contoso is marked as Trusted Location or not...

upvoted 1 times

MS_KoolaidMan 8 months, 2 weeks ago

I don't think it matters if Contoso is trusted or not.

It is simply a named location and used to determine if the CAP applies or not.

upvoted 3 times

icebw22 9 months, 2 weeks ago

Yes, no, no

As per diagram, condition is limited to azure portal not web services.

upvoted 1 times

majstor86 10 months ago

Yes
No
No

upvoted 2 times

Amialijoonz 1 year ago

Yes
No
No

upvoted 1 times

F117A_Stealth 1 year, 1 month ago

Answer is correct....

Y
N
N

upvoted 1 times

Eltooth 1 year, 9 months ago

Yes No No

upvoted 3 times

udmraj 1 year, 10 months ago

Yes-No-No is the correct Answer

upvoted 2 times

rohitmedi 2 years, 1 month ago

correct answer

upvoted 1 times

ashishg2105 2 years, 3 months ago

Given answer is correct
YES NO NO

upvoted 1 times

kakakayayaya 2 years, 4 months ago

For me answers are: n n n

Portal Policy is used to provide access to the Microsoft Azure Management cloud app.
Policy is not limit access to portal. It limits access to cloud app only.
Unfortunately we don't know the name of used Cloud App but it definitely not Web or Portal.

upvoted 1 times

> **kakakayayaya** 2 years, 4 months ago
>
> I was wrong!
> The Microsoft Azure Management application includes Azure portal! So provided answers are correct.
> https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps
>
> upvoted 6 times
>
> > **us3r** 1 year, 8 months ago
> >
> > plot twist
> >
> > upvoted 2 times

ad7399 2 years, 5 months ago

I just tested this on the portal. People in the Contoso location are included in the policy. The policy does not apply to those who are not in the Contoso location, therefore the answer to the third question is "No". The answer to the first two questions depends on what's selected under "Cloud Apps and Actions". As this isn't shown in the question (although it might be shown on the exam), it's impossible to say what the correct answer is.

For anyone interested in trying this out, I noticed a long delay (>30 mins) between making changes to the policy and them taking effect.

upvoted 3 times

justinp 2 years, 5 months ago

on exam, today

upvoted 2 times

catsforthewin 2 years, 5 months ago

What do you think the correct answer is?

upvoted 1 times

gsidhwani77 2 years, 5 months ago

Yes Yes No [Contoso is included for MFA] and hence OutSide Contose it will be allowed without MFA

upvoted 1 times

Jacquesvz 2 years, 5 months ago

Given answers are correct. for nr2, The policy does not apply to web services host in Azure.

upvoted 2 times

gsidhwani77 2 years, 5 months ago

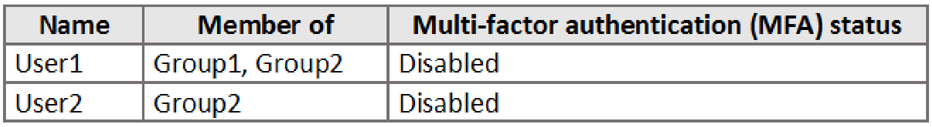
All should be yes. As Approved Apps are not selected. All Apps used from Contoso Location should be allowed access MFA. In case of Location Constraint - If coming from outside Contoso then MFA is mandatory.

upvoted 2 times

Question #25 Topic 2

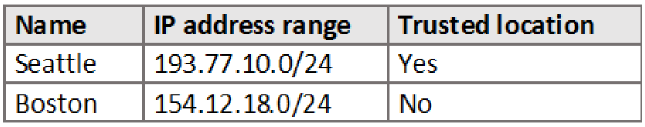
HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



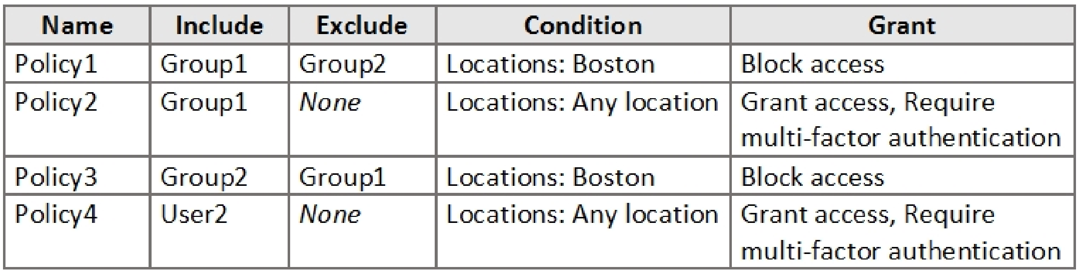
Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.



Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

You create the conditional access policies for a cloud app named App1 as shown in the following table.

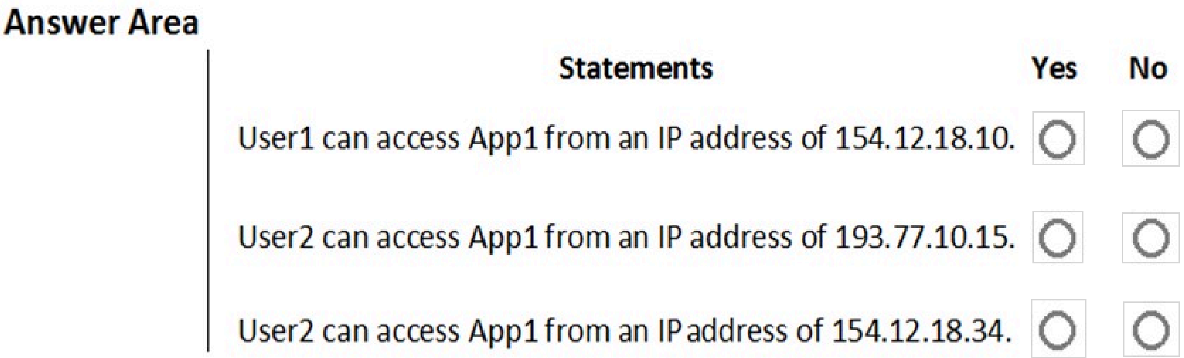


Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	*None*	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	*None*	Locations: Any location	Grant access, Require multi-factor authentication

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

NOTE: Each correct selection is worth one point.

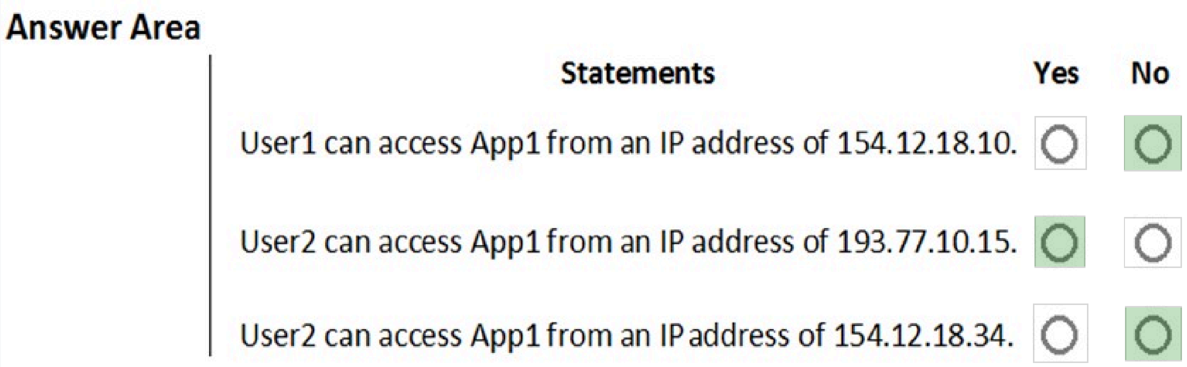
Hot Area:



Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	○	○
User2 can access App1 from an IP address of 193.77.10.15.	○	○
User2 can access App1 from an IP address of 154.12.18.34.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	○	[✓ ○]
User2 can access App1 from an IP address of 193.77.10.15.	[✓ ○]	○
User2 can access App1 from an IP address of 154.12.18.34.	○	[✓ ○]

Naqsh27 Highly Voted 3 years, 6 months ago

User 1 from Boston:

is user 1 member of Group 1 - yes - Block

is user 1 member of Group 2 - yes Exclusion takes priority - Allow

Policy 1 does not apply

Policy 2 Applies

Policy 3 and 4 does not apply

User 1 - Allowed

Is user 2 member of Group 1 - No

Is user 2 member of Group 2 - Yes - Exclusion takes Priority - Allow
Policy 1 does not apply - Allow
Policy 2 does not apply - no Result
Policy 3 - User is in group 2 - but in Seattle - Policy does not apply
Policy 4 - User 2 can be anywhere - Allowed with MFA
User 2 allowed

Is user 2 member of Group 1 - No
Is user 2 member of Group 2 - Yes - Exclusion takes Priority - Allow
Policy 1 does not apply - Allow
Policy 2 does not apply - no Result
Policy 3 - User is in group 2 - And in Boston - Policy applies - Block
Policy 4 - User 2 can be anywhere - But Block Policy take precedence in Policy 3
User 2 not allowed

Y - Y - N

upvoted 108 times

⊟ **waqas** 3 years, 6 months ago

To me it would be NYN...mentioned answers are correct..... First option will be No. Because If both grant and block policies match, block will always win. No exceptions! So policy 3 will be applied here.

upvoted 4 times

⊟ **mansc3wth1s** 3 years, 4 months ago

Policy1 and Policy3 have exclued for the user and they are in both groups. Which means.. They are EXCLUDED from the policy. That means do not use/apply to any user in that group. The second policy satisfies all conditions and they are not excluded so they may be granted access.

You're right that a DENY will always trump taking into account all policies IF multiple are satisfied. It's just in this case User1 was exempt from two (1,3) from even applying.

upvoted 3 times

⊟ **datz** 1 year ago

YYN

When organizations both include and exclude a user or group, the user or group is excluded from the policy. The exclude action overrides the include action in policy. Exclusions are commonly used for emergency access or break-glass accounts. More information about emergency access accounts and why they're important can be found in the following articles:

upvoted 2 times

⊟ **glitchlessxddd** 1 year, 3 months ago

N - Y - N

Policy 3 blocks user 1 from access in boston because user 1 is part of group 2

upvoted 4 times

⊟ **pentium75** 11 months ago

No because User1 is also in Group1 which is excluded from Policy3.

upvoted 1 times

⊟ **CrocoGreen** 3 years, 6 months ago

MFA is disabled. Users cannot access resources when the MFA is required but is disabled for users.

upvoted 13 times

⊟ **chancer** 3 years, 3 months ago

No no no

upvoted 12 times

⊟ **mansc3wth1s** 3 years, 4 months ago

In these types of questions when they list MFA almost never does it really matter. If someone requests access to something and it says 'disabled' you can simple just request to add the MFA when you are allowed. Disabled just means that at the time they do not have it setup.

upvoted 12 times

⊟ **koreshio** 2 years, 8 months ago

this is correct, the per-user MFA status does not seem to matter in CAPS and PIM. see ref:
https://learn.microsoft.com/en-us/answers/questions/529070/user-mfa-is-disabled-however-pim-activation-is-ask.html
https://www.vcloudnine.de/mfa-disabled-but-azure-asks-for-second-factor/#:~:text=Conditional%20Access%2C%20or%20enabled%20Security,MFA%20for%20a%20specific%20user.

upvoted 4 times

yooi 3 years, 2 months ago

All users start out Disabled. When you enroll users in per-user Azure AD Multi-Factor Authentication, their state changes to Enabled. When enabled users sign in and complete the registration process, their state changes to Enforced. Administrators may move users between states, including from Enforced to Enabled or Disabled.

so:
Enabled = The admin has enabled MFA on the account, but the user hasn't set it up.
Enforced = The user has completed the setup of their MFA.

upvoted 4 times

mahi83 Highly Voted 👍 3 years, 6 months ago

Policy 1 & 3 - Boston location - block access so option 1 & 3 is No
Option 2 - user 2 - policy 4 - require MFA and user is disabled for MFA so answ is NO for 2nd option.
so according to me: N-N-N

upvoted 20 times

pentium75 11 months ago

YYN because group exclusion takes precedence, and MFA "disabled" does not mean that he cannot enroll

upvoted 1 times

ca7859c Most Recent ⊙ 1 month, 1 week ago

YYN
Disabled ❌ No ❌ No Normal sign-in
Enabled ⚠ Yes (for registration) ❌ No (yet) Asked to register
Enforced ✅ Yes ✅ Yes MFA enforced

upvoted 1 times

WilianCArias 1 year, 6 months ago

Yes, Yes, No.

upvoted 3 times

Obama_boy 1 year, 6 months ago

in exam 08/12/2023

upvoted 2 times

wardy1983 1 year, 7 months ago

Explanation:
User1 can access - Remember, exclusions take precedence. Policy1 won't apply since group2 is excluded, policy2 allows, policy3 won't apply since group1 is excluded, policy4 won't apply.
User2 can access - there are no policies blocking the Seattle range
User2 cannot access - policy1 won't apply since group2 is excluded, policy2 allows, but policy3 blocks access for group2

upvoted 2 times

tweleve 1 year, 8 months ago

In exam 13 Oct

upvoted 3 times

iVath 1 year, 10 months ago

for case1 : User1 from Boston, Policy1 is NOT applied for User1.

see https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups :
Exclude users
When organizations both include and exclude a user or group, the user or group is excluded from the policy. The exclude action overrides the include action in policy.

upvoted 1 times

heatfan900 1 year, 10 months ago

TRUSTED IP LOCATIONS overrides MFA. N,Y,N

The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Azure AD Multi-Factor Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

upvoted 2 times

FedericoBellotti 2 years, 1 month ago

Y-Y-N this is the correct answer. To be sure i create the same configuration on my test tenant. Policy 1 and 3 don't work because exclusion has priority over inclusion

upvoted 2 times

zellck 2 years, 1 month ago

YYN is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips
The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Azure AD Multi-Factor Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

upvoted 3 times

xRiot007 11 months, 2 weeks ago

I think the first one is No.
Trusted IPs can bypass MFA, but the user tries to access from a Boston IP, which is NOT a trusted location. Policy 2 allows but requires MFA, which is disabled for User 1.

So User 1 has disabled MFA and he can't bypass MFA because he tries to access from a location that is NOT trusted (Boston). I would say that's a No.

upvoted 2 times

Gerd95 1 year, 3 months ago

Then it should be NYN, What part of the first question overrides MFA?
The user is from Boston, which is not a trusted location.
He is allowed by Policy2, which still requires MFA

upvoted 2 times

Gesbie 2 years, 2 months ago

In Exam April 11, 2023

upvoted 7 times

icebw22 2 years, 3 months ago

Should be Y,Y,N
exclude group takes precedence over include groups

upvoted 1 times

majstor86 2 years, 3 months ago

Yes
Yes
No

upvoted 2 times

sofieejo 2 years, 5 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 4 times

fonte 2 years, 5 months ago

Hi all,
Passed my exam (13JAN2023) with 918.
50 questions (45 + 5 of a case study).
Around 95% of the questions are here.
I've compiled the questions and my answers in a ppt, feel free to check it out and hope it helps.
https://www.dropbox.com/s/ay00xp2fnloq1ex/AZ%20500%20-%20Exam%20Topics.pptx?dl=0
Use pass az500prep to open the file.

Thanks to all the people that comment on questions, I wouldn't have passed without them :)

upvoted 2 times

nnd 2 years, 5 months ago

Hello, File is not opening

upvoted 1 times

fonte 2 years, 5 months ago

you can't open it directly... download and use the pass provided.

upvoted 1 times

josh_josh 2 years, 5 months ago

File has been deleted

upvoted 4 times

ltjones12 2 years, 5 months ago

The correct answers are Y,Y,N

User1 can access - Remember, exclusions take precedence. Policy1 won't apply since group2 is excluded, policy2 allows, policy3 won't apply since group1 is excluded, policy4 won't apply.

User2 can access - there are no policies blocking the Seattle range

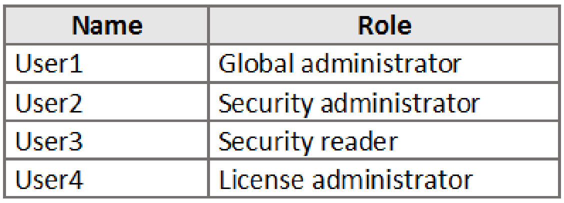
User2 cannot access - policy1 won't apply since group2 is excluded, policy2 allows, but policy3 blocks access for group2.

upvoted 3 times

Question #26 Topic 2

HOTSPOT -

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

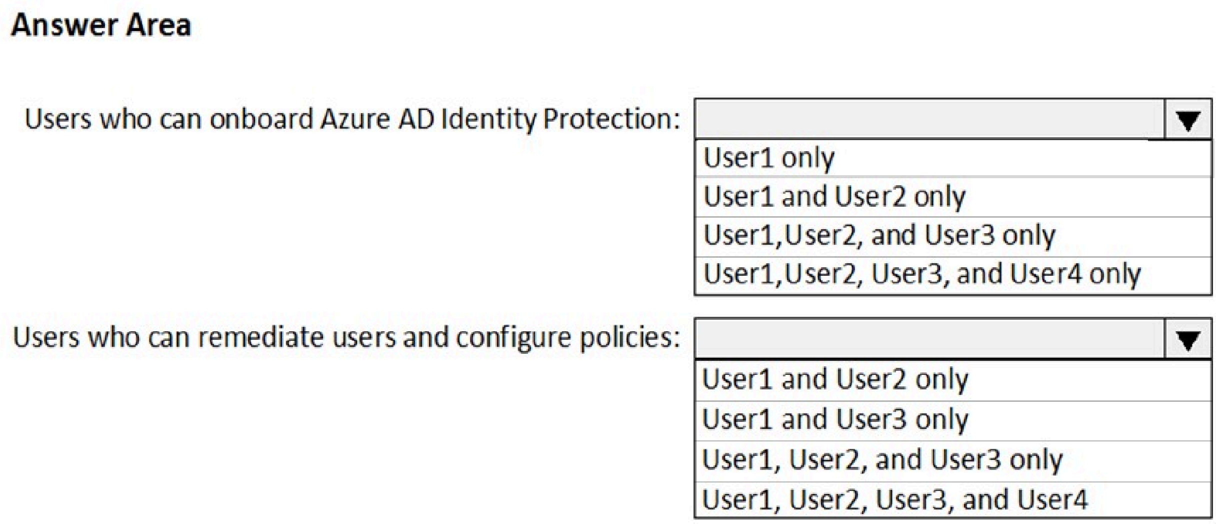
Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

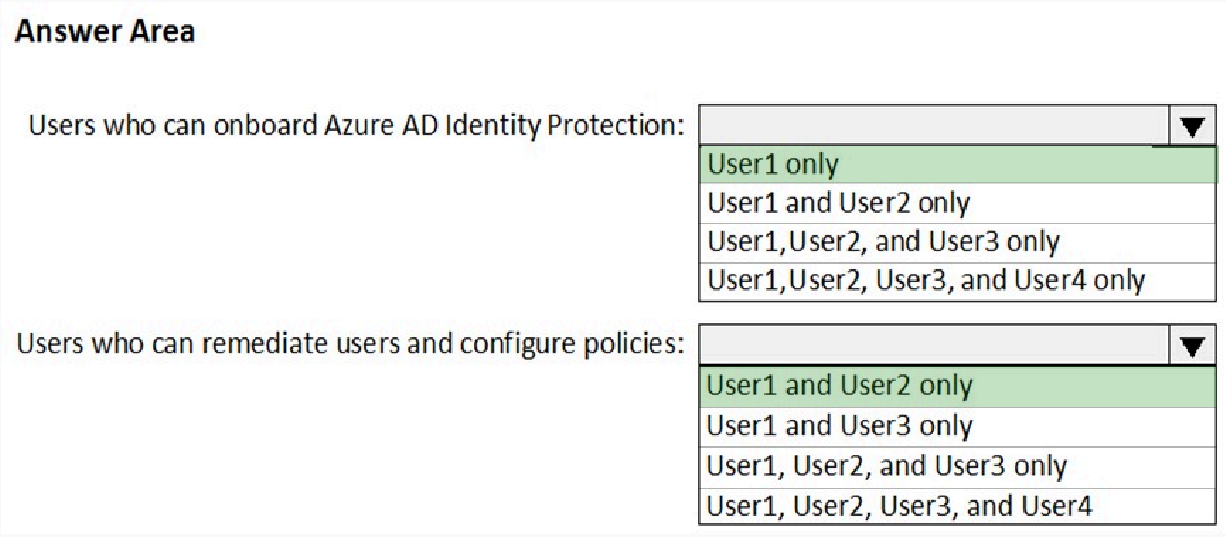


Answer Area

Users who can onboard Azure AD Identity Protection: ▼
- User1 only
- User1 and User2 only
- User1,User2, and User3 only
- User1,User2, User3, and User4 only

Users who can remediate users and configure policies: ▼
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Suggested Answer:



Answer Area

Users who can onboard Azure AD Identity Protection: ▼
- [✓ User1 only]
- User1 and User2 only
- User1,User2, and User3 only
- User1,User2, User3, and User4 only

Users who can remediate users and configure policies: ▼
- [✓ User1 and User2 only]
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

teehex Highly Voted 2 years, 7 months ago

Global Administrator and Security Administrator have full access to Identity Protection. However only Global Administrator can onboard Identity Protection.

Security Administrator has full access so it can remediate and configure policies. It can't reset user password tho.

Security Reader can view all Identity Protection reports and Overview blade. It can't configure policies.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions

The given answer is correct.

- Users who can onboard Azure AD Protection - User1 only
- Users who can remediate users and configure policies - User1 and User2 only

upvoted 87 times

⊟ **jessicamendez10** Highly Voted 👍 2 years, 9 months ago

In exam 20/03/2021

upvoted 23 times

⊟ **Sammy50** 2 years, 7 months ago

Thanks

upvoted 2 times

⊟ **awalao** 2 years, 3 months ago

thanks Jessica

upvoted 2 times

⊟ **hang10z** 2 years, 9 months ago

Thank you Jessica, important info

upvoted 7 times

⊟ **majstor86** Most Recent ⊙ 10 months ago

1. User 1 only
2. Users 1 and 2 only

upvoted 4 times

⊟ **Eltooth** 1 year, 9 months ago

User 1

User 1 & 2

upvoted 2 times

⊟ **WhalerTom** 2 years ago

In exam Dec 21. 40 questions, 1 case study, no labs.

upvoted 5 times

⊟ **AS179** 2 years ago

correct answer

upvoted 2 times

⊟ **rohitmedi** 2 years, 1 month ago

correct answer

upvoted 1 times

⊟ **Incredible99** 2 years, 1 month ago

Not sure how the answer is correct. For Box 1 should be User 1, User 2 and User 3 only. Reference: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

If we check in the permission section, it says "Identity Protection requires users be a Security Reader, Security Operator, Security Administrator, Global Reader, or Global Administrator in order to access.".

upvoted 1 times

⊟ **jantoniocesargatica** 1 year, 9 months ago

The first box is asking who can onboard. that means assigns the Security Administrator Role or any Identity protection role to manage policies, remediate in the AD Identity Protection section... User2 can NOT assign an user from the AD Assigned Role section and assigns a role (for instance Security Administrator) to other users. For that reason only Global Administrator can do this task.

upvoted 4 times

⊟ **ad7399** 2 years, 2 months ago

It's an old article, but it describes the roles:

https://identityexperts-home.azurewebsites.net/news/protecting-identities-with-azure-active-directory-identity-protection/

upvoted 1 times

⊟ **Jco** 2 years, 3 months ago

#exam question # 29 Sep

upvoted 1 times

⊟ **francis6170** 2 years, 3 months ago

Got this in the AZ-500 exam (Sept 2021)! I answered the same

upvoted 2 times

⊟ **Sjn9** 2 years, 8 months ago

Correct

upvoted 1 times

⊟ **debsauce** 2 years, 9 months ago

The give answer is correct

upvoted 8 times

⊟ **hang10z** 2 years, 9 months ago

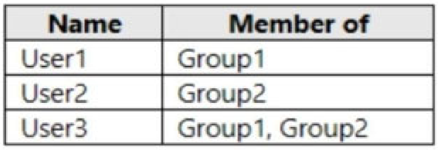
Verified

upvoted 1 times

Question #27 *Topic 2*

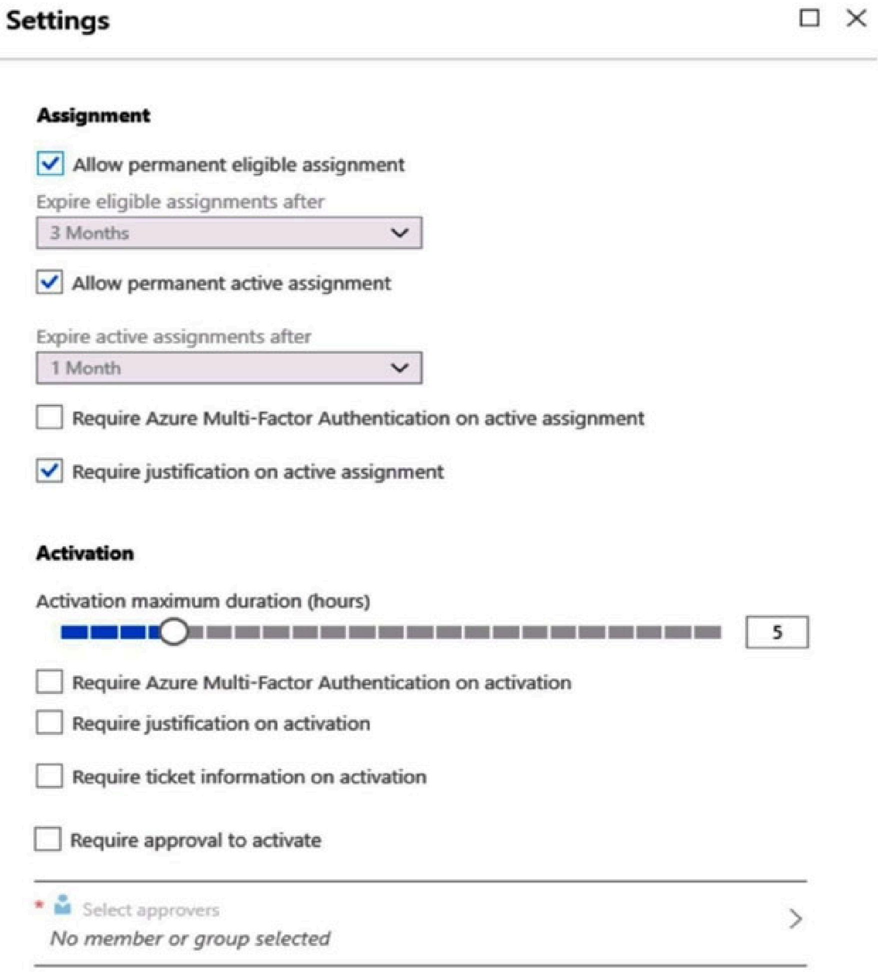
HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.



Settings

Assignment

☑ Allow permanent eligible assignment

Expire eligible assignments after: 3 Months

☑ Allow permanent active assignment

Expire active assignments after: 1 Month

□ Require Azure Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Activation

Activation maximum duration (hours): 5

□ Require Azure Multi-Factor Authentication on activation

□ Require justification on activation

□ Require ticket information on activation

□ Require approval to activate

* Select approvers

No member or group selected

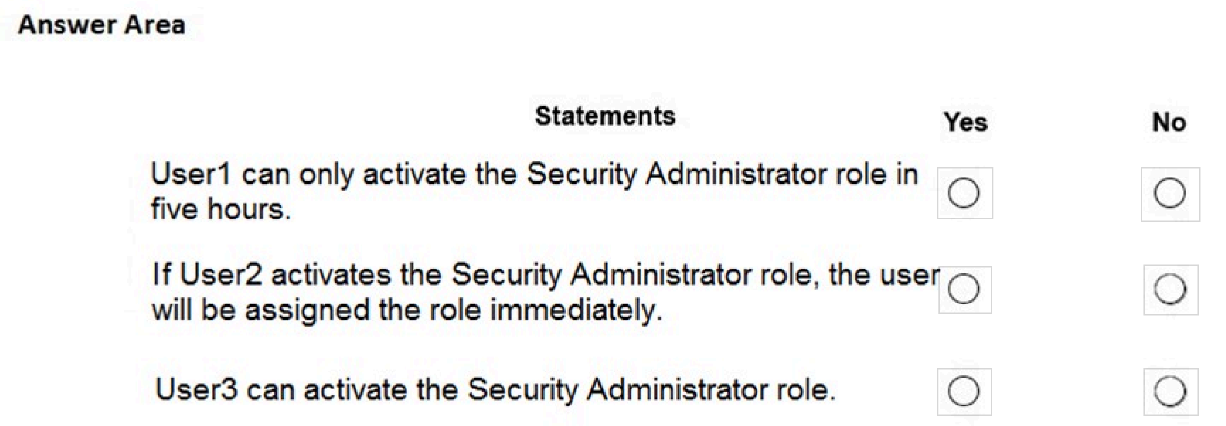
From PIM, you assign the Security Administrator role to the following groups:

- Group1: Active assignment type, permanently assigned
- Group2: Eligible assignment type, permanently eligible

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

NOTE: Each correct selection is worth one point.

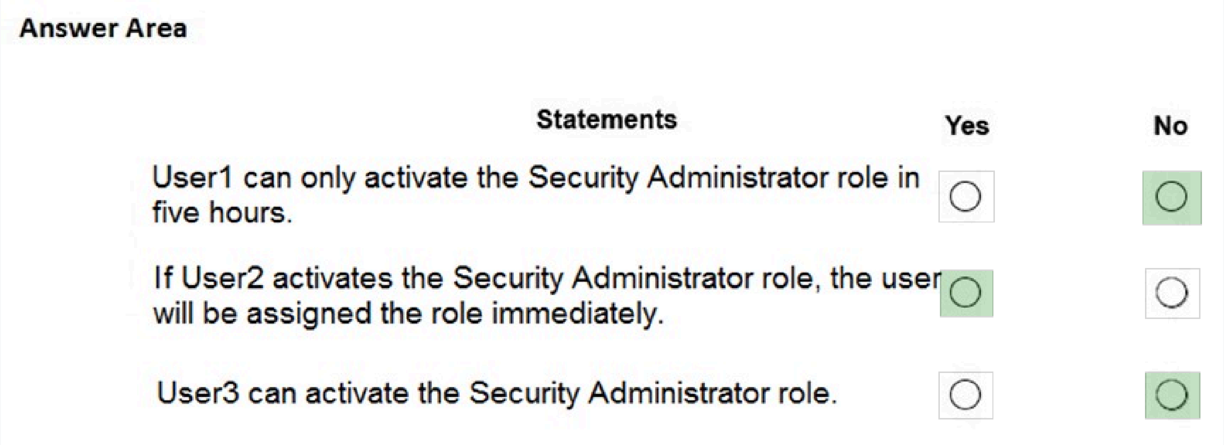
Hot Area:



Answer Area

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	[✓ ○]
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	[✓ ○]	○
User3 can activate the Security Administrator role.	○	[✓ ○]

Box 1: No -

User1 is a member of Group1. Group1: Active assignment type, permanently assigned

Box 2: Yes -

Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role

Box 3: No -

User3 is member of Group1 and Group2.

Group1: Active assignment type, permanently assigned

Group2: Eligible assignment type, permanently eligible

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

[Removed] Highly Voted 4 years, 3 months ago

I think answer should be:

No - this user already has the role assigned and 5 hours is how long the role can be assigned for when an eligible user activates it.

Yes - but not for the reason stated, user 2 is eligible and there are no items required for approval so it will be automatic and assigned for 5 hours

No - this user is already active in the role and will be for 1 month

upvoted 91 times

Startkabels 4 years, 3 months ago

5 hours is is not the expiration time, it is the activation time.

The permissions for user2 will not be assigned for 5 hours but for for 3 months

User 3 can active the role since he is a member of both the group for eligable assignment as for active assignment. Nowhere it states that the user already has the role.

upvoted 5 times

Startkabels 4 years, 3 months ago

Correction, what I said is incorrection: 5 hours is actually the expiration time after activation and the 3 months is the expiration for activating

upvoted 7 times

BalderkVeit 4 years, 1 month ago

User 3 canNOT activate role. he has it permanently active and if you'll try to activate already active role, you'll get error. So IT's a No.

upvoted 13 times

Pinto Highly Voted 4 years, 3 months ago

Box1: No. User1 can activate the role in 5 hours does not make sense. The role is already active.

Box2: Yes. User2 can activate the role and no approval is needed. Will have to just fill in the reason box.

Box3: No. User2 is part of group1 and the role is already active. No activation required.

upvoted 30 times

cfsxtuv33 3 years, 4 months ago

Box 3 is "user 3" and they are a part of group 1 AND group 2...but since he is part of group 1 then he is already "active" and does not need to be assigned.

upvoted 4 times

1dd60c0 Most Recent 4 months, 1 week ago

"If User 2 activates the Security Administrator role, the user will be assigned the role immediately"

But upon requesting activation would user 2 not first be prompted for justification.. meaning User 2 isn't immediately assigned the role..

By this logic you could say that once a user requests to activate the role if they are required to perform MFA that they are then immediately assigned the role too.

upvoted 1 times

pentium75 11 months ago

NO ("IN five hours" is nonsense)
YES (permanently eligible, no approval required)
No (has already an active assignment, no need to elevate)

upvoted 1 times

bob_sez 1 year, 7 months ago

The permanent eligible is enabled so the 3 months and 1 month in the boxes below will have no affect to the permanent eligibility. Permanent means permanent.

upvoted 5 times

ArchitectX 1 year, 9 months ago

it should be N N Y

upvoted 1 times

massnonn 2 years ago

N-N-Y Because Group2: Eligible assignment type, permanently eligible

upvoted 1 times

baye 1 year, 6 months ago

The Required Approuval to Activate is disabled

upvoted 1 times

majstor86 2 years, 3 months ago

No
Yes
No

upvoted 5 times

ltjones12 2 years, 5 months ago

Answers are correct

upvoted 1 times

F117A_Stealth 2 years, 7 months ago

No - this user already has the role assigned and 5 hours is how long the role can be assigned for when an eligible user activates it.
Yes - but not for the reason stated, user 2 is eligible and there are no items required for approval so it will be automatic and assigned for 5 hours
No - this user is already active in the role and will be for 1 month

upvoted 1 times

Muaamar_Alsayyad 2 years, 8 months ago

Just test it on the lab, user 3 can't activate the role, it gives an error saying " the rule arledy active"
Even though, the same role shows under active and eligible

upvoted 3 times

Doc_Pep 2 years, 10 months ago

IN 5 hours (as stated) or FOR 5 hours... If the question worded as is here on test (which I think is a mistake) then NO if it says FOR 5 hours, then yes...

upvoted 3 times

Ivanvazovv 2 years, 10 months ago

Answers are NYN, but User2 doesn't need to provide justification at all. Justification is required for the admin that assigns the roles to explain why he assigns them.

upvoted 1 times

WhalerTom 3 years, 6 months ago

In exam Dec 21. 40 questions, 1 case study, no labs.

upvoted 2 times

Incredible99 3 years, 6 months ago

In 12/18/21 exams

upvoted 4 times

zioggs 3 years, 7 months ago

Exam - 4/11/21

upvoted 3 times

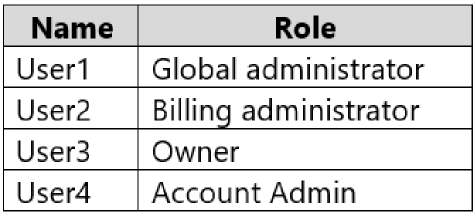
SecurityAnalyst 3 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 1 times

HOTSPOT -

Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.



Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

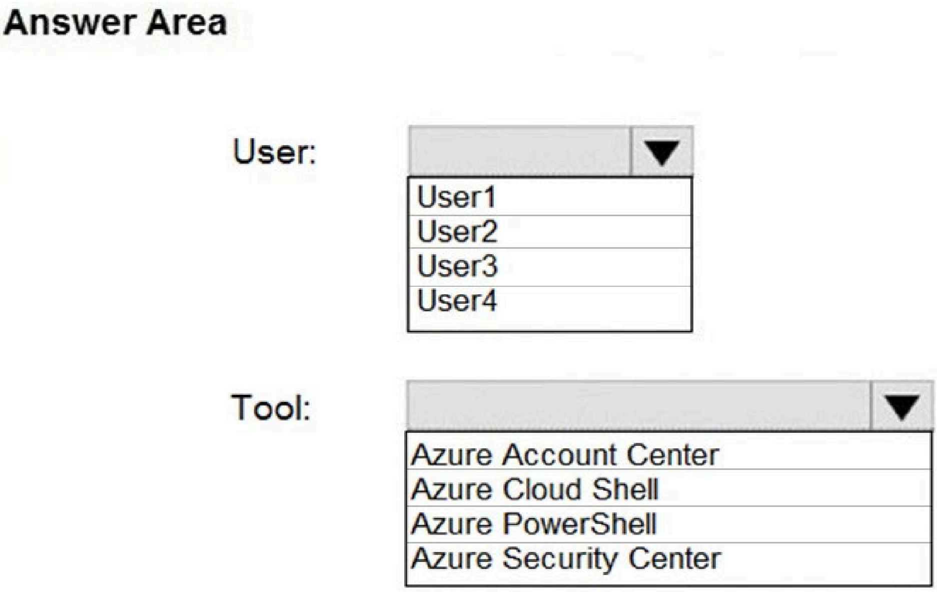
The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

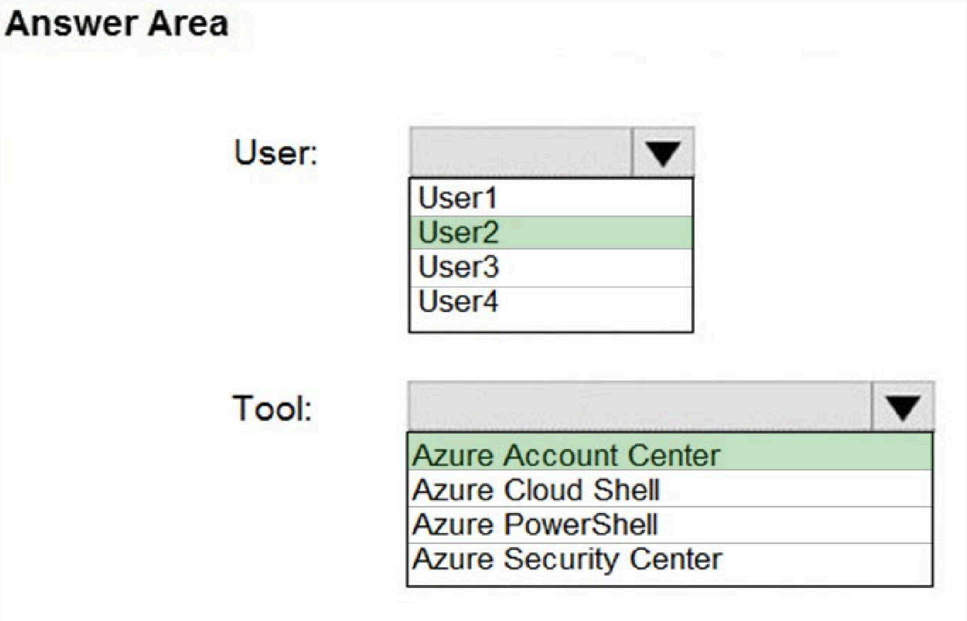
User:

User1
User2
User3
User4

Tool:

Azure Account Center
Azure Cloud Shell
Azure PowerShell
Azure Security Center

Suggested Answer:



Answer Area

User:

User1
[✓ User2]
User3
User4

Tool:

[✓ Azure Account Center]
Azure Cloud Shell
Azure PowerShell
Azure Security Center

Box 1; User2 -

Billing Administrator -

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center -

Azure Account Center can be used.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azure-subscription

acmaws Highly Voted 3 years, 5 months ago
Only the billing administrator of an account can transfer ownership of a subscription
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer#:~:text=Only%20the%20billing%20administrator%20of,transfer%20ownership%20of%20a%20subscription.
upvoted 18 times

Rohini12 Highly Voted 3 years, 2 months ago
In Exam - 21/10/2021
upvoted 11 times

806ae0b Most Recent 1 month, 3 weeks ago
„Only the account administrator of an account can transfer ownership of a subscription.„

Why would it be the billing admin?
upvoted 1 times

[Removed] 1 year ago
Prerequisites
To complete these steps, you will need:

Bash in Azure Cloud Shell or Azure CLI
Account Administrator of the subscription you want to transfer in the source directory
A user account in both the source and target directory for the user making the directory change
upvoted 1 times

Hot_156 4 months ago
Transferring Azure subscription ownership can be done through the Azure portal, but not directly through Azure Management Center, Bash in Azure CLI, or Azure CLI. Here are the steps to transfer ownership using the Azure portal:

Sign in to the Azure portal as the Account Admin.

Navigate to the "Subscriptions" blade.

Select the subscription you want to transfer.

Click on "Transfer billing ownership".

Enter the email address of the new owner.

Send the transfer request.
upvoted 1 times

gen33 1 year ago
correct
upvoted 1 times

wardy1983 1 year, 1 month ago
Box 1; User2 -
Billing Administrator -
Select Transfer billing ownership for the subscription that you want to transfer.
Enter the email address of a user who's a billing administrator of the account that will be the new owner for
the subscription.
Box 2: Azure Account Center -
Azure Account Center can be used.
upvoted 3 times

[Removed] 1 year, 1 month ago

Transfer billing ownership of an Azure subscription

Sign in to the Azure portal as an administrator of the billing account that has the subscription that you want to transfer. If you're not sure if you're an administrator, or if you need to determine who is, see Determine account billing administrator.

Navigate to Subscriptions and the select the one that you want to transfer.

upvoted 1 times

wardy1983 1 year, 2 months ago

Only the billing administrator of an account can transfer ownership of a subscription

upvoted 1 times

saturation97 1 year, 8 months ago

Transfer Billing Ownership:

https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

upvoted 3 times

fimbulvetrk 1 year, 8 months ago

Outdated question... Azure Account Center does not exist anymore and the permissions may change if you want to transfer the billing ownership within the actual tenant or if you want to transfer the Subscription to another tenant.

upvoted 8 times

majstor86 1 year, 10 months ago

User 2 = Billing Administrator

Tool = Azure Portal (Azure Account Centre-outdated)

upvoted 3 times

F117A_Stealth 2 years, 1 month ago

User 2 = Billing Administrator

Tool = Azure Portal (Question is outdated, otherwise, if Azure Portal is not there, just select Azure Account Centre)

upvoted 6 times

OpsecDude 2 years, 3 months ago

According to this doc: https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer, it is from the Azure Portal that you transfer Billing Ownership. I did it 2 weeks ago simply by clicking on my Subscription with a Billing Admin account, and then Transfer Ownership.

upvoted 4 times

jayek 2 years, 3 months ago

https://docs.microsoft.com/en-us/azure/role-based-access-control/transfer-subscription?WT.mc_id=Portal-Microsoft_Azure_SubscriptionManagement#understand-the-impact-of-transferring-a-subscription

upvoted 1 times

agente232 2 years, 3 months ago

for me, billing ownership and subscription ownership are two different things

upvoted 2 times

asfgsertweg 2 years, 8 months ago

Sorry but don't agree with this beautiful consensus. I don't see any Billing Admin anywhere, the billing ownership is Assigned to an Account Admin. The account admin can be fund in the Subscription properties or in the overview page of the Cost and Billing. Therefore transferring the billing ownership will defined a new Admin Account. Additionally, the account center is not used, as shown in the linked procedure, the transfer is done from the AZURE portal !!!!

upvoted 1 times

OpsecDude 2 years, 3 months ago

Since Azure Portal is not an option (question might be updated), the one left would be Account Center, just like Daniel76 said.

upvoted 1 times

Daniel76 2 years, 8 months ago

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

"Only the billing administrator of an account can transfer ownership of a subscription.".

Azure Account Center = Azure Portal -> Billing Account

upvoted 2 times

Eltooth 2 years, 9 months ago

Correct answer.

Billing Admin

Account Admin Centre.

upvoted 2 times

Question #29 *Topic 2*

SIMULATION -

The developers at your company plan to create a web app named App12345678 and to publish the app to https://www.contoso.com.

You need to perform the following tasks:

✑ Ensure that App12345678 is registered to Azure Active Directory (Azure AD).

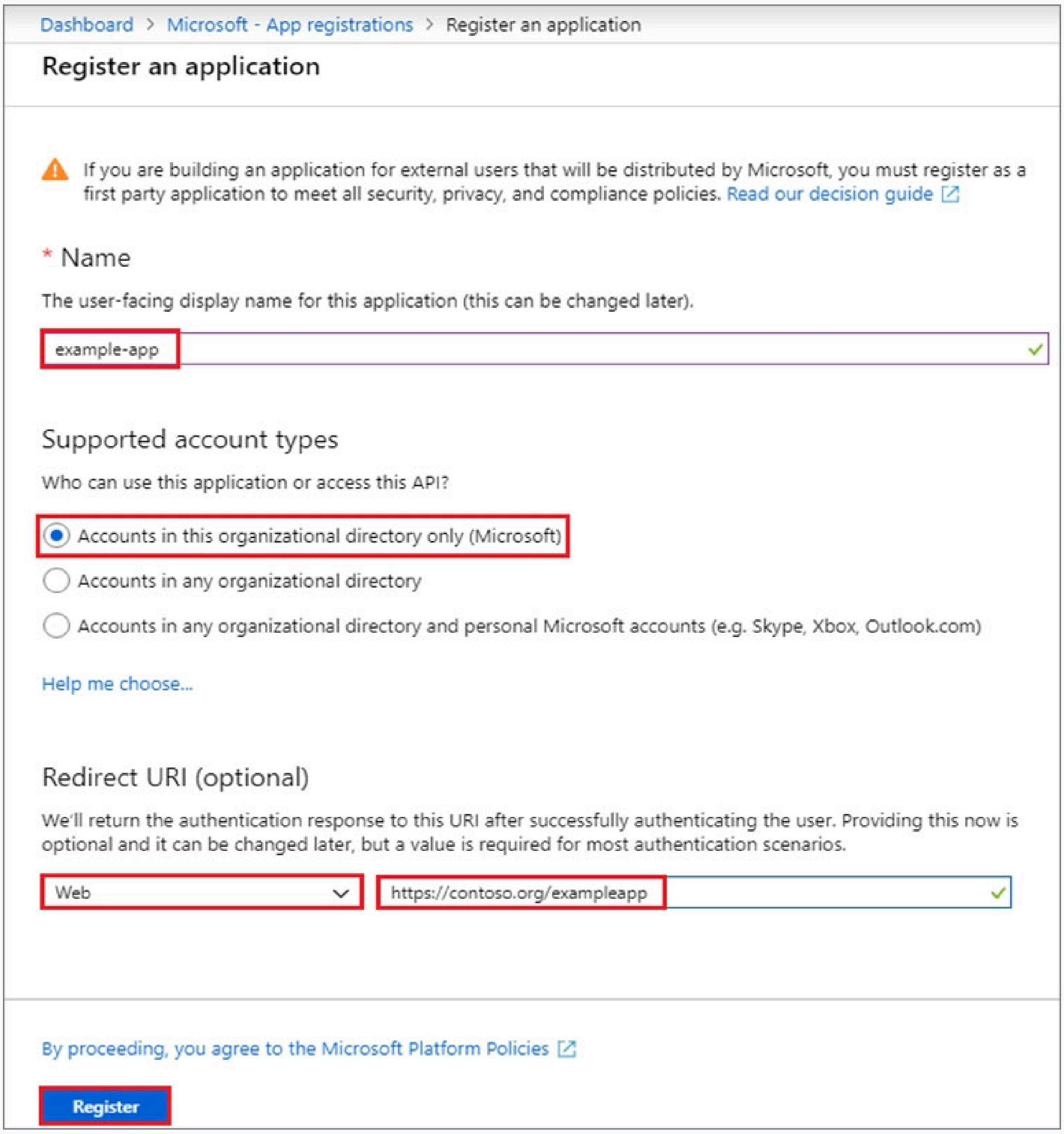
✑ Generate a password for App12345678.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

Step 1: Register the Application

1. Sign in to your Azure Account through the Azure portal.
2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application 12345678. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: https://www.contoso.com , where the access token is sent to.



Dashboard > Microsoft - App registrations > Register an application

Register an application

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://contoso.org/exampleapp ✓

By proceeding, you agree to the Microsoft Platform Policies

6. Click Register

Step 2: Create a new application secret

If you choose not to use a certificate, you can create a new application secret.

7. Select Certificates & secrets.
8. Select Client secrets -> New client secret.
9. Provide a description of the secret, and a duration. When done, select Add.

After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later. You provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

⊟ **gbx077** Highly Voted 👍 2 years, 3 months ago

on exam March 24, 2023

upvoted 9 times

⊟ **obaali1990** 2 years, 2 months ago

Where you able to solve it? Did you pass?

upvoted 1 times

⊟ **somenick** Highly Voted 👍 2 years, 9 months ago

Steps provided in the solution section looks OK to me.

upvoted 6 times

⊟ **Jimmy500** Most Recent 🕓 1 year ago

There is no way I think to add secret manually it is being generated by Azure we can only choose expiration date for secret and we can add description for it .

upvoted 1 times

⊟ **ErikPJordan** 1 year, 9 months ago

Entra ID these days, new registration button, enter name and redirect uri

upvoted 4 times

Question #30 *Topic 2*

SIMULATION -

You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com and a user named User1 in the new directory.

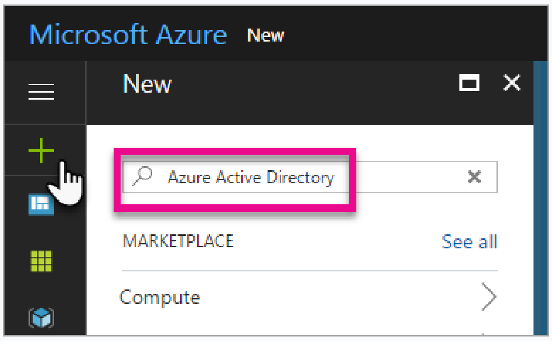
To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

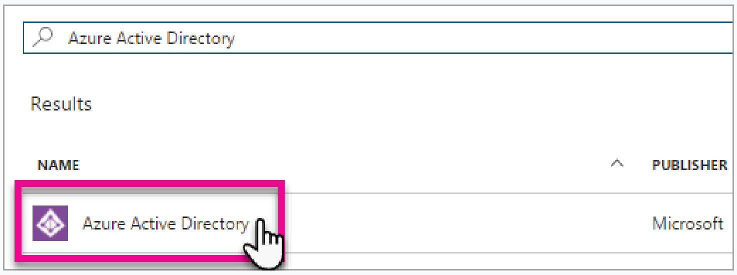
Step 1: Create an Azure Active Directory tenant

1. Browse to the Azure portal and sign in with an account that has an Azure subscription.

2. Select the plus icon (+) and search for Azure Active Directory.

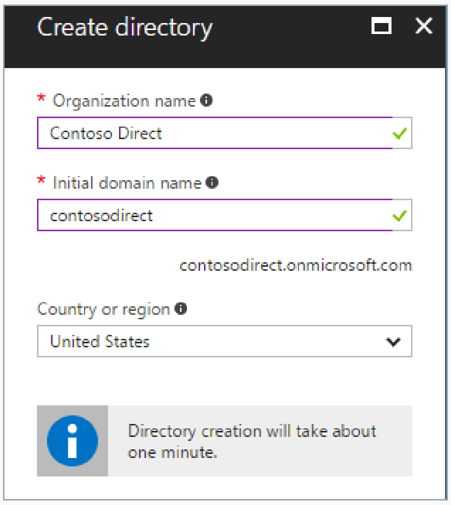


3. Select Azure Active Directory in the search results.



4. Select Create.

5. Provide an Organization name and an Initial domain name (12345678). Then select Create. Your directory is created.


Create directory

* Organization name: Contoso Direct

* Initial domain name: contosodirect

contosodirect.onmicrosoft.com

Country or region: United States

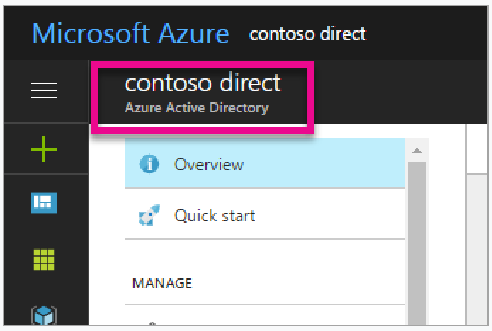
Directory creation will take about one minute.

6. After directory creation is complete, select the information box to manage your new directory.

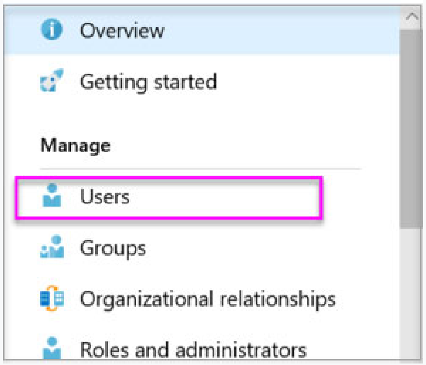
Next, you're going to add tenant users.

Step 2: Create an Azure Active Directory tenant user

7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



8. Under Manage, select Users.

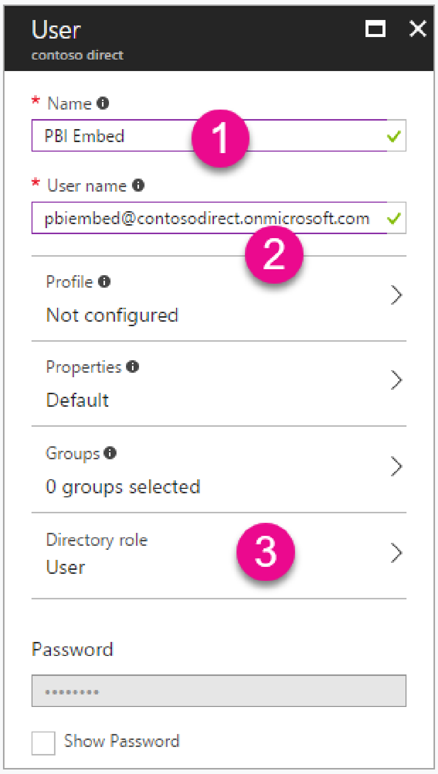


9. Select All users and then select + New user.

10. Provide a Name and User name (user1) for the regular user tenant. You can also show the temporary password. When you're done, select Create.

Name: user1 -

User name: user1@12345678.onmicrosoft.com



User
contoso direct

* Name: PBI Embed

* User name: pbiembed@contosodirect.onmicrosoft.com

Profile: Not configured

Properties: Default

Groups: 0 groups selected

Directory role: User

Password: ••••••••

□ Show Password

Reference:

https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

BinuHaneef Highly Voted 3 years ago

New structure is different,
From the Azure portal menu, select Azure Active Directory.
On the overview page, select Manage tenants
then create new directory
Select Create.

upvoted 21 times

OpsecDude 2 years, 3 months ago

Yeap, just checked that out. Correct.

upvoted 1 times

gbx077 Highly Voted 1 year, 9 months ago

# Exam Question March 24, 2023

upvoted 6 times

DjoCh Most Recent 11 months, 2 weeks ago

For simulation questions, do we need to have an account, or one already provided in the exam environment? thx

upvoted 1 times

⊟ **jacobtriestech** 8 months, 2 weeks ago

Provided to you

upvoted 2 times

⊟ **sarath** 2 years, 1 month ago

The solution is correct. Just verified the same on my personal subscription. If you don't have any AAD setup already, you just need to select the AAD option in the basics tab of create tenant. Works from a test point of view.

upvoted 1 times

⊟ **sinh** 2 years, 2 months ago

What should I answer for this?

upvoted 1 times

⊟ **imie** 2 years, 12 months ago

in Exam 31 Dec 2021.

upvoted 4 times

⊟ **adamsca** 3 years ago

# Exam Question 12/10/2021

upvoted 2 times

⊟ **adamsca** 3 years ago

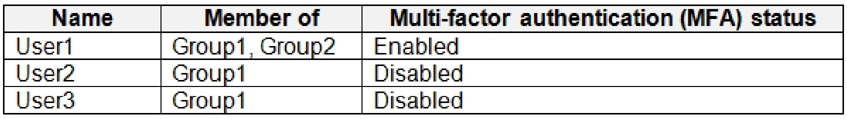
# Exam Question 12/10/2021

upvoted 1 times

Question #31 Topic 2

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

✑ Assignments: Include Group1, exclude Group2

✑ Conditions: Sign-in risk level: Medium and above

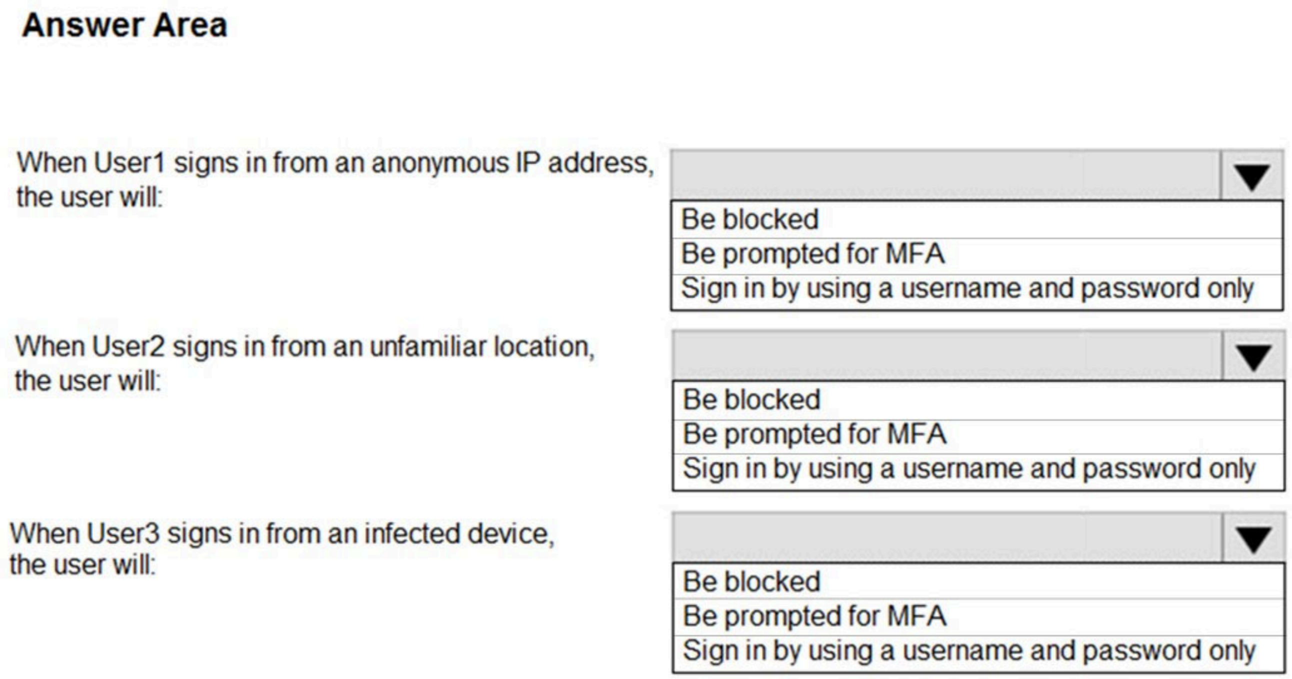
✑ Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

What should you identify for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

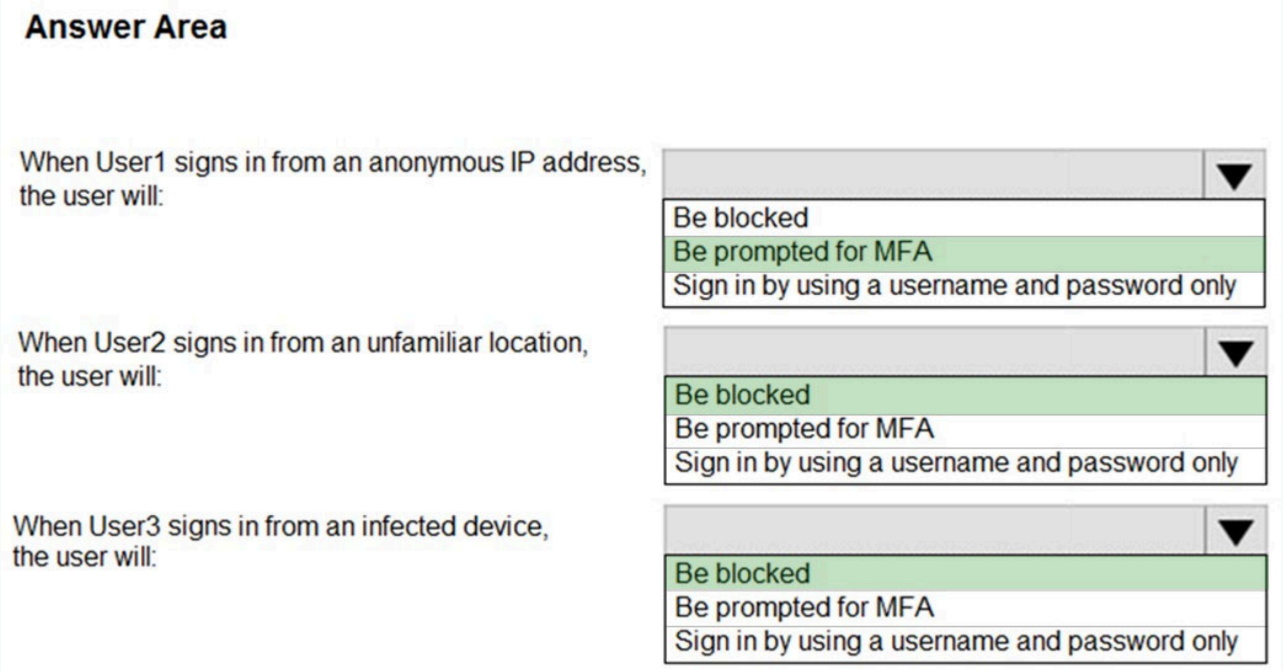
When User2 signs in from an unfamiliar location, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

Suggested Answer:



Answer Area

When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- [✓ Be prompted for MFA]
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

References:

http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/ https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Bjarki2330 Highly Voted 👍 3 years, 11 months ago

Answers are correct:

1) MFA is enabled and whenever on next log-in he will have to sign up anyway, regardless of the policy, therefore prompted.

2) Blocked - "Users must register for Azure AD MFA and SSPR before they face a situation requiring remediation. Users not registered are blocked and require administrator intervention."

3) Blocked - See text in 2)

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

upvoted 87 times

Hot_156 4 months ago

When Azure AD Identity Protection requires MFA for a sign-in and the user has MFA disabled, the behavior depends on the specific policy configuration. If the policy is set to "allow access, request MFA," Identity Protection will prompt the user to register for MFA during the sign-in process. This means that even if MFA is disabled for the user, they will be required to complete the MFA registration and verification to gain access.

upvoted 1 times

Hot_156 4 months ago

Ignore this. It will be blocked

upvoted 1 times

pentium75 11 months ago

MFA is "enabled" which means that it is NOT enforced and he will NOT "have to sign up anyway".

"Enabling MFA for a user means that the user has the option to set up MFA, but it is not required. Enforcing MFA means that the user is required to set up MFA and cannot access their account until they have completed the MFA setup process. "

upvoted 2 times

BillBaits 3 years, 7 months ago

According to the official Skillpipe book, "sign-ins from infected devices" are considered as "low".

upvoted 17 times

BP_lobster 3 years, 3 months ago

you are correct imho/number 3 would now be Username & password

upvoted 5 times

BP_lobster 3 years, 3 months ago

Source: https://github.com/toddkitta/azure-content/blob/master/articles/active-directory/active-directory-identityprotection-risk-events-types.md

(official github repo, states "sign-ins from infected devices" are considered classified as "low")

upvoted 2 times

azure_2563 1 year, 9 months ago

User3 will be blocked:

Reason- sign-ins from infected devices is considered as "Medium" so policy will be applied. Since user3 is MFA enabled it will be blocked.

upvoted 2 times

xRiot007 11 months, 2 weeks ago

Sign in from infected devices is "Low". If things go south and user credentials are leaked that is "High".

upvoted 1 times

azure_2563 1 year, 9 months ago

sorry MFA is disabled so admin action is required.

upvoted 2 times

canonigo Highly Voted 👍 4 years, 3 months ago

1- Prompt for MFA -> User is excluded, but MFA is Enabled, user is always prompted for MFA.

2.- Prompt for MFA -> Risk is medium and policy applies

3.- Single Authentication -> Policy doesn't apply, risk low

upvoted 72 times

eroms 4 years, 1 month ago

User 3 --> Prompted for MFA

upvoted 4 times

cjace 4 years, 1 month ago

MFA MFA MFA

upvoted 26 times

Denn81 4 years, 1 month ago

Sign-ins from infected devices - Medium thus MFA

upvoted 10 times

Payday123 3 years, 4 months ago

That would correct for Conditional Access but question is about Identity Protection. According to Microsoft: "Users must register for Azure AD MFA and SSPR before they face a situation requiring remediation. Users not registered are BLOCKED and require administrator intervention."

upvoted 13 times

OhBee 4 years, 3 months ago

I respectfully disagree with number 2, although I stand to be corrected.

2.- Be blocked --> Risk is medium and policy applies, HOWEVER MFA is disabled for User 2 and this he/she is blocked.

upvoted 8 times

3abmula 4 years ago

Even if MFA is disabled, since conditional access policy applied, user will be prompted for MFA enrollment, and to login using MFA. And by the way, even after the user activates MFA, status will remain disabled for that user, because it will be only used when a conditional access policy is met.

upvoted 8 times

gigiscula 3 years, 9 months ago

This is not Conditional Access. It is Identity Protection, and as stated by docs if the user isn't enrolled in MFA, it will be blocked.

upvoted 11 times

Stews 3 years, 2 months ago

Not true, this is the legacy method of assigning mfa to users. Security baselines means that all tenants have mfa enforced by default anyways. It should be managed via CA and being disabled here means nothing. I think this question is ancient, but I still wanted to add this.

upvoted 5 times

macco455 4 years, 3 months ago

Yes MFA is disabled for User 2 on his account, BUT since he matches the policy he will need to use MFA to log in now as the policy supercedes his AAD settings. Therefore User 2 will be Prompted for MFA

upvoted 9 times

gumibobo Most Recent 1 year, 4 months ago

right answers

upvoted 1 times

heatfan900 1 year, 10 months ago

USER 1 WILL ALWAYS BE PROMPTED REGARDLESS OF POLICY ASSIGNMENT BECAUSE MFA IS ENFORCED AGAINST THEIR ACCT.

USER 2 WILL BE BLOCKED BECAUSE THEY ARE SOLELY IN GROUP 1 AND THE MEET THE CONDITIONS OF THE POLICY ASSIGNED WITH MFA DISABLED WHICH GOES AGAINST THE POLICY REQUIREMENTS.

USER 3 WILL BE ALLOWED TO LOGIN WITH USERNAME AND PASSWORD ONLY BECAUSE, ALTHOUGH THEY ARE IN GROUP 1 THEY DO NOT MEET THE CONDITIONS AND DO NOT HAVE MFA ENFORCED DIRECTLY AGAINST THEIR ACCT. SIGNING IN FROM AN INFECTED DEVICE IS CONSIDERED LOW RISK..

upvoted 8 times

pentium75 11 months ago

No, MFA is "enabled", not "enforced".

upvoted 2 times

majstor86 2 years, 3 months ago

MFA

Blocked

Username and password

upvoted 5 times

ltjones12 2 years, 5 months ago

The first 2 are correct, the third is "sign in with username and pw only". It's low risk, and MFA is disabled for the user

upvoted 3 times

TweetleD 2 years, 7 months ago

sign ins from an infected device is classified as a low risk so user3 will be able to sign in by using a username and password only

upvoted 2 times

somenick 2 years, 9 months ago

Latest update: Microsoft doesn't provide specific details about how risk is calculated. Each level of risk brings higher confidence that the user or sign-in is compromised.

So this question is obsolete

upvoted 10 times

Fal991l 2 years, 7 months ago

It's still good practice though

upvoted 1 times

fro_prince 2 years, 10 months ago

2 and 3 - blocked

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

upvoted 2 times

Ivanvazovv 2 years, 10 months ago

All "Sign in from unfamiliar location", "Sign in from infected device" and "Sign in from anonymous IP address" are medium risk thus all satisfy the condition to require MFA. User1 will be prompted from MFA regardless. So all three sign ins require MFA.

upvoted 1 times

certmonk 3 years, 1 month ago

All 3 should be prompted for MFA. Because all of them are in Group1 and the Access level is set to Allow access Require MFA. For 2 and 3 the user should still be prompted for MFA but since they have MFA disabled so they will not be able to proceed with MFA.

upvoted 2 times

DaveBinDC 3 years, 2 months ago

Answers are correct.

The key here is that user MUST complete MFA registration for the identity protection sign-in risk policy to take effect. Since USER1 is the only one that is MFA enabled (registered), he is the only one that will be forced to use MFA to sign in. The other two will be blocked. https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

upvoted 1 times

CJ32 3 years, 5 months ago

1.) Username and Password only. User is a part of Group 2. Exclusion takes precedence.

2.) Blocked. User MUST sign up for MFA beforehand or they will be blocked. (https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies)

3.) Blocked. Same reasoning as above.

upvoted 3 times

stack120566 3 years, 5 months ago

1. Sign in Username and Pw only .. user1 is member of group 2 (excluded from risk policy)

2. Blocked .. MFA required but User 2 MFA status is disabled

3. Sign In with UserName and Pw only... Low risk so policy does not apply

upvoted 3 times

Payday123 3 years, 4 months ago

1. User1 is MFA in user's properties

upvoted 3 times

[Removed] 3 years, 5 months ago

MFA

Blocked

Single Authentication

upvoted 3 times

snake_alejo 3 years, 6 months ago

my answers based on that:

user1 will ask MFA for being a medium threat.

user2 will ask for MFA for being a medium type threat (unfamiliar location.)

User 3 does not apply the policy since the risk, according to Microsoft, is low.

in no case user 1 and 2 are blocked.

upvoted 1 times

Patchfox 3 years, 6 months ago

As gigiscual said: Users must register for Azure AD MFA and SSPR BEFORE they face a situation requiring remediation. Users not registered are blocked and require administrator intervention.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

So, User2 will be blocked.

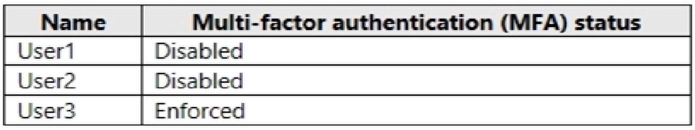
But I do not agree with answer three because Microsoft classify sign-ins from infected devices with low risk.

upvoted 4 times

Question #32 *Topic 2*

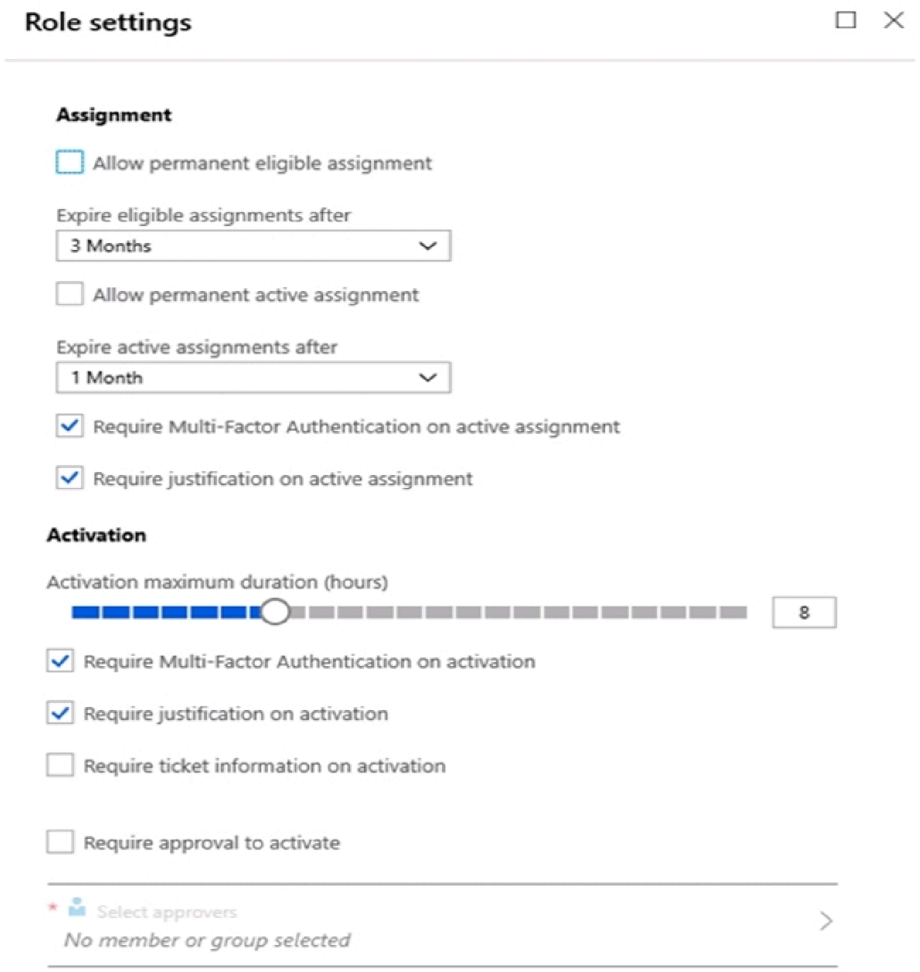
HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Disabled
User3	Enforced

In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)



Role settings

Assignment

☐ Allow permanent eligible assignment

Expire eligible assignments after: 3 Months

☐ Allow permanent active assignment

Expire active assignments after: 1 Month

☑ Require Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Activation

Activation maximum duration (hours): 8

☑ Require Multi-Factor Authentication on activation

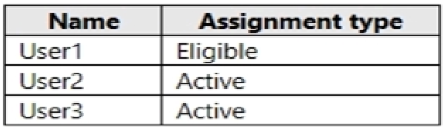
☑ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

* Select approvers
No member or group selected

You assign users the Contributor role on May 1, 2019 as shown in the following table.

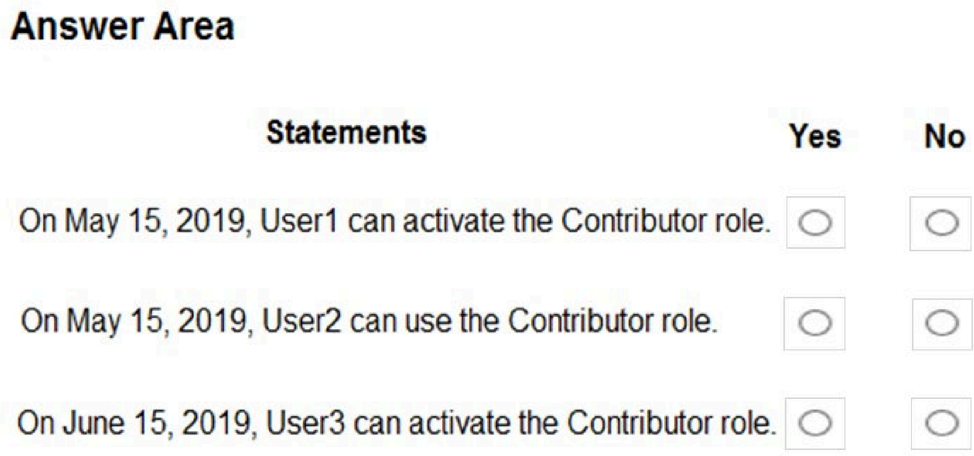


Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

NOTE: Each correct selection is worth one point.

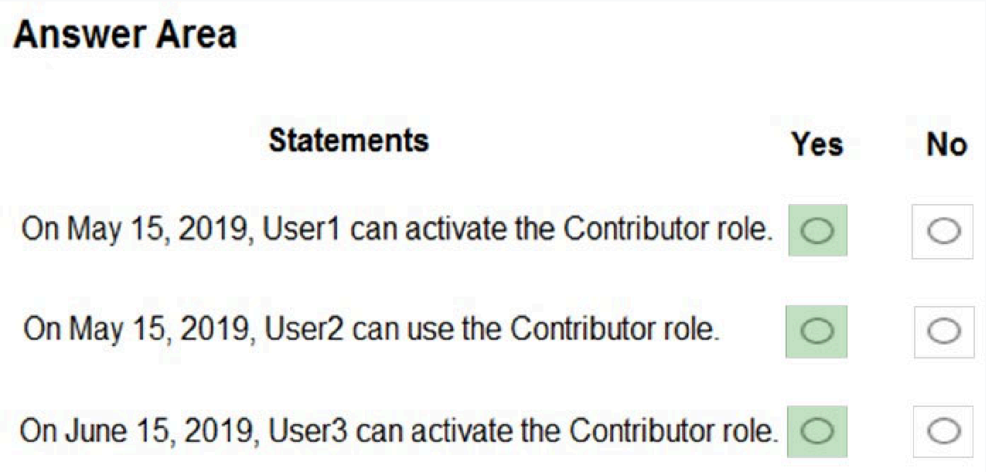
Hot Area:



Answer Area

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	○	○
On May 15, 2019, User2 can use the Contributor role.	○	○
On June 15, 2019, User3 can activate the Contributor role.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	[✓ ○]	○
On May 15, 2019, User2 can use the Contributor role.	[✓ ○]	○
On June 15, 2019, User3 can activate the Contributor role.	[✓ ○]	○

References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

hang10z Highly Voted 4 years, 3 months ago

The answer is YES, YES, NO. MFA Disabled/Enabled means nothing, its there to trick you. That is for 0365 only "Basic" MFA which wouldn't be in use at this point since in order to use PIM you must have EMS E5 licenses/P2 AD so those MFA enable/disabled settings are ignored. They would just get an MFA enrollment wizard/prompt to setup their phone first.

upvoted 102 times

rgullini 4 years, 2 months ago

MFA disabled/enabled means nothing if you have "Security defaults" enabled in Azure AD. If Security Defaults" are disabled, then the MFA configuration applies.

upvoted 6 times

abcd1234000 3 years, 9 months ago

Thanks for great explanation!

upvoted 2 times

Startkabels 4 years, 3 months ago

Could be, our company has that configuration and my own MFA status is disabled when checking from AAD > Security > MFA > Additional cloud-based MFA settings.

This link takes you to https://account.activedirectory.windowsazure.com/ where you can find MFA settings per user where MFA is disabled for all our users.
So I would go with you and say that using PIM which requires an AAD P2 license ignores this setting

upvoted 1 times

OhBee 4 years, 3 months ago

I think you might be overthinking this. If MFA is disabled, we must assume that the user has not yet even registered to it. So he must register first.

Now if asking for registration and then allowing them in is considered as a YES by MS, I have no idea...but I would go with NO on the first one.

upvoted 1 times

Narragr Highly Voted 4 years, 3 months ago

User3 cannot because his active right is expired on the 15th June 2019

upvoted 28 times

Geeky93 4 years, 3 months ago

How can User2 use contributor role if he has MFA disabled ? For me it seems to be No No NO

upvoted 8 times

sureshatt 4 years, 3 months ago

MFA status for user DOES NOT MATTER (for PIM, Conditional Access Control and Identity Protection). That is, PIM, Conditional Access Control and Identity Protection will prompt to setup MFA regardless the user MFA status.

upvoted 16 times

gcpbrig01 4 years, 3 months ago

also user1 can't activate the role since activation requires MFA and its is disabled for the user and user2 is role activated when logged in on May 15, 2019.
No, Yes, No
upvoted 26 times

LJack 4 years, 3 months ago
Agree, no yes no
upvoted 8 times

SofiaLorean Most Recent 3 months, 3 weeks ago
Yes, Yes, No?
upvoted 1 times

ITFranz 8 months ago
To support the answer #2.

Microsoft Entra PIM for Azure resources provides two distinct assignment types:

Eligible assignments require the member to activate the role before using it. Administrator may require role member to perform certain actions before role activation, which might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

Active assignments don't require the member to activate the role before usage. Members assigned as active have the privileges assigned ready to use. This type of assignment is also available to customers that don't use Microsoft Entra PIM.
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-resource-roles-assign-roles

Answer: Yes, YES, NO
upvoted 3 times

Hot_156 4 months, 1 week ago
N - User 1 has MFA disabled. PIM won't prompt the user to register as CA does.
Y - The role is already enabled
N - Active assignment already expired
upvoted 1 times

Hot_156 3 months, 4 weeks ago
Y - PIM and CA prompt users to register for MFA! Identity Protection DOESNT!
Y - The Role is already enabled
N - Active assignment already expired
upvoted 1 times

AZ500Xmen 9 months, 1 week ago
Yes Yes No.

MFA doesn't matter here.
User 3 cannot activate PIM because it has expired. A user cannot have both Active and Eligible assignments, so after 15 June, User 3 has no PIM roles since active assignments which it was given, expires 1st June.
upvoted 1 times

ch23rr 10 months, 4 weeks ago
the answer is N Y N.
upvoted 4 times

pentium75 11 months ago
Yes, Yes, No. The per-user MFA setting is completely irrelevant.
upvoted 1 times

AZ5002023 1 year, 6 months ago
YYY
mfa is disabled but he can activate it when he activate the role
User3 the activate's state expired , but the question here is to ACTIVATE NOT USE like the second question
upvoted 5 times

wardy1983 1 year, 7 months ago

YES, YES, NO.
MFA Disabled/Enabled means nothing, its there to trick you. That is for 0365 only "Basic" MFA which wouldn't be in use at this point since in order to use PIM you must have EMS E5 licenses/P2 AD so those MFA enable/disabled settings are ignored. They would just get an MFA enrollment wizard/prompt to setup their phone first.

upvoted 4 times

JunetGoyal 1 year, 8 months ago

YEs,yes, no.
User 3 active role expire after a month! so on june 15 he cannot active .
User 2 has active assignment
user1 is eligible can activate

upvoted 3 times

heatfan900 1 year, 10 months ago

IT CLEARLY STATES MFA FOR ACTIVATION OF ELIGIBLE AND MFA FOR ACTIVE ASSIGNMENTS. N,N,Y

upvoted 1 times

Mnguyen0503 1 year, 5 months ago

You're incorrect. MFA for active assignment is only applied to the admin assigning the active role, there's no "activation" required for the admins receiving those assignments.

upvoted 1 times

Yesvanth1 2 years ago

Answers are correct - YYY: Box-3: After the active role is expired on May 30th, only the users active access expired.
The user is still eligible for 2 more months, meaning the user can activate it on June15th.

upvoted 6 times

Tweety1972 2 years, 1 month ago

Assigned the 1st of May. On the 1st of June the Active Assignments are expired. On the 1st of August the Eligible Assignments are expired too.

User1 has an Eligible Assignment so he/she can activate his/her account -> Yes
User2 has an Active Assignment so he/she can use his/her account -> Yes
User3 has an Active Assignment which was expire after 1 months. So he/she has no longer access to this role -> No

upvoted 6 times

pekay 2 years, 2 months ago

YES, YES NO.

upvoted 3 times

majstor86 2 years, 3 months ago

Yes
Yes
No

upvoted 6 times

student9k 2 years, 4 months ago

Approvers are not able to approve their own role activation requests.
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow

upvoted 1 times

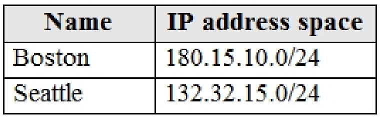
samimshaikh 2 years, 5 months ago

1. Yes, can activate because eligible
2. Yes, Can use it because already an active assignment
3. No, f a user's Privileged Identity Management (PIM) active assignment expires, the user will lose their elevated privileges and will no longer be able to perform privileged actions within the Azure AD environment.

upvoted 3 times

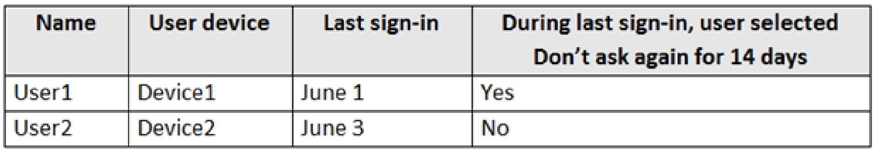
HOTSPOT -

You work at a company named Contoso, Ltd. that has the offices shown in the following table.



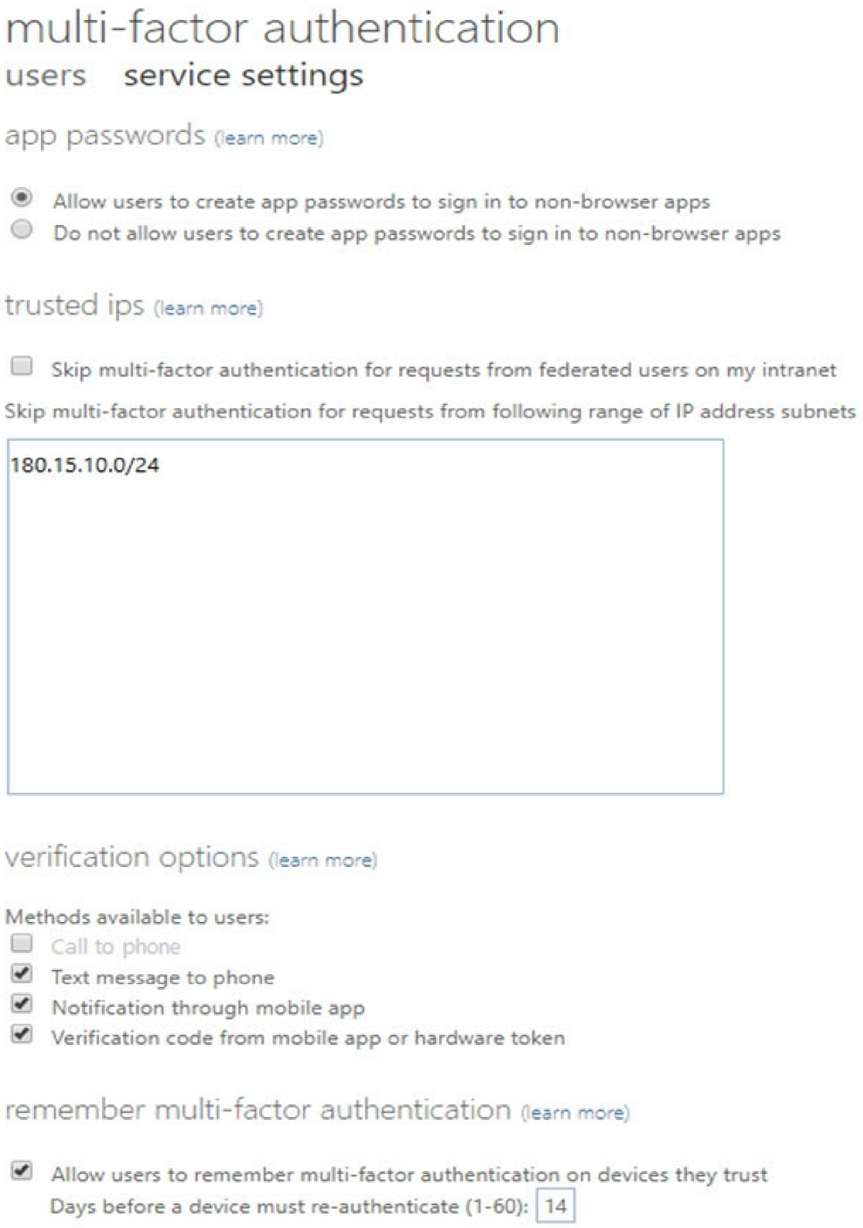
Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All contoso.com users have Azure Multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.



Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device2	June 3	No

The multi-factor authentication settings for contoso.com are configured as shown in the following exhibit.



multi-factor authentication

users service settings

app passwords (learn more)

● Allow users to create app passwords to sign in to non-browser apps

○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

□ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

verification options (learn more)

Methods available to users:

□ Call to phone

☑ Text message to phone

☑ Notification through mobile app

☑ Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

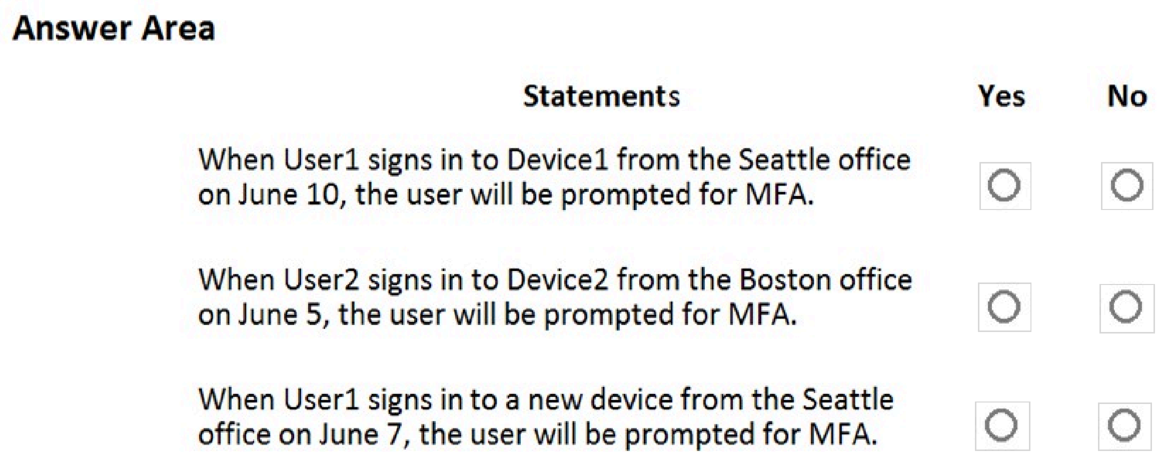
☑ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60): 14

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

NOTE: Each correct selection is worth one point.

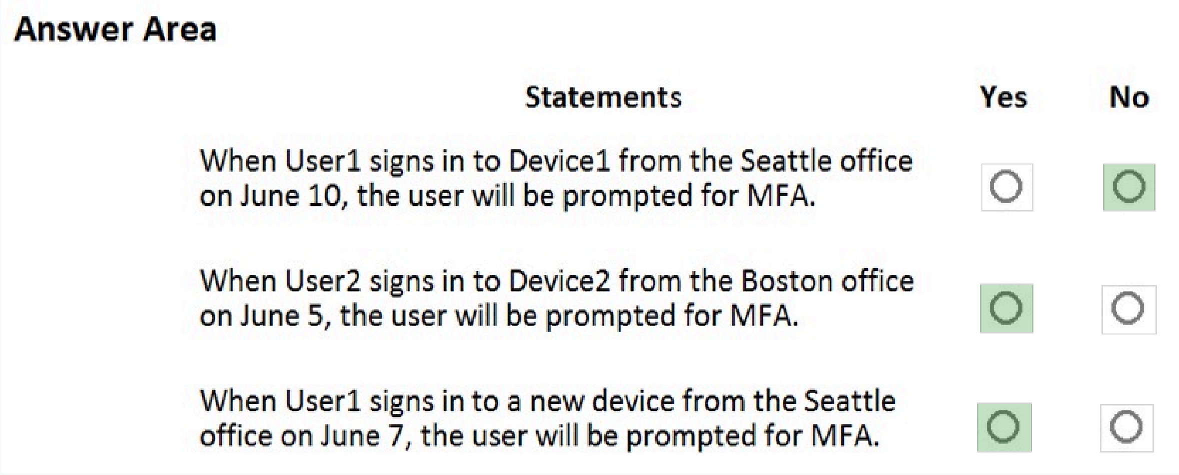
Hot Area:



Answer Area

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	○	○
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	○	○
When User1 signs in to a new device from the Seattle office on June 7, the user will be prompted for MFA.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	○	[✓ ○]
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	[✓ ○]	○
When User1 signs in to a new device from the Seattle office on June 7, the user will be prompted for MFA.	[✓ ○]	○

RameshSesetti Highly Voted 4 years, 3 months ago

Answer is : No-No-Yes.

upvoted 209 times

Narragr 4 years, 3 months ago

Why the option trusted ip is not checked

upvoted 5 times

xaccan 4 years, 3 months ago

Check box is not for trusted ip, it is for federated users

upvoted 28 times

Jimmy500 1 year, 7 months ago

There i can not see federated users

upvoted 1 times

LJack 4 years, 3 months ago

Agree should be no, no, yes

upvoted 22 times

Sethoo 4 years, 3 months ago

Agree with your answer. The user from Boston (guestion 2)will not be asked for MFA because at present , the IP address from Boston is excluded from MFA requirements

upvoted 18 times

DarkCyberGhost 3 years, 5 months ago

But the Checkbox is blank so that function has not been enabled. therefore they will be asked for MFA as the Ip Range is not being excluded.

upvoted 6 times

khengoolman 3 years, 4 months ago

Please read the function, it has nothing to do with the IP whitelist. N N Y is correct

upvoted 6 times

rockyykrish 3 years, 10 months ago

No-Yes-Yes. The second answer will be yes. Skip multifactor authentication for trusted locations is not enabled.

upvoted 23 times

rawrkadia 3 years, 10 months ago

That checkbox is to skip MFA for federated intranet locations, simply having IPs or Ranges in the text box for trusted IPs turns it on.

upvoted 32 times

Vikku30 3 years, 5 months ago

Then why do they have the check box, I guess we need to check the check-box, is it not the case?

upvoted 3 times

domtopics 2 years, 9 months ago

Check box is for when users hit the internal interface of AD FS and receive a token, regardless of public IP address they go to Azure with.

IP list is for public IP address they go to Azure with, regardless of how they authenticate.

upvoted 8 times

Pinto Highly Voted 👍 4 years, 3 months ago

Box1: No. because user1 had already signed in from device1 and had selected the 14 day period hence, won't be asked for MFA.

Box2: No because Boston IP range is trusted.

Box3: Yes because new device and Seattle IP is not trusted.

upvoted 77 times

SofiaLorean Most Recent 🕒 3 months, 3 weeks ago

No, No, Yes

upvoted 1 times

pentium75 11 months ago

No-No-Yes.

upvoted 2 times

Obama_boy 1 year, 6 months ago

in exam 08/12/23

upvoted 2 times

wardy1983 1 year, 7 months ago

Box1: No. because user1 had already signed in from device1 and had selected the 14 day period hence, won't be asked for MFA.

Box2: No because Boston IP range is trusted.

Box3: Yes because new device and Seattle IP is not trusted.

upvoted 5 times

Kiano 1 year, 2 months ago

This is exactly what Pinto said. Why comment when you have no additional information?

upvoted 1 times

TheProfessor 1 year, 9 months ago

NNY is the answer. Boston's IPs are trusted.

upvoted 2 times

ArchitectX 1 year, 9 months ago

No-No-Yes

upvoted 3 times

heatfan900 1 year, 10 months ago

N = USER 1 CHECKED THE 'DON NOT ASK ME FOR 14 DAYS' CHECKBOX

N = USER 2 IS SIGNING IN FROM A TRUSTED LOCATION WHICH BYPASSES MFA

Y = USER 1 SIGNING IN AFTER THE 14 DAYS FROM A UNTRUSTED LOCATION.

upvoted 4 times

xRiot007 11 months, 2 weeks ago

Wrong. It's Yes because user is signing in using a new device, not from an untrusted location.

upvoted 1 times

⊟ **xRiot007** 11 months, 2 weeks ago

Ignore first reply. Unstrusted location seems to be medium.

upvoted 1 times

⊟ **ESAJRR** 1 year, 11 months ago

No-Yes-Yes.
The second answer will be yes. Skip multifactor authentication for trusted locations is not enabled.

upvoted 2 times

⊟ **zellck** 2 years, 1 month ago

NNY is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips
The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Azure AD Multi-Factor Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

upvoted 1 times

⊟ **Jimmy500** 1 year, 7 months ago

Check box is not picked for second one

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication
The remember multi-factor authentication feature lets users bypass subsequent verifications for a specified number of days, after they've successfully signed in to a device by using MFA. To enhance usability and minimize the number of times a user has to perform MFA on a given device, select a duration of 90 days or more.

upvoted 1 times

⊟ **Gesbie** 2 years, 2 months ago

In Exam April 11, 2023

upvoted 6 times

⊟ **pekay** 2 years, 2 months ago

the answer is no no yes

upvoted 2 times

⊟ **r_git** 2 years, 3 months ago

No = User1 on Device1 selected Don't ask again for 14 days on June 1.

No = User2 on Device2 signs in from the Boston office IP address subnet 180.15.10.0/24 which is added in trusted ips textbox
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips

Yes = User1 signs in to a new device which triggers MFA since it is a new sign in from a new device. The previous 14 days selection was tied to session on Device1

upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

NO
NO
YES

upvoted 2 times

⊟ **fonte** 2 years, 5 months ago

Hi all,
Passed my exam (13JAN2023) with 918.
50 questions (45 + 5 of a case study).
Around 95% of the questions are here.
I've compiled the questions and my answers in a ppt, feel free to check it out and hope it helps.
https://www.dropbox.com/s/ay00xp2fnloq1ex/AZ%20500%20-%20Exam%20Topics.pptx?dl=0
Use pass az500prep to open the file.

Thanks to all the people that comment on questions, I wouldn't have passed without them :)

upvoted 3 times

⊟ **Tweety1972** 2 years, 2 months ago

Doesn't work

upvoted 1 times

⊟ **josh_josh** 2 years, 6 months ago

The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Azure AD Multi-Factor Authentication prompt.

upvoted 2 times

Question #34 *Topic 2*

You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.
What are two possible effects of the change? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Role assignments at the subscription level are lost.

B. Virtual machine managed identities are lost.

C. Virtual machine disk snapshots are lost.

D. Existing Azure resources are deleted.

Suggested Answer: *AB*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

Community vote distribution

AB (100%)

⊟ **Exam_Master_Me** Highly Voted 4 years, 11 months ago
Review the following list of changes that will occur after you associate or add your subscription, and how you might be affected:

Users that have been assigned roles using RBAC will lose their access
Service Administrator and Co-Administrators will lose access
If you have any key vaults, they'll be inaccessible and you'll have to fix them after association
If you have any managed identities for resources such as Virtual Machines or Logic Apps, you must re-enable or recreate them after the association
If you have a registered Azure Stack, you'll have to re-register it after association

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory
upvoted 41 times

⊟ **tuta** Highly Voted 4 years, 6 months ago
tested - AB
upvoted 29 times

⊟ **workhard** Most Recent 11 months, 2 weeks ago
This is a more updated documentation
https://learn.microsoft.com/en-us/azure/role-based-access-control/transfer-subscription#understand-the-impact-of-transferring-a-subscription
upvoted 2 times

⊟ **ESAJRR** 1 year, 11 months ago
Selected Answer: AB
A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago
Selected Answer: AB
A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
upvoted 1 times

⊟ **us3r** 3 years, 2 months ago
Selected Answer: AB
captain obvious
upvoted 4 times

⊟ **Eltooth** 3 years, 3 months ago
Selected Answer: AB

A & B are correct.

upvoted 3 times

AS179 3 years, 6 months ago

Selected Answer: AB

Correct

upvoted 4 times

LDodge 3 years, 6 months ago

Selected Answer: AB

Correct

upvoted 2 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 1 times

Jco 3 years, 9 months ago

#exam question # 29 Sep

upvoted 2 times

francis6170 3 years, 9 months ago

Got this in the AZ-500 exam (Sept 2021)! A: A&B

upvoted 4 times

swi48 3 years, 11 months ago

AB should the correct answer

upvoted 1 times

kumax 4 years ago

On exam, May 2021.

upvoted 3 times

SandroAndrade 4 years, 1 month ago

Correct Answer

upvoted 2 times

teehex 4 years, 1 month ago

A and B are correct answers.

When you change to a different Azure AD tenant your user identities are changed to. This basically mean the role assignment assigned to those identities are no longer valid.

When you enable a system-assigned managed identity an identity is created in Azure AD that is tied to the lifecycle of that service instance. So if you change to different Azure AD such an identity is no longer valid.

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#managed-identity-types

upvoted 5 times

JohnYinToronto 4 years, 3 months ago

Answer correct. AB

upvoted 3 times

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 have an Azure subscription named Sub1.
You have an Azure Storage account named sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to sa1.
Solution: You generate new SASs.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
Reference:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

Community vote distribution

B (100%)

PDR Highly Voted 4 years, 10 months ago
I agree with B as just creating a new one does not effect the currently created SASs - so either delete, rename as stated or you could also regenerate the KEY used to create the SAS which would have teh effect of disabling all SASs created with that previous generated key.
upvoted 31 times

gfhbox0083 Highly Voted 4 years, 6 months ago
B, for sure.
upvoted 11 times

Ivan80 Most Recent 11 months ago
In exam 1/28/24
upvoted 2 times

Obama_boy 1 year ago
in exam 08/12/23
upvoted 3 times

trashbox 1 year, 2 months ago
Selected Answer: B
The question was given on the October 9, 2023 exam.
upvoted 3 times

ESAJRR 1 year, 5 months ago
Selected Answer: B
B, for sure.
upvoted 1 times

johansson73 1 year, 5 months ago
In Exam July 2023 (1 case study.no lab)
upvoted 1 times

Gesbie 1 year, 8 months ago
In Exam April 11, 2023

upvoted 1 times

⊟ **majstor86** 1 year, 10 months ago

Selected Answer: B

B: NO is answer

upvoted 1 times

⊟ **majstor86** 1 year, 10 months ago

B: NO is answer

upvoted 1 times

⊟ **sarath** 2 years, 1 month ago

Selected Answer: B

The old SAS need to be revoked for the expected behaviour to be implemented

upvoted 2 times

⊟ **Diallo18** 2 years, 2 months ago

In Exam 10/18/2022. One case study (6 Ques), no lab.

upvoted 2 times

⊟ **Amit3** 2 years, 3 months ago

# In EXAM - 01-Oct-2022, 1 Case Study (6 ques), no Labs, Plus 44 Ques.

upvoted 1 times

⊟ **BlackZeros** 2 years, 3 months ago

This whole case study was in exam September 15, 2022

upvoted 2 times

⊟ **MoFami** 2 years, 6 months ago

In Exam 01/07/2022

upvoted 2 times

⊟ **Exams_Prep_2021** 2 years, 6 months ago

In Exam - 20/6/2022 - 1 Case Study (6) - Lab (10 Tasks)

upvoted 2 times

⊟ **Eltooth** 2 years, 9 months ago

Selected Answer: B

Orrery answer is B

upvoted 1 times

Question #36 *Topic 2*

You have an Azure subscription that contains virtual machines.
You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop.
What should you do first?

A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.

B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.

C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.

D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

Community vote distribution
C (94%) 6%

⊟ **Exam_Master_Me** Highly Voted 4 years, 11 months ago
Correct, https://docs.microsoft.com/nl-nl/azure/security-center/security-center-just-in-time
upvoted 38 times

⊟ **Pinto** Highly Voted 4 years, 3 months ago
C. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc
upvoted 9 times

⊟ **workhard** Most Recent 11 months, 2 weeks ago
Selected Answer: C
https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage#request-access-to-a-jit-enabled-vm-from-the-azure-virtual-machines-connect-page
upvoted 1 times

⊟ **TheProfessor** 1 year, 9 months ago
Correct Answer: C
upvoted 1 times

⊟ **ESAJRR** 1 year, 11 months ago
Selected Answer: C
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
upvoted 2 times

⊟ **zellck** 2 years, 1 month ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage#request-access-to-a-jit-enabled-vm-from-microsoft-defender-for-cloud
upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago
Selected Answer: C
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
upvoted 3 times

⊟ **nqwang** 2 years, 9 months ago
Selected Answer: C
correct answer
upvoted 2 times

⊟ **mohamed1999** 2 years, 10 months ago

Selected Answer: B

you need owner rights first on te vm to change the rules in the nsg, so i guess it is B

upvoted 1 times

pentium75 11 months ago

You don't want to "change the rules in the NSG", you want to "access" the VM.

upvoted 1 times

mohamed1999 2 years, 10 months ago

I see it now, you need to request it form "Microsoft Defender for Cloud" and not from PIM.

upvoted 1 times

OpsecDude 2 years, 9 months ago

But the question is not mentioning any changes to any NSG that might affect the VM, just an access request after configuring JIT

upvoted 3 times

Alessandro365 3 years ago

Selected Answer: C

correct answer

upvoted 3 times

Eltooth 3 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 4 times

rohitmedi 3 years, 7 months ago

correct answer

upvoted 2 times

abcd1234000 3 years, 9 months ago

correct

upvoted 2 times

LazyEngineer 3 years, 11 months ago

Correct

upvoted 2 times

zic04 4 years, 5 months ago

Agree correct

upvoted 6 times

tuta 4 years, 6 months ago

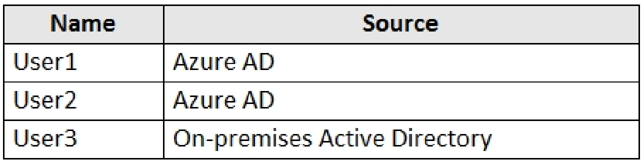
correct

upvoted 5 times

Question #37 Topic 2

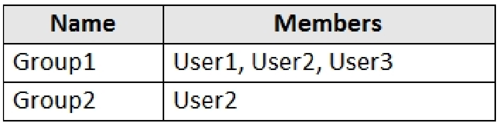
HOTSPOT -

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.



Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

✑ Assignments:

- Include: Group1

- Exclude: Group2

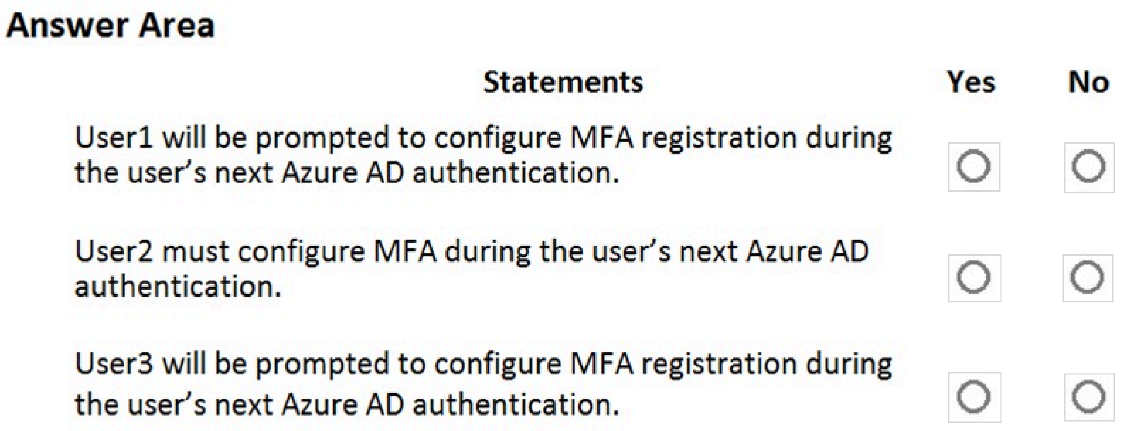
✑ Controls: Require Azure MFA registration

✑ Enforce Policy: On

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

NOTE: Each correct selection is worth one point.

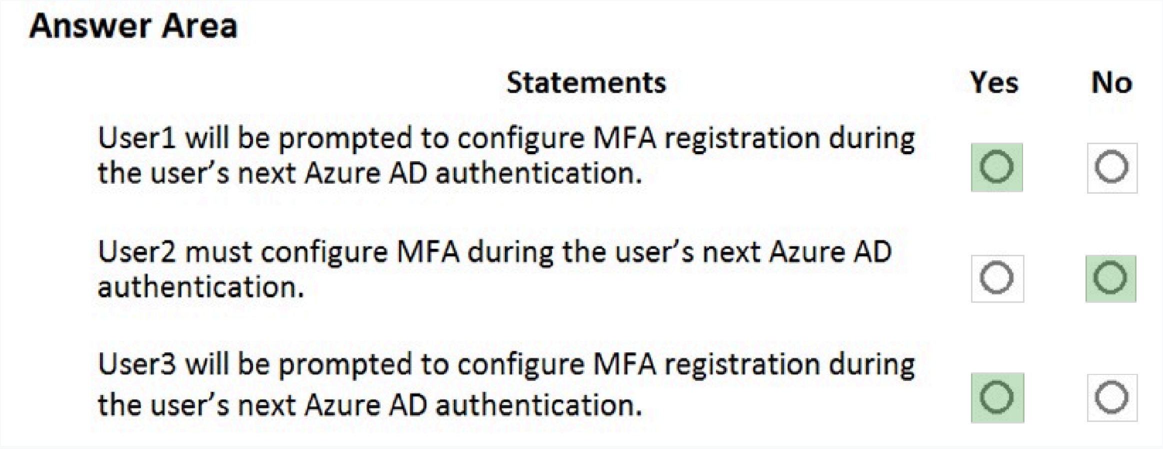
Hot Area:



Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○
User2 must configure MFA during the user's next Azure AD authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	[✓ ○]	○
User2 must configure MFA during the user's next Azure AD authentication.	○	[✓ ○]
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	[✓ ○]	○

Jhonsteve83 Highly Voted 4 years, 3 months ago

Answer is correct : Yes-No-Yes

upvoted 66 times

teehex Highly Voted 4 years, 1 month ago the only exception here is User2 because it belongs to Group2 which is excluded in the Policy.

Yes - No - Yes

upvoted 24 times

⊟ **SofiaLorean** Most Recent 3 months, 1 week ago

Yes, No, Yes

upvoted 1 times

⊟ **goalkiller** 1 year, 2 months ago

in exam today 53 q 5 casestudy -- no lab -- (in test center)

upvoted 5 times

⊟ **wydad** 1 year, 2 months ago

there is any news questions, not listed in this dump ?

upvoted 1 times

⊟ **Weerayuth** 1 year, 6 months ago

I am not sure about "MFA registration" and "during the user's next Azure AD authentication". For the next Azure AD authentication one should not conduct "MFA registration" again since he/she shoul already did the MFA registration.

upvoted 1 times

⊟ **pentium75** 11 months ago

Question assumes that "you configure MFA", which indicates that it hasn't been configured before and your users are not registered yet.

upvoted 1 times

⊟ **xRiot007** 11 months, 2 weeks ago

Not if the user has legacy login without MFA, prior to this.

upvoted 1 times

⊟ **heatfan900** 1 year, 10 months ago

Y = USER 1 IS ONLY ASSIGNED TO GROUP 1 WHICH ENFORCES MFA REGISTRATION.

N = USER 2 BELONGS TO, BOTH, GROUP 1 AND 2 WHICH IS EXCLUDED. WHEN THERE IS A CONFLICT THE EXCLUSION WINS OUT.

Y = USER 3 BELONGS SOLELY TO GROUP 1 AS DOES USER 1 AND WILL NEED TO REGISTER WITH MFA DO TO THE ENFORECMENT.

upvoted 19 times

⊟ **timHAG** 1 year, 10 months ago

isn't user three bieng in differeing onprem active directory? hence AAD MFA would not apply to him? hence third option is NO

upvoted 2 times

⊟ **ESAJRR** 1 year, 11 months ago

YES

NO

YES

upvoted 2 times

⊟ **zellck** 2 years, 1 month ago

YNY is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#policy-configuration

Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts.

upvoted 2 times

⊟ **majstor86** 2 years, 3 months ago

YES

NO

YES

upvoted 3 times

⊟ **samimshaikh** 2 years, 5 months ago

f a user (User B) is a member of two groups in Azure AD (Group 1 and Group 2), and an MFA policy is enforced only for Group 1, while Group 2 is excluded, the following will occur when User B logs on:

If User B attempts to access a resource that is protected by the MFA policy and they are accessing the resource as a member of Group 1, they will be prompted to perform MFA.

If User B attempts to access a resource that is not protected by the MFA policy, or if they are accessing the resource as a member of Group 2, they will not be prompted to perform MFA.

In other words, the MFA policy will only apply to User B when they access resources as a member of Group 1. When accessing resources as a member of Group 2, the user will not be required to perform MFA. In this case, Group 2 user is accessing resources which excluded for MFA... I am satisfied with answer Yes, No, Yes

upvoted 2 times

certmonk 3 years, 1 month ago

The magic statement is "Require mfa REGISTRATION"

upvoted 4 times

Eltooth 3 years, 3 months ago

Yes - No _ Yes is correct answer.

upvoted 1 times

siobhan1 3 years, 3 months ago

## On today's exam 03/12/2022 ##

upvoted 4 times

cfsxtuv33 3 years, 4 months ago

Hey look at that...they got it right!

upvoted 7 times

macka2005 2 years, 6 months ago

For a change...

upvoted 2 times

CJ32 3 years, 5 months ago

YES - NO - YES

Exclusion takes precedence over inclusion

upvoted 1 times

Cessyd 3 years, 5 months ago

On today's exam 06/01/22

upvoted 3 times

Question #38 *Topic 2*

SIMULATION -

The developers at your company plan to publish an app named App12345678 to Azure.

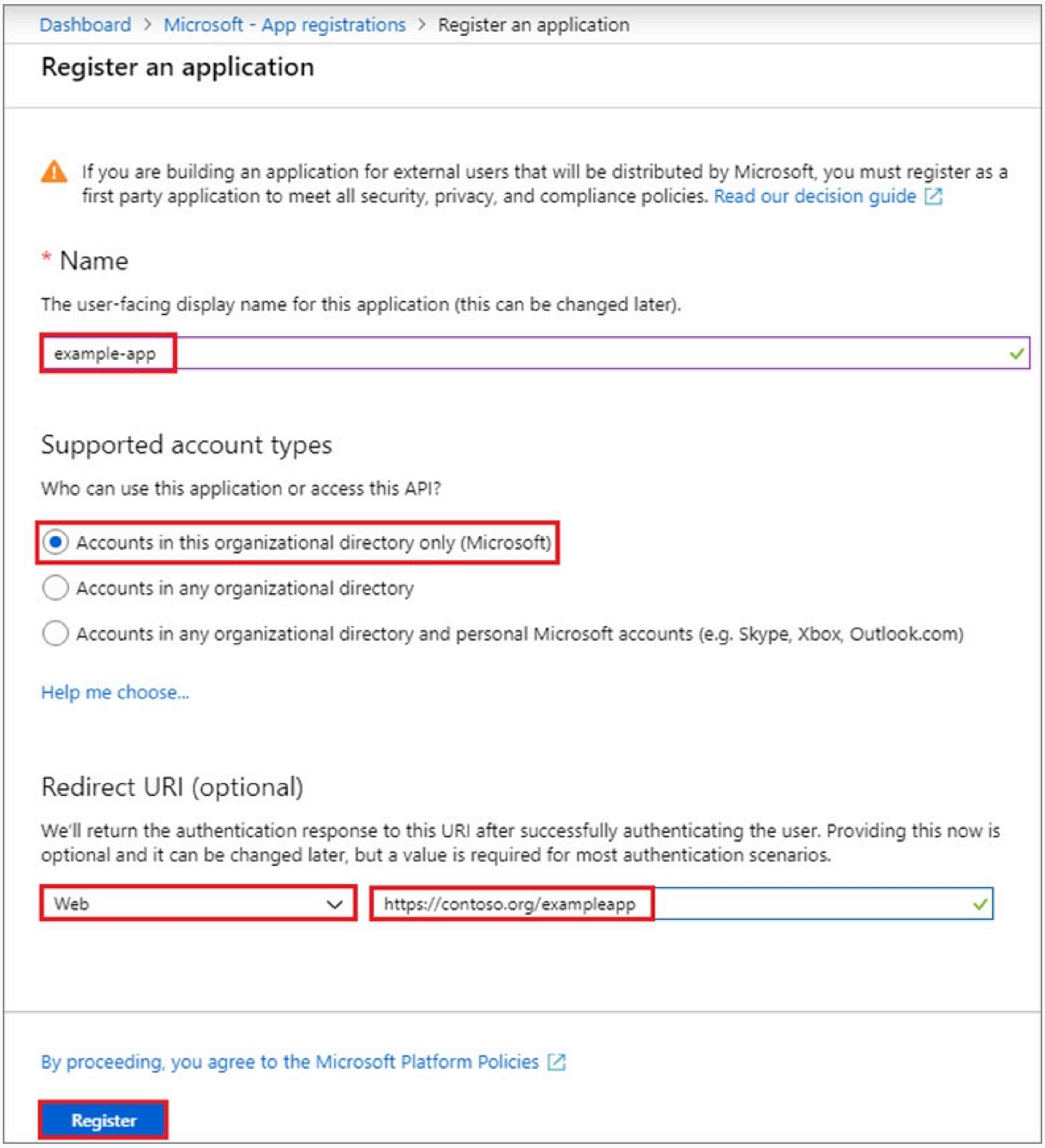
You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of https://app.contoso.com.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Suggested Answer: *See the explanation below.*

Step 1: Register the Application

1. Sign in to your Azure Account through the Azure portal.
2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application App12345678. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: https://app.contoso.com , where the access token is sent to.



Dashboard > Microsoft - App registrations > Register an application

Register an application

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://contoso.org/exampleapp

By proceeding, you agree to the Microsoft Platform Policies

6. Click Register

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

dumdada Highly Voted 2 years, 4 months ago

The exam doesn't have simulations like this since covid times

upvoted 9 times

Psychosikh 9 months ago

It now does again since 24/03/2023

upvoted 3 times

avicoder Highly Voted 👍 2 years, 9 months ago

Correct

upvoted 6 times

somenick Most Recent 🕐 1 year, 3 months ago

Shouldn't it be App registrations > Branding & properties > Home page URL (The URL to this application’s home page or the URL where users can sign-in and use this application) ?

upvoted 2 times

imie 1 year, 12 months ago

in Exam 31 Dec 2021.

upvoted 4 times

adamsca 2 years ago

# Exam Question 12/10/2021

upvoted 2 times

ReadyToLearn 2 years, 2 months ago

simulations are now showing up in tests

upvoted 4 times

AZ50018 2 years, 2 months ago

People have mentioned in discussion that they got simulations

upvoted 1 times

us3r 1 year, 8 months ago

bots I guess

upvoted 1 times

Question #39 *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 Roles and administrators blade, assign the Security administrator role to Admin1.

B. From the Organizational relationships blade, add an identity provider.

C. From the Custom domain names blade, add a custom domain.

D. From the Users blade, modify the External collaboration settings.

Suggested Answer: *D*
You need to allow guest invitations in the External collaboration settings.

Community vote distribution
D (100%)

⊟ **Teesmd** Highly Voted 3 years, 10 months ago
The provided answer "D" is correct: See the link below
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/delegate-invitations
upvoted 40 times

⊟ **thomastrain** 3 years, 7 months ago
D is right, but the setting is located in Azure Active Directory -> External Identities -> External collaboration settings.
upvoted 21 times

⊟ **milind8451** Highly Voted 3 years, 4 months ago
Right ans, Go to AAD -> Users -> User Settings -> "Manage External Collaboration Settings", here you need to allow "Guest Invite"
upvoted 13 times

⊟ **ESAJRR** Most Recent 9 months, 1 week ago
Selected Answer: D
D. From the Users blade, modify the External collaboration settings.
upvoted 1 times

⊟ **zellck** 1 year, 1 month ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure
upvoted 1 times

⊟ **majstor86** 1 year, 3 months ago
Selected Answer: D
D. From the Users blade, modify the External collaboration settings.
upvoted 1 times

⊟ **mung** 1 year, 7 months ago
This same question comes on AZ-104 exam as well
upvoted 3 times

⊟ **F117A_Stealth** 1 year, 7 months ago
Selected Answer: D
D. From the Users blade, modify the External collaboration settings.
upvoted 1 times

⊟ **Alessandro365** 2 years ago

Selected Answer: D

D is correct answer.

upvoted 1 times

salmantarik 2 years ago

D is correct

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 2 times

udmraj 2 years, 4 months ago

Correct Answer - D

upvoted 1 times

rohitmedi 2 years, 7 months ago

correct answer

upvoted 2 times

teehex 3 years, 1 month ago

Set Members can invite = Yes in External Collaboration settings.

D is the correct answer.

upvoted 2 times

reha 3 years, 5 months ago

D is correct!

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/generic-authorization-exception-inviting-azure-ad-gests/m-p/274742

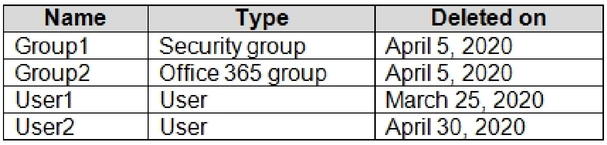
upvoted 5 times

> **the_dstryr** 2 years, 5 months ago
>
> wow they literally took questions from real users and turn it into exam question!!!
>
> upvoted 1 times

Question #40 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant.

You have the deleted objects shown in the following table.



Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center.

Which two objects can you restore? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Group1

B. Group2

C. User2

D. User1

Suggested Answer: *BC*

Deleted users and deleted Office 365 groups are available for restore for 30 days.

You cannot restore a deleted security group.

Reference:

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

Community vote distribution

BC (100%)

jessicamendez10 Highly Voted 👍 3 years, 9 months ago

In exam 20/03/2021

upvoted 25 times

Protonenpaule Highly Voted 👍 3 years, 8 months ago

Correct. User retention is also 30 days: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-restore?context=/azure/active-directory/enterprise-users/context/ugr-context

upvoted 12 times

yonie Most Recent ⏱ 1 year ago

Selected Answer: BC

B C

When objects such as users, Microsoft 365 Groups, or application registrations are soft deleted, they enter a suspended state in which they aren't available for use by other services. In this state, items retain their properties and can be restored for 30 days. After 30 days, objects in the soft-deleted state are permanently, or hard, deleted.

https://learn.microsoft.com/en-us/entra/architecture/recover-from-deletions#recover-from-soft-deletion

upvoted 1 times

ESAJRR 1 year, 5 months ago

Selected Answer: BC

B. Group2

C. User2

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: BC

BC is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-restore-deleted

When you delete a Microsoft 365 group in Azure Active Directory (Azure AD), part of Microsoft Entra, the deleted group is retained but not visible for 30 days from the deletion date. This behavior is so that the group and its contents can be restored if needed. This functionality is restricted exclusively to Microsoft 365 groups in Azure AD. It is not available for security groups and distribution groups. Please note that the 30-day group restoration period is not customizable.

upvoted 3 times

majstor86 1 year, 10 months ago

Selected Answer: BC

B. Group2

C. User2

upvoted 1 times

samimshaikh 1 year, 11 months ago

In Azure AD, Office 365 groups (also known as Unified Groups) can be restored if they are deleted, while security groups cannot.

Office 365 groups are backed up by the Microsoft data center and can be recovered by Microsoft Support within 30 days of deletion. However, it is important to note that restoring a deleted Office 365 group may not restore all associated data, such as email messages or calendar events.

Security groups, on the other hand, cannot be restored because they are not backed up by the Microsoft data center and their associated membership and access permissions are permanently lost once they are deleted.

In summary, Office 365 groups can be restored if they are deleted due to the backup process provided by Microsoft, while security groups cannot be restored once deleted due to the permanent loss of their associated membership and access permissions.

So B,C

upvoted 5 times

Alessandro365 2 years, 6 months ago

Selected Answer: BC

B and C are correct.

upvoted 3 times

Eltooth 2 years, 9 months ago

Selected Answer: BC

B and C are correct.
If you delete a security group - its gone. Forever. Immediately.
User 3 was deleted over 30 days ago, hence no longer within the 30 day AAD "recycle bin".
O365 group and user deleted within 30 days so able to restore.

upvoted 8 times

Bouncy 2 years, 10 months ago

Selected Answer: BC

May the 4th be with you on this exam!

upvoted 6 times

micofucho 2 years, 10 months ago

I think the answer is NO. You need to create at least to create NIC (there is not one in the resources list available) and you will need to join the VM to the subnet. These permissions are not included in Microsoft/compute/*
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

upvoted 2 times

subhuman 2 years, 10 months ago

Correct !
" When you delete a Microsoft 365 group in the Azure Active Directory (Azure AD), the deleted group is retained but not visible for 30 days from the deletion date. This functionality is restricted exclusively to Microsoft 365 groups in Azure AD. It is not available for security groups and distribution groups."

upvoted 2 times

WhalerTom 3 years ago

Selected Answer: BC

In exam Dec 21. 40 questions, 1 case study, no labs.

BC is correct

upvoted 5 times

rohitmedi 3 years, 1 month ago

correct answer
upvoted 1 times

⊟ **Marski** 3 years, 1 month ago
On the matter, how about increasing that to a quarter or 2 fiscal quarters, e.g. 90.180 days. Nowadays people work as consultants and just might come back! At least here in Finland.
upvoted 1 times

⊟ **Sandomj55** 3 years, 4 months ago
In Exam 8/4/2021
upvoted 1 times

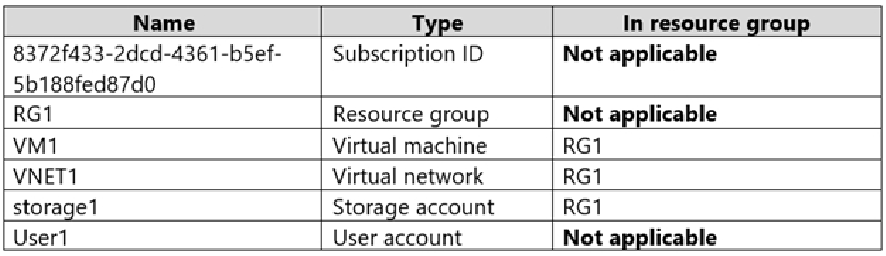
⊟ **sathas** 3 years, 6 months ago
Why can't we restore User2,
If we see the date he was deleted more recently than others and there should be more probability to restore his object.
upvoted 1 times

⊟ **sathas** 3 years, 6 months ago
Sorry wrong comment.. Can;t edit here
upvoted 1 times

Question #41 *Topic 2*

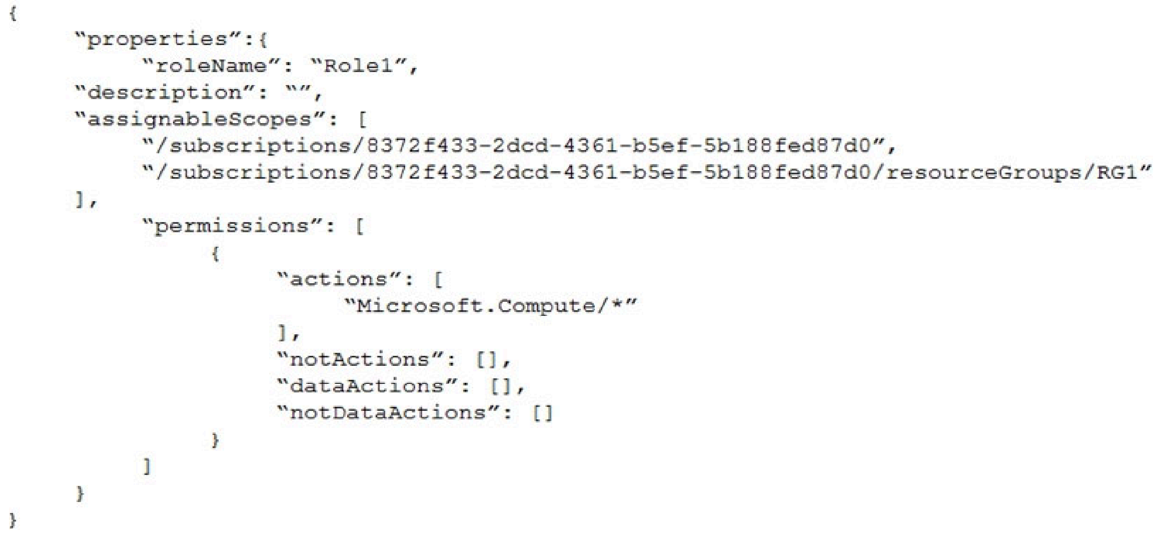
HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.



Name	Type	In resource group
8372f433-2dcd-4361-b5ef-5b188fed87d0	Subscription ID	**Not applicable**
RG1	Resource group	**Not applicable**
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage1	Storage account	RG1
User1	User account	**Not applicable**

You create an Azure role by using the following JSON file.



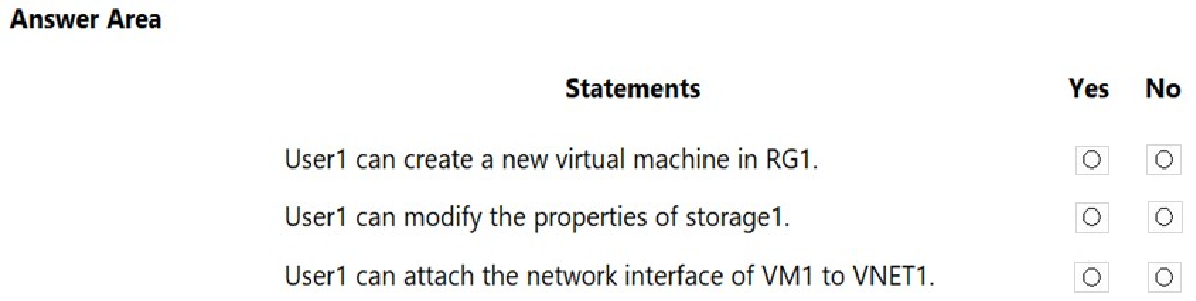
```
{
      "properties":{
            "roleName": "Role1",
      "description": "",
      "assignableScopes": [
            "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
            "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
      ],
            "permissions": [
                  {
                        "actions": [
                              "Microsoft.Compute/*"
                        ],
                        "notActions": [],
                        "dataActions": [],
                        "notDataActions": []
                  }
            ]
      }
}
```

You assign Role1 to User1 for RG1.

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

NOTE: Each correct selection is worth one point.

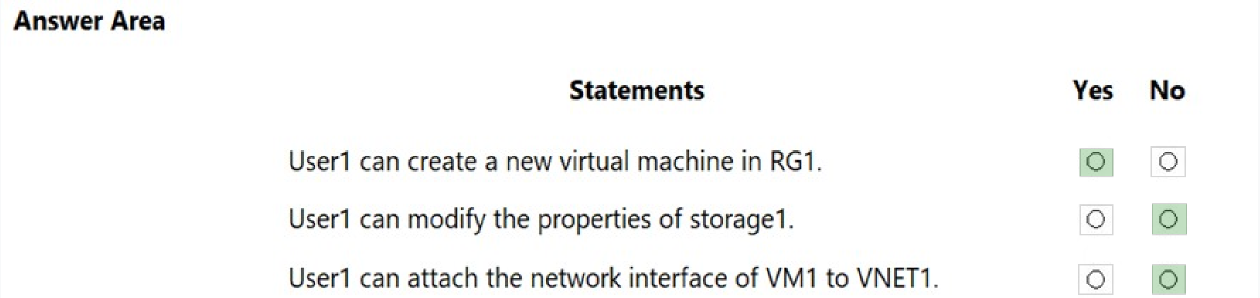
Hot Area:



Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	○	○
User1 can modify the properties of storage1.	○	○
User1 can attach the network interface of VM1 to VNET1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	[✓ ○]	○
User1 can modify the properties of storage1.	○	[✓ ○]
User1 can attach the network interface of VM1 to VNET1.	○	[✓ ○]

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute

Outbreak Highly Voted 3 years, 11 months ago

I think answer is correct, YES NO NO.

Azure custom roles: https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

Available permissions (e.g. “Microsoft.Compute/*”): https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

User1 can create new virtual machine in RG1: YES

(Permission needed is: Microsoft.Compute/virtualMachines/write, Creates a new virtual machine or updates an existing virtual machine)

User1 can modify the properties of storage1: NO

(Microsoft.Storage/storageAccounts/write, Creates a storage account with the specified parameters or update the properties or tags or adds custom domain for the specified storage account.)

User1 can attach the network interface of VM1 to VNET1: NO

(I’m not sure of the exact resource provider operation here, but from the docs it looks like it’s not possible from Microsoft.Compute/*, so I’m pretty sure answer is NO. The relevant operation should be in Microsoft.Network/virtualNetworks/*, I guess.)
upvoted 61 times

xRiot007 10 months, 3 weeks ago
Compute is not enough. When creating a VM, assigning it a VNET and a subnet is REQUIRED. If there is no VNET and subnet, you need to create them. Either way, you need Networking permissions to do this.
upvoted 1 times

ITFranz 11 months ago
To contribute to the answer 3
User1 can attach the network interface of VM1 to VNET1: NO
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface?tabs=azure-portal
Microsoft.Network/networkInterfaces/join/action Attach a network interface to a virtual machine
upvoted 1 times

[Removed] 3 years, 6 months ago
Microsoft.Network/virtualNetworks/read
upvoted 3 times

rsamant 3 years, 6 months ago
VM Creation Requires Network access also
upvoted 4 times

geuser 2 years, 9 months ago
adding NIC to VNET is a different story tho
upvoted 2 times

stuart563214 Highly Voted 3 years, 8 months ago
NO NO NO

Just tested and VM creation fails because you need further permissions to join a subnet. My JSON:

```
{
"id": "/subscriptions/16ea6f64-d8b2-4fb4-a7c4-4e6aaad4d751/providers/Microsoft.Authorization/roleDefinitions/f40893f6-07cc-476d-9b74-75fbf3499s47",
"properties": {
"roleName": "rbac1",
"description": "",
"assignableScopes": [
"/subscriptions/16ea6f64-d8b2-4fb4-a7c4-4e6aaad4d751",
"/subscriptions/16ea6f64-d8b2-4fb4-a7c4-4e6aaad4d751/resourceGroups/rbac1"
],
"permissions": [
{
"actions": [
"Microsoft.Compute/*"
],
"notActions": [],
"dataActions": [],
"notDataActions": []
}
]
}
}
```

upvoted 32 times

xRiot007 11 months, 2 weeks ago

You are not required to do anything with the VM, just create it. Box 1 is YES.

upvoted 3 times

BP_lobster 3 years, 3 months ago

Very helpful, thank you Stuart (changed my mind/now agree with this).

upvoted 2 times

lahl 2 years, 9 months ago

Tested in lab.... all answers should be NO, NO, NO

upvoted 4 times

JackGelder Most Recent 7 months, 4 weeks ago

NNN. Everyone who says that Microsoft.Compute/* is enough to create VM please check Virtual Machine Contributor Role that actually has the right permissions to create VMs

upvoted 1 times

rahmatellah 10 months, 2 weeks ago

false answer:
no no no
Minimum Permissions:
If you are assigning custom roles or minimum necessary permissions, ensure that the user has at least the following permissions on the resource group:

Microsoft.Compute/virtualMachines/*/write
Microsoft.Network/networkInterfaces/*/write
Microsoft.Storage/storageAccounts/*/read

upvoted 1 times

wardy1983 1 year, 8 months ago

Microsoft.Compute/* Grants access to all actions for all resource types in the Microsoft.Compute resource provider

upvoted 2 times

BigShot0 1 year, 9 months ago

No, No , No - Adding the compute/* role to the resource group will grant that permission to new resources but will not modify permissions on existing resources. You will not be able to attach the virtual machine to the existing virtual network so the VM creation will fail.

upvoted 4 times

ErikPJordan 1 year, 9 months ago

Action string Description
*/read Grants access to read actions for all resource types of all Azure resource providers.
Microsoft.Compute/* Grants access to all actions for all resource types in the Microsoft.Compute resource provider.
Microsoft.Network/*/read Grants access to read actions for all resource types in the Microsoft.Network resource provider.
Microsoft.Compute/virtualMachines/* Grants access to all actions of virtual machines and its child resource types.
microsoft.web/sites/restart/Action Grants access to restart a web app.

upvoted 2 times

zellck 2 years, 1 month ago

NNN is the answer.

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

upvoted 2 times

naylinu 2 years, 3 months ago

No , No , No

Minimum requirements:

"Microsoft.Compute/*/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Network/*/read",
"Microsoft.Storage/*/read",
"Microsoft.Authorization/*/read",
"Microsoft.Resources/*/read",
"Microsoft.Compute/virtualMachines/extensions/write"

upvoted 6 times

naylinu 2 years, 3 months ago

Above comment is just minimum requirements for creating vm.

upvoted 1 times

majstor86 2 years, 3 months ago

YES
NO
NO

upvoted 3 times

edurakhan 2 years, 7 months ago

Microsoft.Compute/* includes everything under it, including Microsoft.Compute/virtualMachines/write, which says “ Creates a new virtual machine or updates an existing virtual machine”. So the first one is YES
YES NO NO

upvoted 2 times

kabooze 2 years, 6 months ago

Even if users here claim they can't create a VM. Obviously microsoft's documentation says you can: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor
virtual machine contributor falls under compute and you have computer/* permissions

upvoted 1 times

Muaamar_Alsayyad 2 years, 8 months ago

Just testd on LAB
NO
NO
NO

upvoted 5 times

tblazeen 2 years, 9 months ago

YES-NO-NO is correct.

Microsoft.Compute/virtualMachines/write Creates a new virtual machine or updates an existing virtual machine

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources:~:text=Microsoft.Compute/virtualMachines/write

upvoted 2 times

Eltooth 3 years, 3 months ago

NO NO NO

upvoted 4 times

udmraj 3 years, 4 months ago

Correct Answer -- Yes, No, No

upvoted 1 times

Pravindes 3 years, 4 months ago

Answer is correct YNN
If existing vents we can create virtual machine

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

upvoted 1 times

⊟ **rohitmedi** 3 years, 7 months ago

correct answer

upvoted 1 times

Question #42 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.
You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Security administrator

B. Cloud application administrator

C. Application administrator

D. User administrator

E. Application developer

Suggested Answer: *BC*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

Community vote distribution
BC (100%)

arunjana Highly Voted 👍 4 years ago
Granting tenant-wide admin consent requires you to sign in as Global Administrator, an Application Administrator, or a Cloud Application Administrator.
upvoted 65 times

deegadaze1 Highly Voted 👍 3 years, 10 months ago
in exam
upvoted 16 times

stonwall12 Most Recent 🕘 4 months, 2 weeks ago
Selected Answer: BC
Answer:
1. B, Cloud application administrator
2. C, Application administrator

1. The Cloud application administrator role has permissions to create and manage all aspects of enterprise applications, application registrations, and application proxy settings. Most importantly, this role can grant admin consent for delegated permissions and application permissions, which is exactly what's needed for User1.
2. The Application administrator role has similar permissions to the Cloud application administrator. It can manage all aspects of applications and service principals, including the ability to grant admin consent for the tenant, which matches the requirement for User1.

Reference:
1. https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-application-administrator
2. https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#application-administrator
upvoted 1 times

scottyboy23 8 months, 2 weeks ago
on exam BC 13/04/24
upvoted 6 times

brooklyn510 11 months, 4 weeks ago
On exam 1/2/24
upvoted 3 times

yonie 1 year ago
Selected Answer: BC

To grant tenant-wide admin consent, you need:

A Microsoft Entra user account with *one of the following roles*:

Global Administrator or Privileged Role Administrator, for granting consent for apps requesting any permission, for any API.
Cloud Application Administrator or Application Administrator, for granting consent for apps requesting any permission for any API, except Microsoft Graph app roles (application permissions).
A custom directory role that includes the permission to grant permissions to applications, for the permissions required by the application.
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal#prerequisites

upvoted 2 times

tweleve 1 year, 2 months ago

In exam 13 Oct

upvoted 3 times

Self_Study 1 year, 4 months ago

On exam 7/8/23. A bit different answers to choose from.

upvoted 2 times

AzureAdventure 1 year, 4 months ago

Cloud APPLICATION Administrator
APPLICATION Administrator

upvoted 1 times

AzureAdventure 1 year, 4 months ago

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent?pivots=portal#:~:text=An%20Azure%20AD,by%20the%20application.

upvoted 1 times

ESAJRR 1 year, 5 months ago

Selected Answer: BC

B. Cloud application administrator
C. Application administrator

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: BC

BC is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent?pivots=portal#prerequisites
Granting tenant-wide admin consent requires you to sign in as a user that is authorized to consent on behalf of the organization.

To grant tenant-wide admin consent, you need:
An Azure AD user account with one of the following roles:
- Global Administrator or Privileged Role Administrator, for granting consent for apps requesting any permission, for any API.
- Cloud Application Administrator or Application Administrator, for granting consent for apps requesting any permission for any API, except Azure AD Graph or Microsoft Graph app roles (application permissions).
- A custom directory role that includes the permission to grant permissions to applications, for the permissions required by the application.

upvoted 1 times

Johnvic 1 year, 8 months ago

Exam.6 case studies. 3 true/false questions. 47 multiple questions and no simulations. Alot of new questions thats not up here

upvoted 1 times

Gesbie 1 year, 8 months ago

In Exam April 11, 2023

upvoted 4 times

majstor86 1 year, 10 months ago

Selected Answer: BC

B. Cloud application administrator
C. Application administrator

upvoted 3 times

⊟ **sofieejo** 1 year, 11 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 1 times

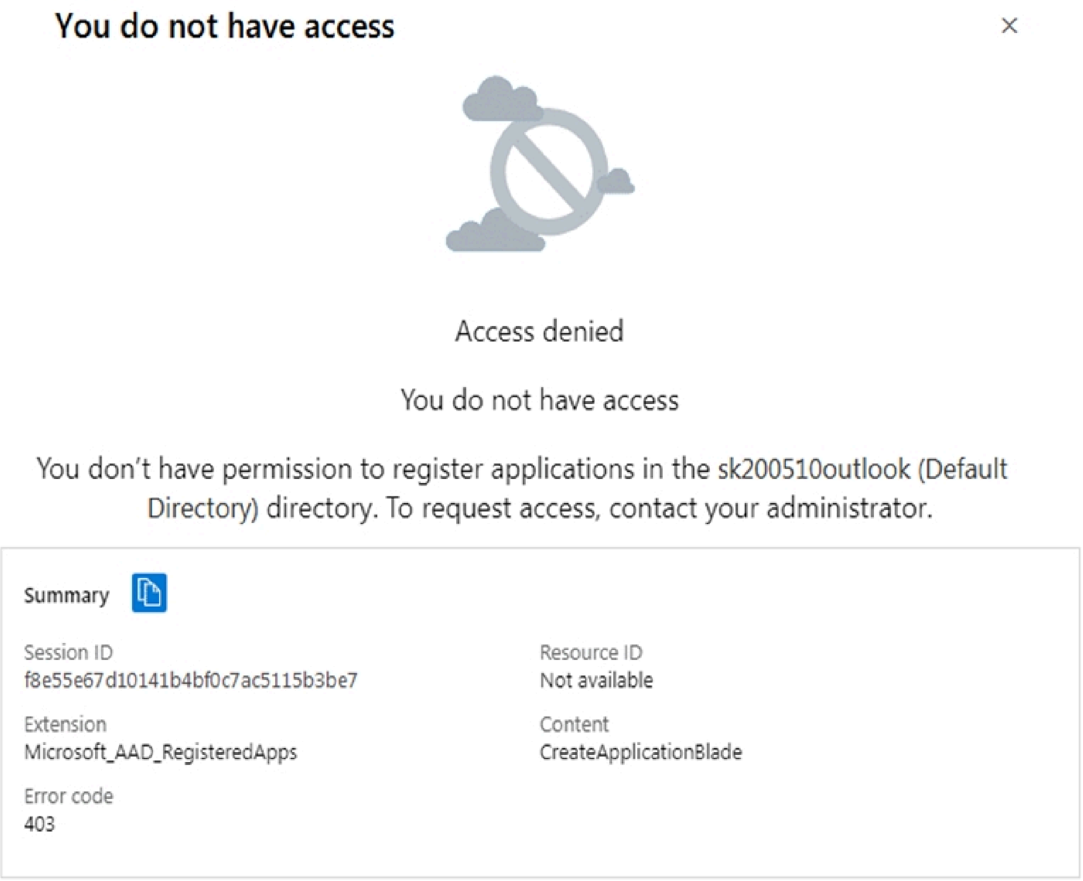
⊟ **Sweet_co** 2 years, 5 months ago

On my exam today: 20-7-2022

upvoted 4 times

Question #43 *Topic 2*

You have an Azure subscription that is associated with an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You do not have access ×

Access denied

You do not have access

You don't have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

Summary

Session ID
f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID
Not available

Extension
Microsoft_AAD_RegisteredApps

Content
CreateApplicationBlade

Error code
403

You need to ensure that the developer can register App1 in the tenant.
What should you do for the tenant?

A. Modify the Directory properties.

B. Set Enable Security defaults to Yes.

C. Configure the Consent and permissions settings for enterprise applications.

D. Modify the User settings.

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

Community vote distribution
D (80%) C (20%)

JohnYinToronto Highly Voted 4 years, 3 months ago
Answer correct.
Microsoft itself uses the default configuration with users able to register applications and consent to applications on their own behalf.
To prevent users from registering their own applications:

In the Azure portal, go to the User settings section under Azure Active Directory
Change Users can register applications to No.
upvoted 32 times

153a793 9 months, 1 week ago

small correction - Change Users can register applications to YES
https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings
upvoted 1 times

⊟ **stepman** 2 years, 2 months ago
I chose this and was On exam 4/27 with the new exam experience. No Sim or lab.
upvoted 7 times

⊟ **ArushiM** 2 years, 2 months ago
Hi
Did you get most of the questions from here? Can you please share your email address to discuss the exam details.. i am giving it on 29th
upvoted 1 times

⊟ **Deepmindx** Highly Voted 4 years ago
### IN EXAM ### 29/6/2021
upvoted 11 times

⊟ **gauravwagh16193** Most Recent 2 months, 3 weeks ago
Selected Answer: D
Why the Other Options Are Incorrect:
A. Modify the Directory properties
→ This doesn't control app registration.

B. Set Enable Security defaults to Yes
→ Security defaults enable MFA, etc., but not related to app registration.

C. Configure Consent and permissions settings
→ Controls API permissions, not app registration rights.
upvoted 2 times

⊟ **stonwall12** 4 months, 2 weeks ago
Selected Answer: D
Answer: D, Modify the User settings

Reason: To enable developers to register applications in Azure AD, you need to modify the User settings in Azure Active Directory. Change Users can register applications to YES.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added#who-has-permission-to-add-applications-to-my-azure-ad-instance
upvoted 1 times

⊟ **Ivan80** 1 year, 5 months ago
In exam 1/28/24
upvoted 2 times

⊟ **Rachy** 1 year, 10 months ago
Got this in my exam 28/08/23
upvoted 6 times

⊟ **ESAJRR** 1 year, 11 months ago
Selected Answer: D
D. Modify the User settings.
upvoted 1 times

⊟ **Ario** 1 year, 12 months ago
Selected Answer: C
Guys please make sure you read exactly questions option D ofc is another way to give consent to specific users but here asking : What should you do for the tenant? so option C for sure
upvoted 2 times

⊟ **Ario** 1 year, 12 months ago
sorry guys my bad , correct answer is D , in this scenario use just doesnt have permission so should modify user setting
upvoted 6 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added#who-has-permission-to-add-applications-to-my-azure-ad-instance

upvoted 1 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 3 times

majstor86 2 years, 3 months ago

Selected Answer: D

D. Modify the User settings.

upvoted 2 times

003nickm 2 years, 3 months ago

This is in exam March 2, 2023

upvoted 4 times

BlackZeros 2 years, 9 months ago

This was in exam September 15, 2022

upvoted 4 times

JMW 2 years, 11 months ago

If a user can't register an application the default permissions for the user have been removed and there will need to be granted again. Microsoft itself uses the default configuration allowing users to register applications and only allows user consent for a very limited set of permissions.
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added#who-has-permission-to-add-applications-to-my-azure-ad-instance

upvoted 3 times

MoFami 2 years, 12 months ago

In exam01/July 2022

upvoted 3 times

jr_luciano 3 years, 2 months ago

Selected Answer: D

If this option is set to yes in the User Settings, then non-admin users may register custom-developed applications for use within this directory.
If this option is set to no in the User Settings, then only users with an administrator role may register these types of applications.

upvoted 2 times

Eltooth 3 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 2 times

cfsxtuv33 3 years, 4 months ago

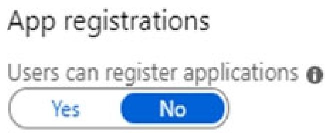
Yes...the answer id correct as I have run into this particular issues with azure and it was rectified by modifying user settings.

upvoted 2 times

Question #44 *Topic 2*

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.



App registrations

Users can register applications

Yes [✓ No]

You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. App Configuration Data Owner for the subscription

B. Managed Application Contributor for the subscription

C. Cloud application administrator in Azure AD

D. Application developer in Azure AD

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

Community vote distribution

D (86%) 14%

SIDNASIR Highly Voted 4 years ago

Correct Answer

Application Developer

Users in this role can create application registrations when the "Users can register applications" setting is set to No.

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

upvoted 32 times

Amin_7 Highly Voted 4 years ago

Application Developer - Create application registration when ability is disabled for all users

upvoted 11 times

stonwall12 Most Recent 4 months, 2 weeks ago

Selected Answer: D

Answer: D, Application developer in Azure AD

Reason: Since App registrations are set to "No" in the tenant settings, users by default cannot register applications. The Application developer role in Azure AD is specifically designed to allow users to register applications while following the principle of least privilege.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#application-developer

upvoted 1 times

xRiot007 10 months, 3 weeks ago

Answer is D - app developer.

It's so annoying that all these options are so interlaced creating a lot of times confusion.

In this case, MS should remove such flags so that all controls are centralized around roles. This would make things clear in a lot of cases.

upvoted 4 times

ESAJRR 1 year, 11 months ago

Selected Answer: D

D. Application developer in Azure AD

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability-is-disabled
Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No.

upvoted 2 times

r_git 2 years, 3 months ago

Selected Answer: D

D is correct
Users in this role can create application registrations when the "Users can register applications" setting is set to No.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#application-developer

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: D

D. Application developer in Azure AD

upvoted 4 times

samimshaikh 2 years, 5 months ago

By default, any user in Azure AD cannot register applications. The ability to register applications in Azure AD is typically restricted to administrators or users with specific permissions.

However, the level of access control for application registration can be configured by an administrator through the use of Azure AD role-based access control (RBAC). For example, an administrator can grant specific users or groups the ability to register applications in Azure AD by assigning them the "Application Developer" role.

In summary, t

The ability to register applications in Azure AD is not available to all users by default but can be granted through the use of Azure AD RBAC.
D is correct considering least priviledged

upvoted 1 times

Sir_Learnalot 2 years, 5 months ago

Selected Answer: D

Application Developer is the least privilege option here

upvoted 2 times

ltjones12 2 years, 6 months ago

Correct. To register an app you need app developer. To grant consent to an app you need with app admin or cloud app admin.

upvoted 1 times

KaleMu92 2 years, 7 months ago

In Exam 02/12/2022. 3 new questions, rest from here.

upvoted 4 times

promto 2 years, 8 months ago

Selected Answer: D

correct

upvoted 2 times

somenick 2 years, 9 months ago

Selected Answer: D

correct: https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

upvoted 3 times

joanjcanals 2 years, 9 months ago

Selected Answer: D

correct: https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

upvoted 2 times

badrmotayeb 2 years, 10 months ago

Application Developer

Can create application registrations independent of the 'Users can register applications' setting.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

upvoted 3 times

luckflying 2 years, 10 months ago

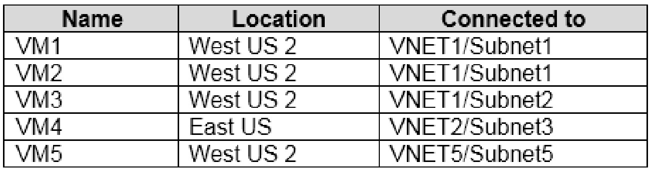
Selected Answer: C

Please check the additional roles, the Cloud App Admin role is the right selection.
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

upvoted 4 times

Question #45 *Topic 2*

You have the Azure virtual machines shown in the following table.



Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1.

What should you identify?

A. VM2 only

B. VM2 and VM3 only

C. VM2, VM3, VM4, and VM5

D. VM2, VM3, and VM5 only

Suggested Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

Community vote distribution

B (100%)

gcpbrig01 Highly Voted 3 years, 9 months ago

If you assign an ASG to a NIC, it means that only NICs in that virtual network can be assigned with that same ASG.

upvoted 54 times

MarioMK Highly Voted 3 years, 7 months ago

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

upvoted 30 times

brooklyn510 Most Recent 11 months, 4 weeks ago

On exam 1/2/24

upvoted 4 times

Obama_boy 1 year ago

Selected Answer: B

in exam 08/12/23

upvoted 3 times

ESAJRR 1 year, 5 months ago

Selected Answer: B

B. VM2 and VM3 only

upvoted 3 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups#allow-database-businesslogic

Application security groups have the following constraints:

- All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You can't add network interfaces from different virtual networks to the same application security group.

upvoted 3 times

twinkl 1 year, 9 months ago

Selected Answer: B

B. All NICs must below to the same VNet

upvoted 1 times

majstor86 1 year, 10 months ago

Selected Answer: B

B. VM2 and VM3 only

upvoted 2 times

fonte 1 year, 11 months ago

Hi all,
Passed my exam (13JAN2023) with 918.
50 questions (45 + 5 of a case study).
Around 95% of the questions are here.
I've compiled the questions and my answers in a ppt, feel free to check it out and hope it helps.
https://www.dropbox.com/s/ay00xp2fnloq1ex/AZ%20500%20-%20Exam%20Topics.pptx?dl=0
Use pass az500prep to open the file.

Thanks to all the people that comment on questions, I wouldn't have passed without them :)

upvoted 4 times

fonte 1 year, 11 months ago

Hi all, you need to download the file. Dropbox doesn't allow to open protected files.

upvoted 3 times

Fornadim89 1 year, 9 months ago

Dropbox says file has been deleted

upvoted 2 times

Makarand123 1 year, 8 months ago

file seems deleted

upvoted 1 times

tnagy 2 years, 5 months ago

Selected Answer: B

Yes, all NICs in the same VNET

upvoted 2 times

Amit3 2 years, 5 months ago

Vnet1 Only, so B is correct.

upvoted 1 times

Alessandro365 2 years, 6 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

salmantarik 2 years, 6 months ago

Key thing to remember "ASG only contain subnets from same vNet"

upvoted 2 times

Ringisai 2 years, 2 months ago

But VM1 is also on the same VNET

upvoted 1 times

alou333 2 years, 6 months ago

# IN EXAM - 3/6/2022 (online).
Lot of new questions. Good luck !

upvoted 3 times

karthi6 2 years, 6 months ago

Did u able to clear with help of exam topics Q&A?
upvoted 1 times

WMG 2 years, 8 months ago

Selected Answer: B

Easy rule to remember: the Vnet of the first network interface to be added to an ASG limits any future additions to that ASG to the same Vnet as the first interface was connected to.

upvoted 6 times

Eltooth 2 years, 9 months ago

Selected Answer: B

B is correct answer.

ASG can only contain subnets from same vNet.

upvoted 3 times

siobhan1 2 years, 9 months ago

## In today's exam 03/12/2022 ##

upvoted 2 times

Question #46 Topic 2

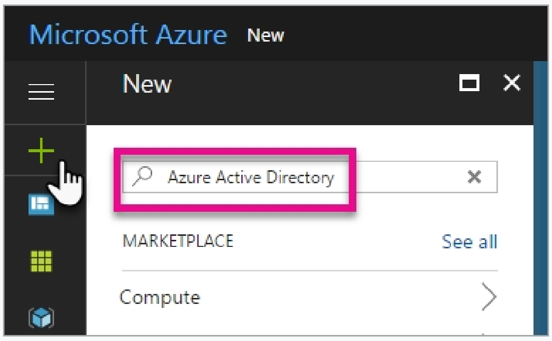
SIMULATION -

You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com. The new directory must contain a user named user12345678 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

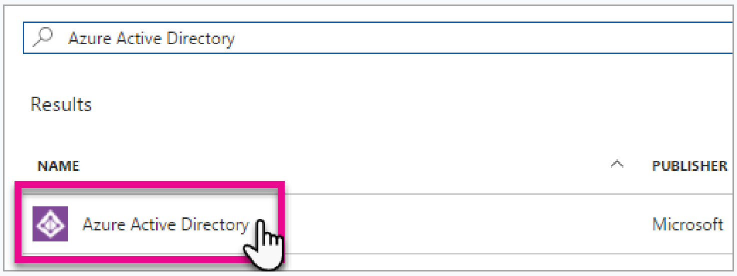
Suggested Answer: *See the explanation below.*

To create a new Azure AD tenant:

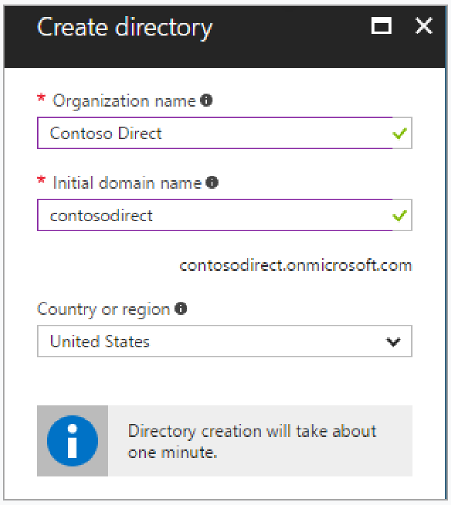
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



4. Select Create.
5. Provide an Organization name (12345678) and an Initial domain name (12345678). Then select Create. This will create the directory named 12345678.onmicrosoft.com.



* Organization name: Contoso Direct

* Initial domain name: contosodirect

contosodirect.onmicrosoft.com

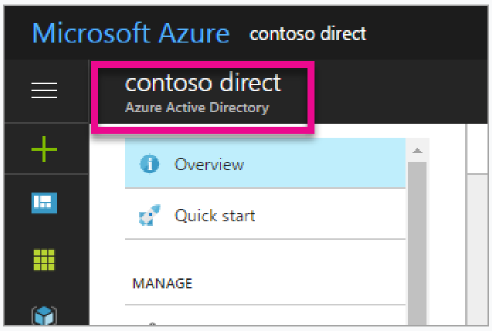
Country or region: United States

Directory creation will take about one minute.

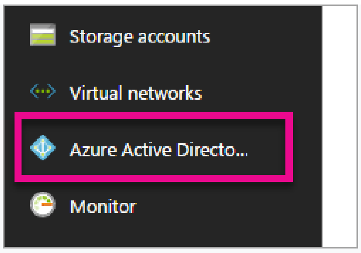
6. After directory creation is complete, select the information box to manage your new directory.

To create the user:

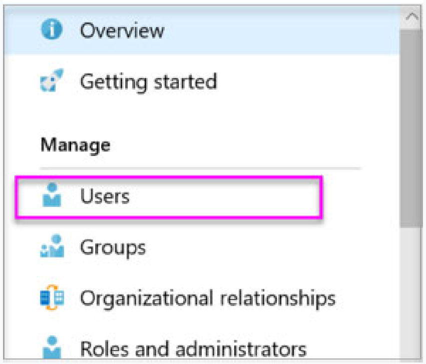
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



2. Under Manage, select Users.

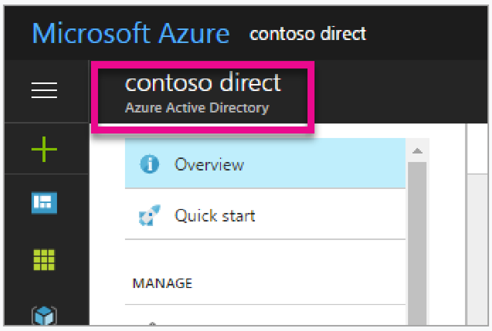


3. Select All users and then select + New user.

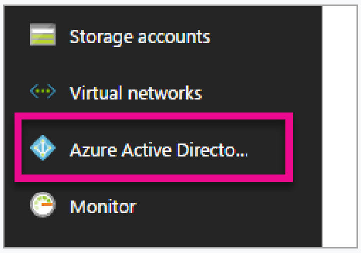
4. Provide a Name and User name (user12345678) for the user. When you're done, select Create.

To enable MFA:

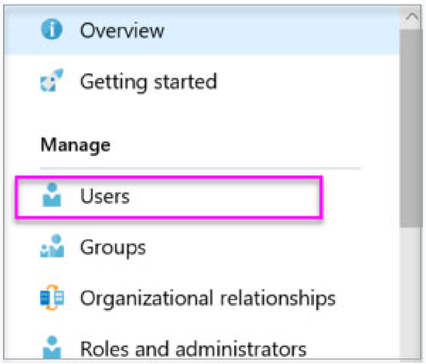
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



2. Under Manage, select Users.



3. Click on the Multi-Factor Authentication link.

4. Tick the checkbox next to the user's name and click the Enable link.

Reference:

https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

⊟ **cfsxtuv33** Highly Voted 👍 3 years, 6 months ago

I have been taking Azure exams since 2019 and have yet to see simulations. I started with the az900, then completed my 303/304 to get my solutions architect expert badge. Not one simulation yet. Now, I cant say that is "written in stone" but I wouldn't worry too much about it, especially if you have the azure platform and use it frequently is noting more than to study.

upvoted 8 times

Psychosikh 2 years, 3 months ago

Now in exam as of 24/3/2023

upvoted 7 times

ltjones12 Highly Voted 2 years, 6 months ago

UI has changed, now search "Azure Active Directory", then choose to manage tenants.

upvoted 5 times

Rhonwen Most Recent 10 months ago

In user → Manage → Authentication methods you can add an authentication method. If you add for example a phone number, at the bottom of the screen it will show "System preferred multifactor authentication method" Status is Enabled and the Method is SMS. So, doesn't this qualify as having MFA enabled?

upvoted 2 times

cris_exam 1 year, 5 months ago

This per-user method to enable/disable or modify MFA settings is no longer available. The new way now is to create a Conditional Policy assigning it to either User/s or Group/s.

https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa

upvoted 3 times

discussionperson 3 years, 11 months ago

Simulation will be there in exam?

upvoted 1 times

rawrkadia 3 years, 11 months ago

No, removed in 2020 and not returned yet due to issues they had during testing with people testing remote due to covid.

upvoted 4 times

thienvupt 4 years ago

Correct Answer, can enable MFA from Users do not use Default Security Setting.

upvoted 2 times

Fred64 4 years, 3 months ago

step 3 or 4 in the answer is not usefull. MFA is activated by default by Default Security Settings

upvoted 3 times

somenick 2 years, 9 months ago

Here they mean per-user MFA

upvoted 1 times

Question #47 *Topic 2*

You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named
RG1.
You create a custom role named Role1 for contoso.com.
Where you can use Role1 for permission delegation?

A. contoso.com only

B. contoso.com and RG1 only

C. contoso.com and Subscription1 only

D. contoso.com, RG1, and Subscription1

Suggested Answer: *D*

Community vote distribution

A (91%) 9%

jpons Highly Voted 4 years ago

A - contoso.com only
Azure AD role permissions can't be used in Azure custom roles and vice versa.
https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-overview
upvoted 41 times

rawrkadia 3 years, 10 months ago

This is correct. Azure AD roles and Azure RBAC are totally different. If you create an AAD role it won't work for subscriptions/MG/RG
upvoted 3 times

Jacquesvz 3 years, 11 months ago

I agree with you, answer A. AD roles are different to RBAC roles. AD roles for domain, RBAC for Subscription and RG's. Still unsure about this one though, anyone else that have more concrete evidence?
upvoted 4 times

shnz03 3 years, 3 months ago

Just to add on the concept of access control for Azure AD and Azure resources. Both are using RBAC model. To think that Azure AD method is NOT using RBAC is wrong.

https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-overview

The difference between these two role-based access control systems is:
Azure AD roles control access to Azure AD resources such as users, groups, and applications using the Microsoft Graph API
Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management
upvoted 5 times

Rahulbard Highly Voted 3 years, 11 months ago

Answer is D .. once a custom role is assinged to a user, the access can be at any level
upvoted 26 times

pentium75 11 months ago

You created a role in contoso.com (the Azure AD tenant), NOT Subscription1 (the Azure subscription). Thus it is an Azure AD role. You can't assign an Azure AD role to an Azure resource.
upvoted 1 times

duffrice 1 year, 8 months ago

https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles
upvoted 1 times

orcnylmz 2 years, 8 months ago

Agree with D. Every resource created in Azure associates with a tenant. In this questions it says custom role created for contoso.com, I understood it like a RBAC role in contoso.com tenant. But question is not so clear. I think you can understand vice versa also.

upvoted 2 times

pentium75 11 months ago

No, contoso.com is the name of the Azure AD tenant, it is NOT an RBAC role in the Azure subscription

upvoted 1 times

mmmyo Most Recent 1 month, 3 weeks ago

Selected Answer: A

When you create a custom role in Azure AD, it is scoped at the directory level (contoso.com) and can only be assigned within the Azure AD tenant. Unlike Azure RBAC roles, which apply to subscriptions, resource groups, and individual resources, Azure AD roles are specific to identity management and directory permissions.

upvoted 1 times

gauravwagh16193 2 months, 3 weeks ago

Selected Answer: D

You can use a custom role created for an Azure AD tenant across various scopes within that tenant. Specifically, custom roles can be assigned at the following levels:

Tenant level (contoso.com)
Resource group level (RG1)
Subscription level (Subscription1)
Therefore, the correct answer is:

D. contoso.com, RG1, and Subscription1

upvoted 1 times

rreghioua 5 months, 1 week ago

Selected Answer: D

Custom roles in Azure can be scoped to different levels:

Azure AD tenant (contoso.com): A role could be scoped to an Azure AD tenant, allowing permissions to be granted at the directory level.
Resource Group (RG1): You can also assign roles at the resource group level, allowing permissions to resources within that specific group.
Subscription (Subscription1): Similarly, roles can be assigned at the subscription level, applying to all resources in that subscription.
In this case, since you created a custom role for the Azure AD tenant contoso.com, it can be used at all levels—contoso.com (Azure AD tenant), RG1 (resource group), and Subscription1 (subscription level). Therefore, D is the most comprehensive option.

upvoted 1 times

Lanwan 6 months, 4 weeks ago

Selected Answer: D

Copilot and chatgpt says D

upvoted 2 times

mrt007 1 year, 3 months ago

D. contoso.com, RG1, and Subscription1

This is because in Azure, the scope of access for a custom role is at the directory level, and it can be assigned to users, groups, and service principals at subscription, resource group, and resource scopes. Therefore, Role1 can be used for permission delegation not only at contoso.com but also at RG1 and Subscription1.

upvoted 2 times

jacqs101 1 year, 4 months ago

A contoso.com only.
Why? Because the role was created in that tenant and Azure AD roles are a flat hierarchy

upvoted 2 times

Adt3ster 1 year, 6 months ago

Selected Answer: A

I choose A since the current description is : Add permissions for this custom role. Currently, permissions for Application registrations and Enterprise applications are supported in custom roles. It's only possible to assign at the directory level

upvoted 1 times

[Removed] 1 year, 6 months ago

AzureAD roles can be scoped into Administrative Units-> Application

upvoted 1 times

ESAJRR 1 year, 11 months ago

Selected Answer: D

D. contoso.com, RG1, and Subscription1

upvoted 1 times

Ario 1 year, 12 months ago

Selected Answer: A

there is nothing about RBAC in this question i will choose A

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-create

The role can be assigned either at the directory-level scope or an app registration resource scope only.

upvoted 3 times

majstor86 2 years, 3 months ago

Selected Answer: A

A. contoso.com only

upvoted 3 times

Marc_Azure 2 years, 4 months ago

Selected Answer: D

delegation

upvoted 1 times

samimshaikh 2 years, 5 months ago

it says that the custom role is created for contoso.com - that its for Azure AD.... if this was asked that a custom role created for subscription than we would have option in a answer list that "Subscription, Resource Group" . Since there is no answer in listed a pair of "Subscription, Resource Group" and I am confident that is question is for Azure AD contoso.com answer : A

upvoted 1 times

ltjones12 2 years, 5 months ago

It says "custom role" but doesn't elaborate on whether it's an RBAC ROle or an Azure AD Role. Not a valid question as it lacks a critical detail

upvoted 6 times

Question #48 *Topic 2*

You have an Azure subscription.
You enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
Your company's security policy for administrator accounts has the following conditions:
✑ The accounts must use multi-factor authentication (MFA).
✑ The accounts must use 20-character complex passwords.
✑ The passwords must be changed every 180 days.
✑ The accounts must be managed by using PIM.
You receive multiple alerts about administrators who have not changed their password during the last 90 days.
You need to minimize the number of generated alerts.
Which PIM alert should you modify?

A. Roles are being assigned outside of Privileged Identity Management

B. Roles don't require multi-factor authentication for activation

C. Administrators aren't using their privileged roles

D. Potential stale accounts in a privileged role

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

Community vote distribution
D (100%)

⊟ **Brodini** Highly Voted 👍 1 year, 9 months ago
Outdated question 09/2022. Per Microsoft link "This alert is no longer triggered based on the last password change date of for an account. This alert is for accounts in a privileged role that haven't signed in during the past n days, where n is a number of days that is configurable between 1-365 days."
upvoted 18 times

⊟ **JhonyTrujillo** Highly Voted 👍 3 years, 3 months ago
In Exam. D - Correct Answer.
upvoted 17 times

⊟ **ESAJRR** Most Recent ⏲ 11 months, 2 weeks ago
Selected Answer: D
D. Potential stale accounts in a privileged role
upvoted 3 times

⊟ **zellck** 1 year, 1 month ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts#potential-stale-accounts-in-a-privileged-role
upvoted 2 times

⊟ **majstor86** 1 year, 3 months ago
Selected Answer: D
D. Potential stale accounts in a privileged role
Outdated
upvoted 2 times

⊟ **agente232** 1 year, 9 months ago
is this question right? password policy says 180 days but admins have not changed it in last 90 days, why I would get an alert?
upvoted 12 times

⊟ **koreshio** 1 year, 8 months ago
exactly, i was wondering same

upvoted 3 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 3 times

DarkCyberGhost 2 years, 5 months ago

Selected Answer: D

Clearly D is the correct Answer here.

upvoted 2 times

Jco 2 years, 9 months ago

#exam ques # 29 Sep

upvoted 2 times

SecurityAnalyst 2 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 5 times

Socgen1 2 years, 10 months ago

In exam on 31/08/2021

upvoted 5 times

Deepmindx 3 years ago

### IN EXAM ### 29/6/2021

upvoted 7 times

kumax 3 years ago

On exam, May 2021.

upvoted 5 times

macco455 3 years, 3 months ago

Answer is correct

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new#potential-stale-accounts-in-a-privileged-role

upvoted 4 times

jeswinjose 3 years, 3 months ago

correct

upvoted 2 times

deegadaze1 3 years, 4 months ago

in Exam

upvoted 3 times

mayenite 3 years, 5 months ago

Correct

upvoted 2 times

Question #49 *Topic 2*

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.
Which Azure AD role should you assign to the domain administrator?

A. Security administrator

B. Global administrator

C. User administrator

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

Community vote distribution
B (100%)

deegadaze1 Highly Voted 3 years, 4 months ago
It was in Exam
upvoted 29 times

deegadaze1 Highly Voted 3 years, 4 months ago
Correct
upvoted 16 times

stonwall12 Most Recent 4 months, 2 weeks ago
Selected Answer: B
Answer: B, Global administrator

Reason: To modify Azure AD Connect synchronization options, even for domain administrators of the on-premises Active Directory, a Global administrator role in Azure AD is required. This is because changing sync configurations affects the entire Azure AD tenant and requires the highest level of privileges. While this might seem to conflict with the principle of least privilege, it is the minimum required role that can modify Azure AD Connect settings.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions#azure-ad-global-administrator
upvoted 2 times

ITFranz 6 months ago
Selected Answer: B
To support the answer:
While the Global Administrator role is needed for setup and major changes, for ongoing synchronization tasks, Azure AD Connect uses a special service account. This account is granted the Directory Synchronization Accounts role, which has limited permissions specifically for performing directory synchronization tasks
It's important to note that after the initial setup, you can reduce the privileges of the account used for day-to-day synchronization operations. However, any significant changes to the synchronization configuration will still require Global Administrator permissions.
Answer: B in this case.
upvoted 1 times

ESAJRR 11 months, 2 weeks ago
Selected Answer: B
B. Global administrator
upvoted 4 times

majstor86 1 year, 3 months ago
Selected Answer: B
B. Global administrator
OUTDATED

upvoted 3 times

Pearthfect 1 year, 4 months ago

This is an old question. The new role for least privileged is: Hybrid Identity Administrator on the newer versions of AAD. But in this question, B is correct.

upvoted 12 times

whosdatboi 1 year, 3 months ago

Azure AD Global Administrator account or Hybrid Identity Administrator account

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites#accounts

upvoted 4 times

Alessandro365 2 years ago

Selected Answer: B

B is correct answer.

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

Jco 2 years, 9 months ago

#exam question # 29 Sep

upvoted 7 times

TonytheTiger 2 years, 9 months ago

## Exam Question - 17 Sept 2021 ##

upvoted 6 times

Benjamin8189 2 years, 11 months ago

Azure AD Global Admin credentials

These credentials are only used during the installation and are not used after the installation has completed. It is used to create the Azure AD Connector account used for synchronizing changes to Azure AD. The account also enables sync as a feature in Azure AD.

upvoted 3 times

Benjamin8189 2 years, 11 months ago

Azure AD Global Administrator account: used to create the Azure AD Connector account and configure Azure AD. You can view global administrator accounts in the Azure portal. See List Azure AD role assignments.

upvoted 1 times

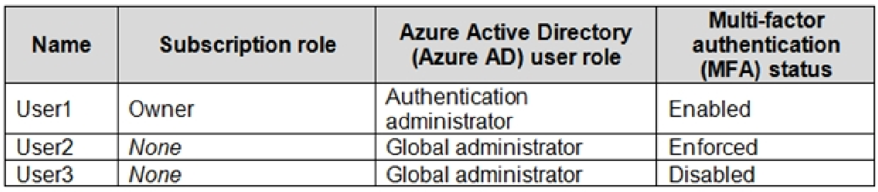
Luketen 3 years, 4 months ago

Confirm.

upvoted 7 times

Question #50 *Topic 2*

You have an Azure subscription that contains the users shown in the following table.



Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	*None*	Global administrator	Enforced
User3	*None*	Global administrator	Disabled

Which users can enable Azure AD Privileged Identity Management (PIM)?

A. User2 and User3 only

B. User1 and User2 only

C. User2 only

D. User1 only

Suggested Answer: *A*

For Azure AD roles in PIM, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators.

Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in PIM.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

Community vote distribution

A (100%)

teehex Highly Voted 4 years, 1 month ago

The given answer is incorrect.

This question is asking who can enable PIM?

To enable PIM there are 3 main steps:

- Login to Azure Portal as a Global Admin.
- Consent to PIM
- You are asked to verify your identity with MFA. If you haven't set up MFA yet you are asked to complete MFA setup before you can consent PIM.

Reference: https://github.com/MicrosoftDocs/azure-docs/commit/755069f4ff7430f739b1933dc082dffe9b6d564f#diff-38273a45d682dbc4e8ca5cb8548a045af63218005855ec067b0707aaa9d406f0

In this case, User2 can enable Azure PIM. How about user3? Yes it can because when MFA is asked the MFA state is changed to Enabled and User3 just needs to complete MFA setup before it can consent and enable PIM.

The correct answer is A - User2 and User3 only.

upvoted 102 times

153a793 8 months, 3 weeks ago

This elaboration is perfect. but, given the state of MFA in question, only user 2 can do it.

upvoted 1 times

fabianotrd Highly Voted 4 years, 3 months ago

Only global admin with MFA enabled can configure PIM

upvoted 37 times

OpsecDude 2 years, 9 months ago

You don't need MFA to enable it. Indeed, I have a brand new fresh AAD and the first thing I did was enable PIM. Another thing: Consent is NO LONGER needed. You just enable it, period.

upvoted 11 times

pentium75 11 months ago

You don't need MFA enabled PER USER (!) to use MFA.

upvoted 1 times

Outbreak 3 years, 11 months ago

Source?

upvoted 4 times

LHU Most Recent 1 month ago

Selected Answer: A

As I understand it; The fact User1 is the owner of a subscription within a tenant has nothing to do with what's going on in the Azure Tenant itself - like the PIM configuration. User1 lacks the privileges to handle those. Therefore, answer A.

upvoted 1 times

Strive_for_greatness_kc 1 year, 5 months ago

We no more need consent to enable PIM, so all global admin regardless of their MFA status can activate PIM

upvoted 3 times

ESAJRR 1 year, 9 months ago

Selected Answer: A

A. User2 and User3 only

upvoted 1 times

ArchitectX 1 year, 9 months ago

Selected Answer: A

right answer

upvoted 1 times

majstor86 2 years, 3 months ago

Selected Answer: A

A. User2 and User3 only

upvoted 2 times

OpsecDude 2 years, 9 months ago

Selected Answer: A

It is A nowadays. Still, that GA with no MFA is a total liability.

upvoted 3 times

Nik2Quik 2 years, 11 months ago

Selected Answer: A

its A as teehex explained, its asking who can enable

upvoted 1 times

TtotheA2021 2 years, 11 months ago

Selected Answer: A

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

upvoted 1 times

tnagy 2 years, 11 months ago

Selected Answer: A

Totally agree with Teehex's explanation

upvoted 2 times

Alessandro365 3 years ago

Selected Answer: A

A is correct answer.

upvoted 1 times

HazemSbaih 3 years ago

A- is Correct : https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- deployment-plan

upvoted 1 times

feln 3 years ago

Selected Answer: A

You need global admin to enable PIM, MFA can be set up by user3 while enabling PIM...

upvoted 6 times

Eltooth 3 years, 3 months ago

Selected Answer: A

Only global admin can first enable PIM.

upvoted 2 times

siobhan1 3 years, 3 months ago

## In today's exam 03/12/2022

upvoted 2 times

gc12345 3 years, 4 months ago

Ans:User2 & User3.
Considering by ...1)they are Global admin. 2)user2 already enforced with MFA ,user3 can opt for MFA when request PIM 3) refer this
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-require-mfa

Hope there P2 licensed user above all of this. I can see many questions here are not providing complete information.It leads us to take wrong answer.
Its not testing our knowledge, it is cheating...lol

upvoted 2 times

Question #51 Topic 2

You have an Azure subscription.
You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.
Which property of the RBAC role definition should you configure?

A. NotActions []

B. DataActions []

C. AssignableScopes []

D. Actions []

Suggested Answer: *D*
To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission.
To read the data in a storage account, ie. open a blob, you need a 'DataAction' permission.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

Community vote distribution
D (100%)

⊟ **milind8451** Highly Voted 4 years, 4 months ago
Right ans, DataAction[] is used at blob level, Action [] is used at container and storage acc level.
upvoted 25 times

⊟ **153a793** 8 months, 3 weeks ago
ARM templates provide 5 arrays to assign RBAC roles to Azure resources:

actions[], notActions[], dataActions[], notDataActions[], and assignableScopes[].

The actions[] array grants explicit access to specified operations, while the notActions[] array explicitly denies certain operations within the allowed actions (e.g., granting read access to storage but explicitly denying delete access).

The assignableScopes[] array defines where these roles can be assigned, such as management groups, subscriptions, resource groups, or specific resources.
upvoted 1 times

⊟ **usit** 3 years, 7 months ago
I don't think this is correct, Look at the Alice & Bob Diagram shown here. You can clearly see Bob has access to the storage account in the Actions category - https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions
upvoted 1 times

⊟ **teehex** Highly Voted 4 years, 1 month ago
The Actions permission specifies the management operations that the role allows to be performed. It is a collection of operation strings that identify securable operations of Azure resource providers (in this case it is Microsoft.Storage).

The DataActions permission specifies the data operations that the role allows to be performed to your data within that object.

Correct answer is D - Action[]
upvoted 14 times

⊟ **pentium75** Most Recent 11 months ago
IMO unclear question, you usually do not "read" a storage account but the data in it.
upvoted 1 times

⊟ **ESAJRR** 1 year, 9 months ago
Selected Answer: D
D. Actions
upvoted 1 times

icebw22 2 years, 3 months ago

Correct answer,

Action for management plane

Data action for data plane

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: D

D. Actions []

upvoted 3 times

tblazeen 2 years, 9 months ago

D is the right answer.

Role-based access control for control plane actions is specified in the Actions and NotActions properties of a role definition. Here are some examples of control plane actions in Azure:

Manage access to a storage account

Create, update, or delete a blob container

Delete a resource group and all of its resources

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions#control-and-data-actions

upvoted 3 times

Siphe 2 years, 10 months ago

Answer = B

DataActions

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete Returns the result of deleting a blob

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read Returns a blob or a list of blobs

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute

upvoted 1 times

> **Ivanvazovv** 2 years, 10 months ago
>
> Storage account is not only Blob.
>
> upvoted 1 times

Alessandro365 3 years ago

Selected Answer: D

D is correct answer.

upvoted 1 times

Eltooth 3 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 2 times

Tash95 3 years, 4 months ago

I'd say answer is B

You create a storage account through the control plane. You use the data plane to read and write data in the storage account.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/control-plane-and-data-plane

upvoted 1 times

> **siuloongwoo** 3 years ago
>
> So far what I've learned is, "read carefully". Question stated "read the storage accounts", not read the "data in" the storage accounts.
>
> upvoted 7 times

udmraj 3 years, 4 months ago

Correct Answer : D

upvoted 1 times

AS179 3 years, 6 months ago

Selected Answer: D

D is correct

upvoted 3 times

⊟ **Farooque** 3 years, 10 months ago

All Answers are correct and regarding the last one, so Virtual Administrator can use for login and not resetting the password.

upvoted 2 times

⊟ **Appuni** 4 years, 3 months ago

correct

upvoted 3 times

⊟ **mayenite** 4 years, 4 months ago

Correct

upvoted 12 times

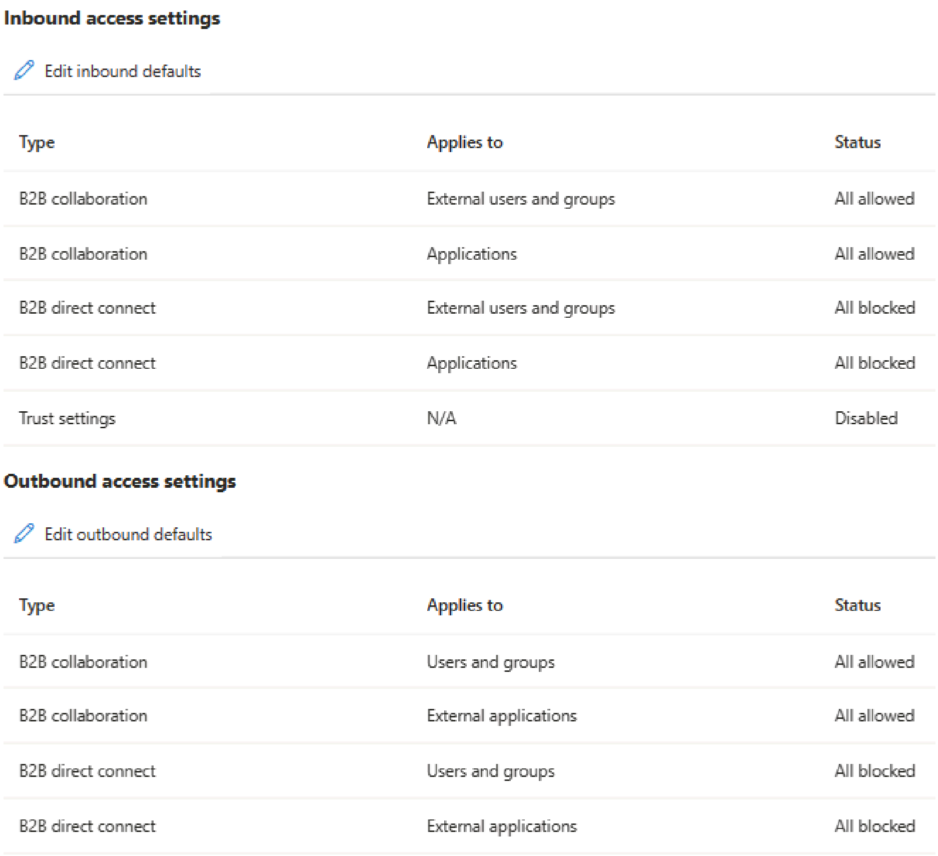
Question #52 *Topic 2*

HOTSPOT -

You have a Microsoft Entra tenant named contoso.com.

You collaborate with a partner organization that has a Microsoft Entra tenant named fabrikam.com. Fabrikam.com has multi-factor authentication (MFA) enabled for all users.

Contoso.com has the Cross-tenant access settings configured as shown in the Cross-tenant access settings exhibit. (Click the Cross-tenant access settings tab.)



Inbound access settings

Edit inbound defaults

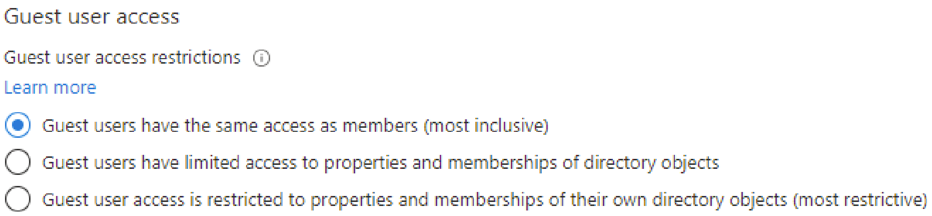
Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled

Outbound access settings

Edit outbound defaults

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed
B2B direct connect	Users and groups	All blocked
B2B direct connect	External applications	All blocked

Contoso.com has the External collaboration settings configured as shown in the External collaboration settings exhibit. (Click the External collaboration settings tab.)



Guest user access

Guest user access restrictions ⓘ

Learn more

● 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)

You create a Conditional Access policy that has the following settings:

• Name: CAPolicy1

• Assignments

o Guest or external users: B2B collaboration guest users

o Target resources

- Include: All cloud apps

• Access controls

- Grant access

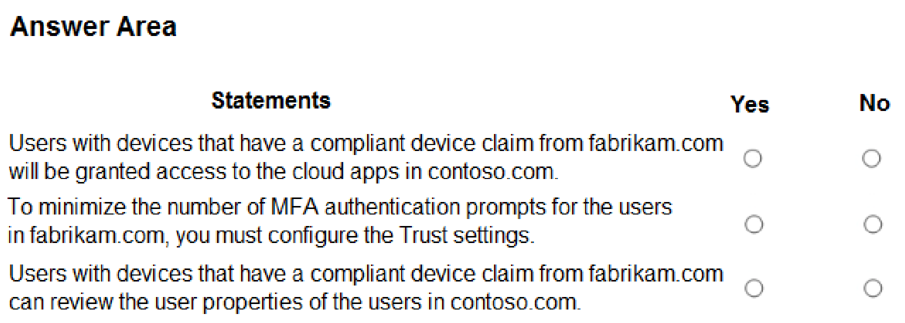
• Require device to be marked as compliant

• Require multi-factor authentication

- Enable policy: On

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

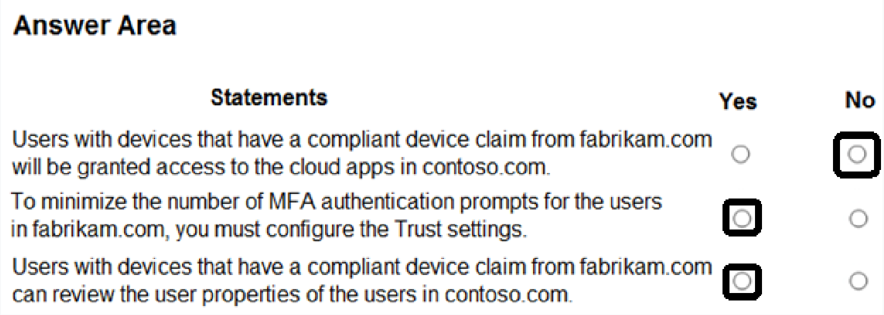
NOTE: Each correct section is worth one point.



Answer Area

Statements	Yes	No
Users with devices that have a compliant device claim from fabrikam.com will be granted access to the cloud apps in contoso.com.	○	○
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	○	○
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Users with devices that have a compliant device claim from fabrikam.com will be granted access to the cloud apps in contoso.com.	○	[✓ ○]
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	[✓ ○]	○
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	[✓ ○]	○

cerifyme85 Highly Voted 8 months, 3 weeks ago

Yes-No-Yes

upvoted 9 times

Andreas_Czech 7 months ago

1: yes; 2: no; 3: yes

1: allowed by the Conditional Policy; 2: enable the Trust Settings would be correct, but the Conditional Policy requires MFA; 3: because of the Guest User Access Restrictions -> ... have the same Access as Members ...

upvoted 5 times

luisribeiro199 Most Recent 1 month, 2 weeks ago

No- device compliance is not recognizable, neither MFA is trusted since Trust settings are disabled.

Yes - Fabrikam.com users already get their internal MFA checks, so if Contoso had their Trust settings configured they could minimize their MFA requests by using the one from Fabrikam's home tenant

No - Their compliance isn't recognizable, so doesn't matter. If it was, then yes they could review user properties since they have the same access as members

upvoted 3 times

Hot_156 4 months, 2 weeks ago

1. No – Truest settings are not enabled for the compliant claims to be used from fabrikam.com

2. Yes – If you enable the truest settings, you can achieve this.

3. Yes/No – See both reasoning,

a. Yes – The user could have both compliant claims but the question is not about access, it is about the GUEST USER ACCESS CONFIGURATION. This is set to users have the same access as members and members can see properties from other users

b. No – The compliant claim thing????

upvoted 1 times

Srirupam 7 months, 3 weeks ago

Yes -Yes -No

upvoted 3 times

153a793 8 months, 3 weeks ago

Following statements, in sequence, describes the functionalities and configurations related to B2B collaboration and B2B direct connect in Microsoft Entra

upvoted 2 times

153a793 8 months, 3 weeks ago

Following statements, in sequence, describes the functionalities and configurations related to B2B collaboration and B2B direct connect in Microsoft Entra:

• B2B collaboration allows inviting guest users without synchronization between Entra organizations. B2B direct connect involves a mutual trust relationship for seamless resource sharing, currently available for Microsoft Teams, without the need for guest user management.

• By default, B2B collaboration does not automatically enable trust for MFA and device claims; these need to be configured. However, without enabling trust, any user can invite guest users. B2B direct connect requires explicit configuration to establish the trust relationship.

• Enabling trust relationship, between two Entra organizations, allows you to accept MFA and device claims from the guest organization, but you can still apply additional Conditional Access policies as needed.

upvoted 2 times

153a793 8 months, 3 weeks ago

• If the trust relationship is not enabled, MFA and device claims from the guest tenant will not be considered. In that case, guest users will need to meet your organization's MFA and device compliance requirements independently, based on Conditional Access policy.

• Disabling Conditional Access at the organization level, including MFA and device claims, can be considered weak security as it reduces the layers of protection for accessing resources.

In case of social identity provider, trust setting are based on security functionality of external identity provider while conditional access can still be configured and enforced for MFA and device claims

upvoted 2 times

shadad 8 months ago

so the answer is ?

upvoted 5 times

ca7859c 1 month, 1 week ago

Answer is: NYN

upvoted 1 times

ca7859c 2 weeks, 5 days ago

2nd One is Y

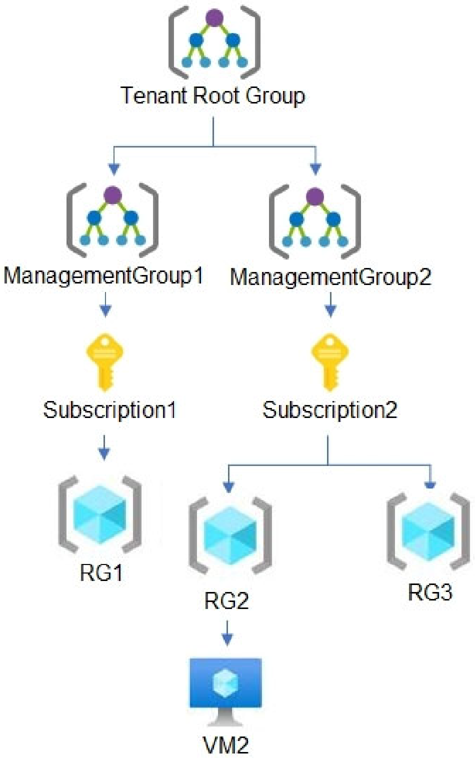
MFA claims\Device Compliance\Hybrid Joined Devices can be trusted from other

https://learn.microsoft.com/en-us/entra/external-id/cross-tenant-access-settings-b2b-collaboration#to-change-inbound-trust-settings-for-mfa-and-device-claims

upvoted 1 times

HOTSPOT -

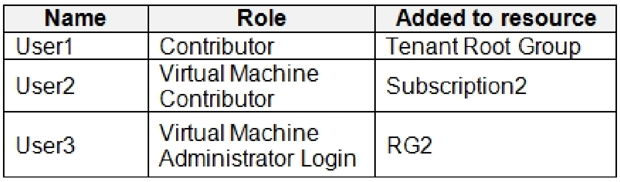
You have the hierarchy of Azure resources shown in the following exhibit.



RG1, RG2, and RG3 are resource groups.

RG2 contains a virtual machine named VM2.

You assign role-based access control (RBAC) roles to the users shown in the following table.

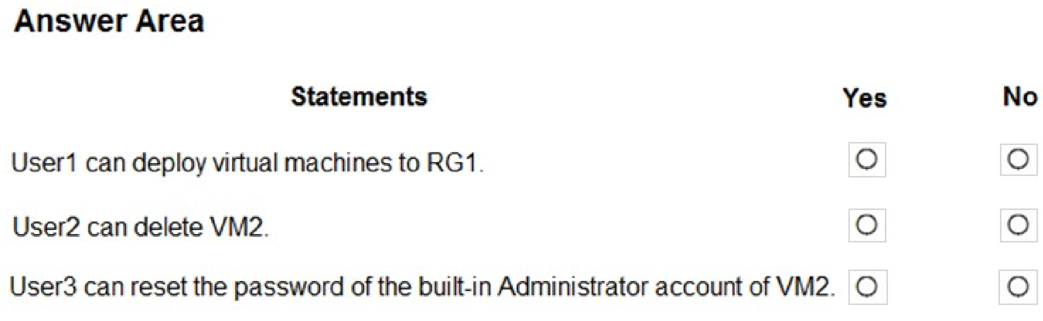


Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

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

NOTE: Each correct selection is worth one point.

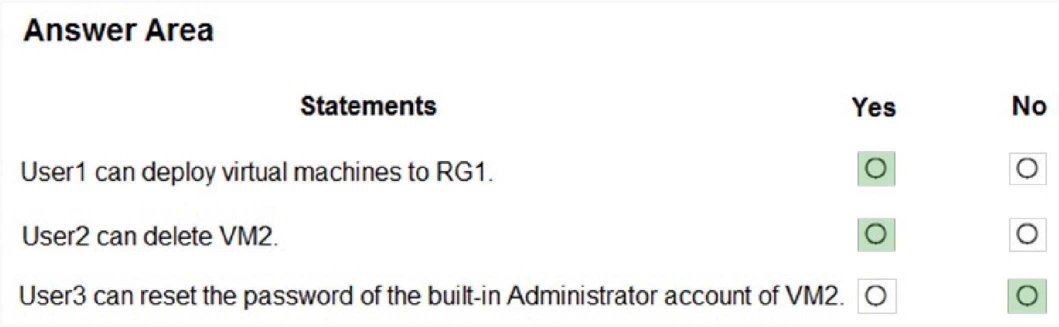
Hot Area:



Answer Area

Statements	Yes	No
User1 can deploy virtual machines to RG1.	○	○
User2 can delete VM2.	○	○
User3 can reset the password of the built-in Administrator account of VM2.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can deploy virtual machines to RG1.	●	○
User2 can delete VM2.	●	○
User3 can reset the password of the built-in Administrator account of VM2.	○	●

Geeky93 Highly Voted 4 years, 3 months ago

Correct answers.

1) Yes

Source : https://docs.microsoft.com/fr-fr/azure/governance/management-groups/overview

2) Yes

The role has this rights :

Microsoft.Compute/virtualMachines/*

Perform all virtual machine actions including create, update, delete, start, restart, and power off virtual machines. Execute predefined scripts on virtual machines.

Source : https://docs.microsoft.com/fr-fr/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

3) No

Virtual Machine Administrator Login -> View Virtual Machines in the portal and login as administrator

Source :

https://docs.microsoft.com/fr-fr/azure/role-based-access-control/built-in-roles

upvoted 80 times

3abmula 4 years, 1 month ago

3). Why No.

If user can login to a VM as an Administrator, then he can reset the built-in Admin password.

upvoted 5 times

eroms 4 years, 1 month ago

Microsoft.Compute/virtualMachines/loginAsAdmin/action Log in to a virtual machine with Windows administrator or Linux root user privileges.. so 3). Yes

upvoted 5 times

Frosticus 4 years ago

on 3, I think the question is asking if the user can reset the admin password from the Azure portal, not login and reset it. They are really asking, if the admin password were lost, forgotten, or locked out, can this user use the portal to reset it. The answer to that question is no. Bad question as it isn't specific enough.

upvoted 7 times

Ivanvazovv 2 years, 10 months ago

When you log in with admin permission you can change the built-in Administrator account password.

upvoted 3 times

teehex Highly Voted 4 years, 1 month ago

Because User1 has Contributor at Tenant Root Group so the role is inherited in subscription under that root group. So User1 can deploy a new VM.

User2 has VM Contributor which can delete a VM2 which is in RG2 which is part of Subscription2.

The statement #3 is tricky to be honest. Infact with Virtual Machine Administrator Login User3 can log in to an Azure virtual machine with administrator privileges. And once he is in the VM he can change local admin password using PowerShell or GUI from Computer Management.

Correct Answer - Yes Yes Yes

upvoted 25 times

ca7859c Most Recent 2 weeks, 3 days ago

Y

Y

N (User needs to be be VM contributor to reset VM passwords)

upvoted 1 times

brooklyn510 1 year, 5 months ago

On exam 1/2/24

upvoted 4 times

[Removed] 1 year, 6 months ago

Tested in the lab 3 is NO

upvoted 1 times

ArchitectX 1 year, 9 months ago

Yes -Yes - Yes is the right answer

upvoted 4 times

Self_Study 1 year, 10 months ago

On exam 7/8/23. Answers are correct but the 3. is a really not clear. If reset means change after login, that its YYY.

upvoted 4 times

zellck 2 years, 1 month ago

YYN is the answer.

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.

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 1 times

zellck 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-administrator-login
View Virtual Machines in the portal and login as administrator

upvoted 1 times

upliftinghut 2 years, 2 months ago

Question 3 Yes, refer to the matrix of which admin can reset other admin password here: https://learn.microsoft.com/en-us/answers/questions/408862/reset-azure-ad-admin-password

upvoted 2 times

xRiot007 11 months, 2 weeks ago

This is for Azure AD itself, not what happens inside of a VM. Do not confuse an Active Directory Admin with a VM built-in admin.

upvoted 1 times

majstor86 2 years, 3 months ago

YES
YES
NO

upvoted 3 times

KaleMu92 2 years, 7 months ago

In Exam 02/12/2022

upvoted 1 times

Ivanvazovv 2 years, 10 months ago

Virtual Machine Administrator Login - Microsoft.Compute/virtualMachines/loginAsAdmin/action - Log in to a virtual machine with Windows administrator or Linux root user privileges. From here - https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-administrator-login
So when you log in with administrative privileges, you can change the password of the built-in Administrator account. I'd vote for triple "Yes".

upvoted 6 times

acexyz 2 years, 12 months ago

# IN EXAM - 30/6/2022

upvoted 2 times

Alessandro365 3 years ago

correct answer is: YYN

upvoted 1 times

alou333 3 years ago

IN EXAM - 3/6/2022 (online).

Lot of new questions. Good luck !

upvoted 2 times

⊟ **ArunRavilla** 2 years, 10 months ago

No, liar. Not many new questions.

upvoted 6 times

⊟ **JakeCallham** 2 years, 9 months ago

maybe all the new question were added after alou33 made the reply here?

upvoted 1 times

⊟ **Fal991l** 2 years, 7 months ago

good one :)

upvoted 1 times

⊟ **certmonk** 3 years, 1 month ago

user3 can rest the local admin password. because the virtual machine administrator login gives him the following -

Microsoft.Compute/virtualMachines/loginAsAdmin/action Log in to a virtual machine with Windows administrator or Linux root user privileges

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-administrator-login

upvoted 3 times

⊟ **Eltooth** 3 years, 3 months ago

Yes, Yes and No (if user 3 is accessing via portal).

upvoted 1 times

Question #54 *Topic 2*

HOTSPOT -

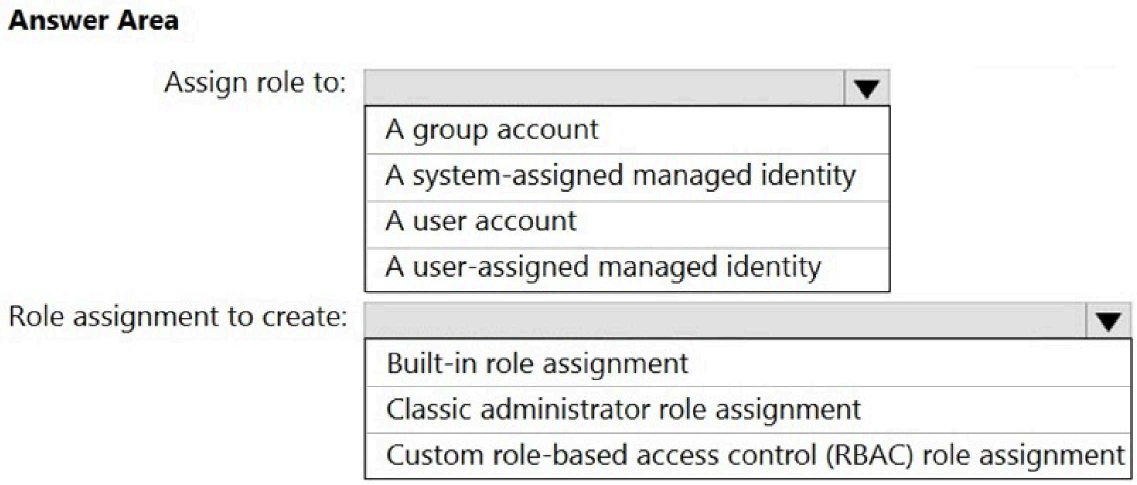
You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

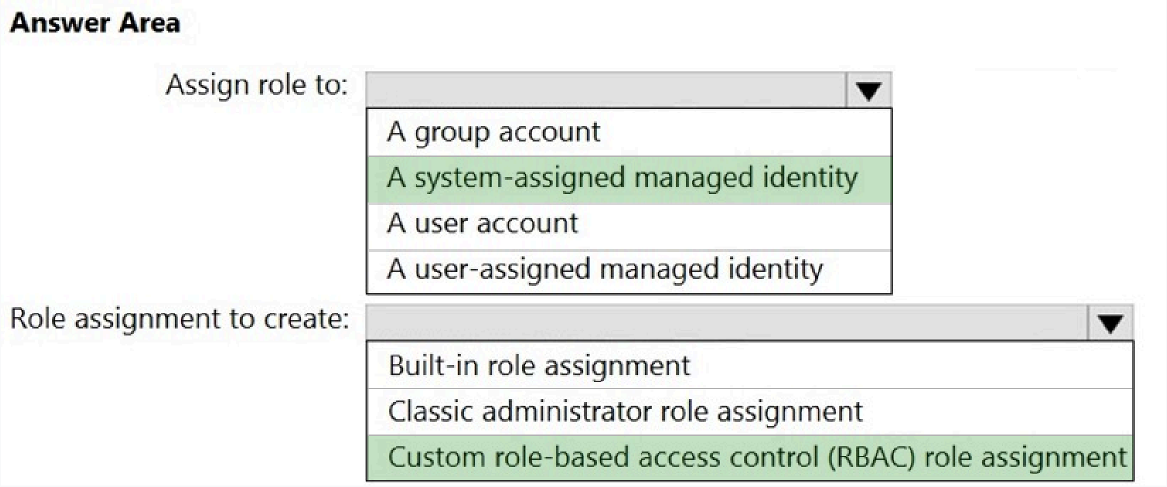
Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

Suggested Answer:



Answer Area

Assign role to:

- A group account
- [✓ A system-assigned managed identity]
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- [✓ Custom role-based access control (RBAC) role assignment]

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal

Fred64 Highly Voted 4 years, 2 months ago

minimize admin effort=> system assign MI

minimum required priviledge => Custom role. All other role have too much priviledges

upvoted 59 times

Troublemaker Highly Voted 1 year, 11 months ago

In Exam - 28/7/2023

upvoted 10 times

hellboycze 1 year, 11 months ago

well, today is 25.7. :D and i am reading questions

upvoted 8 times

stonwall12 Most Recent 4 months, 2 weeks ago

Answer:

1. System-assigned MI

2. Custom RBAC

Reason:
1. A system-assigned managed identity offers automatic Azure management with lifecycle tied to the Azure Function, requiring minimal administrative effort.

2. Custom RBAC role assignment allows defining the exact minimum permissions needed for storage account creation, following the principle of least privilege more strictly than built-in roles or classic administrator roles which might provide excess permissions.

Reference:
1. https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity
2. https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles
upvoted 1 times

zellck 2 years, 1 month ago
1. System-assigned managed identity
2. Custom RBAC role assignment

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#managed-identity-types

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, subscription, and resource group scopes.
upvoted 4 times

icebw22 2 years, 3 months ago
correct

both system or user managed identity would work, but question states less admin so system managed identity wins
upvoted 1 times

153a793 8 months, 3 weeks ago
agree with the justification. if question ask better managed option then user managed identity would be better option
upvoted 1 times

majstor86 2 years, 3 months ago
System Assigned Managed Identity
Custom role (RBAC)
upvoted 3 times

F117A_Stealth 2 years, 7 months ago
minimize admin effort=> system assign MI
minimum required priviledge => Custom role. All other role have too much priviledges
upvoted 2 times

salmantarik 3 years ago
Minimized admin effort
1 - SAMI
2- RBAC (Custom role)
upvoted 2 times

asfgsertweg 3 years, 2 months ago
- User assigned MI, because accounts will be reused for multiples instances
- Customized roles to reduce the scope of privilege
upvoted 7 times

Eltooth 3 years, 3 months ago
I'd go for SAMI and custom role to minimise privileges over admin effort.
upvoted 1 times

zioggs 3 years, 7 months ago
Exam - 4/11/21
upvoted 3 times

Jco 3 years, 9 months ago

#exam question # 29 Sep

upvoted 2 times

⊟ **TonytheTiger** 3 years, 9 months ago

## Exam Question - 17 Sept 2021 ##

upvoted 2 times

⊟ **francis6170** 3 years, 9 months ago

Got this in the AZ-500 exam (Sept 2021)!

upvoted 3 times

⊟ **teehex** 4 years, 1 month ago

Two steps you'd need to do:

- Enable System-assigned Managed Identity (SAMI) in your Azure function app (https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet#add-a-system-assigned-identity)
- Assign it a custom role (Microsoft.Storage/storageAccounts...) with least privilege.

upvoted 7 times

⊟ **Cyberbug2021** 4 years, 2 months ago

Correct answers

upvoted 4 times

⊟ **macco455** 4 years, 3 months ago

Seems like you could use a normal RBAC role for this and assign the managed identity to it instead of creating an entirely new role just for storage account creation.

upvoted 4 times

⊟ **A365** 4 years, 3 months ago

agree, there is a built in role to create storage accounts: https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-account-contributor

upvoted 6 times

⊟ **rooban** 3 years, 4 months ago

IMHO that's too many permissions. It can create AND MANAGE storage accounts, manage deployments etc. So it seems we have to choose either to do a bit of extra administrative work setting up the correct permissions or grant excessive permissions. I believe MS always wants us to strive for minimum required permissions so custom seems more appropriate.

upvoted 1 times

⊟ **Fred64** 4 years, 2 months ago

The scenario is: minimum required priviledge. Where do you take into account this reequirement?

upvoted 4 times

⊟ **macco455** 4 years, 3 months ago

Also, creating a custom role will be more administrative effort than is needed for this.

upvoted 2 times

Question #55 *Topic 2*

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant.
From the Azure portal, you register an enterprise application.
Which additional resource will be created in Azure AD?

A. a service principal

B. an X.509 certificate

C. a managed identity

D. a user account

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

Community vote distribution

A (100%)

LJack Highly Voted 👍 3 years, 3 months ago

Correct answer

upvoted 32 times

Sandomj55 Highly Voted 👍 2 years, 10 months ago

In Exam 8/4/2021

upvoted 7 times

Sabr_ Most Recent 2 months, 3 weeks ago

Selected Answer: A

Exam question 6th April 2025

upvoted 2 times

stonwall12 4 months, 2 weeks ago

Selected Answer: A

Answer: A, a service principal

Reason: When you register an enterprise application in Azure AD through the Azure portal, a service principal is automatically created. This service principal acts as the security identity for the application, defining what the application can access in your Azure AD tenant and what permissions it has.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals#relationship-between-application-objects-and-service-principals

upvoted 1 times

Obama_boy 6 months, 3 weeks ago

in exam 08/12/23

upvoted 4 times

tweleve 8 months, 2 weeks ago

in Exam 13 Oct

upvoted 2 times

Pupu86 1 year ago

After registering an application in AAD, a service principal a.k.a client ID or application ID is created.

upvoted 4 times

zellck 1 year, 1 month ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals#application-registration

If you register an application in the portal, an application object and a service principal object are automatically created in your home tenant.

upvoted 3 times

majstor86 1 year, 3 months ago

Selected Answer: A

A. a service principal

upvoted 2 times

F117A_Stealth 1 year, 7 months ago

Selected Answer: A

The 2 types of objects get created once the app registration is done:

Application Object
Service Principal Object

upvoted 4 times

SBIDS 1 year, 10 months ago

Selected Answer: A

A is correct

upvoted 2 times

acexyz 1 year, 12 months ago

# IN EXAM - 30/6/2022

upvoted 3 times

Alessandro365 2 years ago

Selected Answer: A

A is correct answer.

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 3 times

AS179 2 years, 6 months ago

A is correct

upvoted 3 times

PUSHPENDERA 2 years, 7 months ago

I think the given answer is correct -

ll applications that get registered in AAD, in the tenant, two types of objects get created once the app registration is done.

Application Object
Service Principal Object

Refer - https://docs.microsoft.com/en-us/answers/questions/270680/app-registration-vs-enterprise-applications.html

upvoted 4 times

gc12345 2 years, 4 months ago

I guess "a managed identity" is answer here because application object and service principle object are not resource of AAD.but a managed identity is tied up all the way with a azure AD resource.
agree?

upvoted 2 times

paraelspamparaelspam 2 years, 8 months ago

I think this answer is wrong as the a managed identity manages the creation and automatic renewal of a service principal on your behalf. The question asks "which additional resource WILL BE CREATED in Azure AD", which means that you won't be creating that identity, but Azure will be doing that for you. Therefore, that means that the resource created is a managed identity, a system-managed identity to be more precise.

Please, correct me if I'm wrong. Thank you.

upvoted 4 times

⊟ **examtopics6969** 2 years, 8 months ago

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal#app-registration-app-objects-and-service-principals

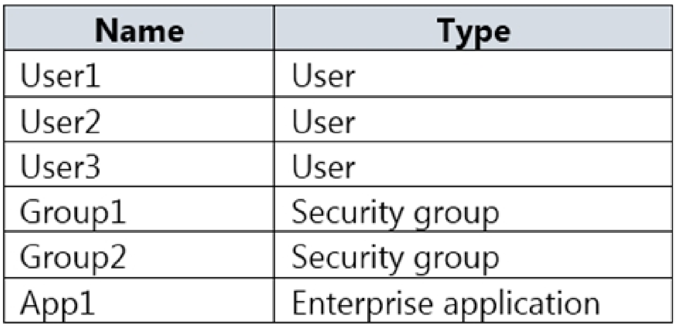
"There is no way to directly create a service principal using the Azure portal. When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant."

upvoted 8 times

Question #56 Topic 2

HOTSPOT -

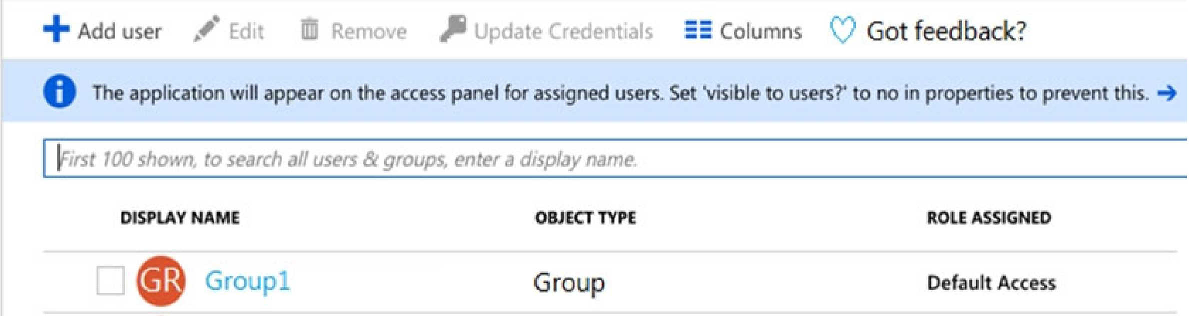
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.



Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.

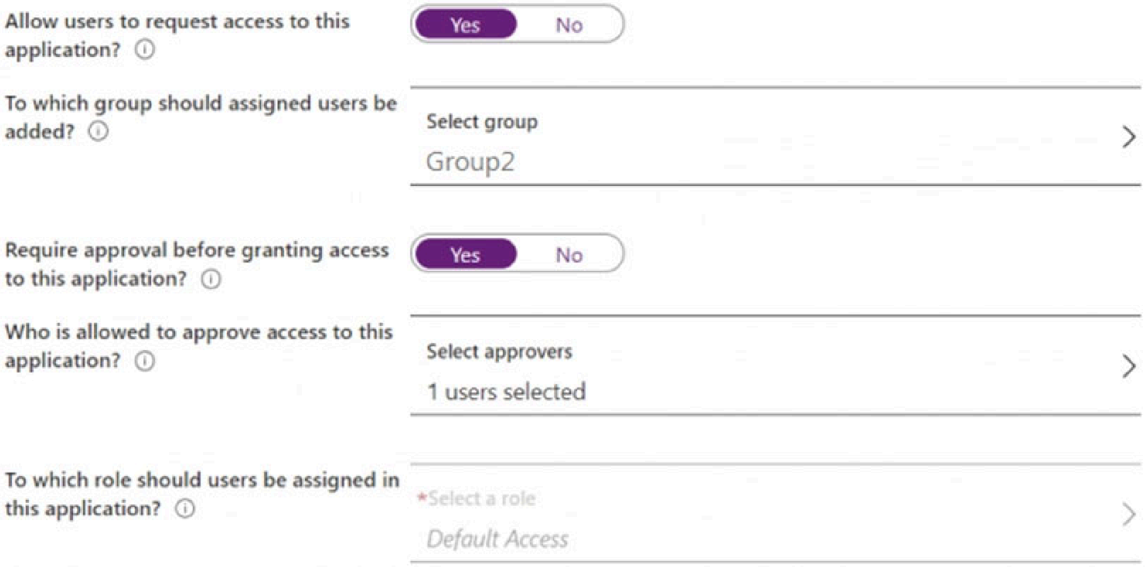


The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
□ GR Group1	Group	Default Access

You enable self-service application access for App1 as shown in the following exhibit.



Allow users to request access to this application? ⓘ [✓ Yes] No

To which group should assigned users be added? ⓘ Select group: Group2

Require approval before granting access to this application? ⓘ [✓ Yes] No

Who is allowed to approve access to this application? ⓘ Select approvers: 1 users selected

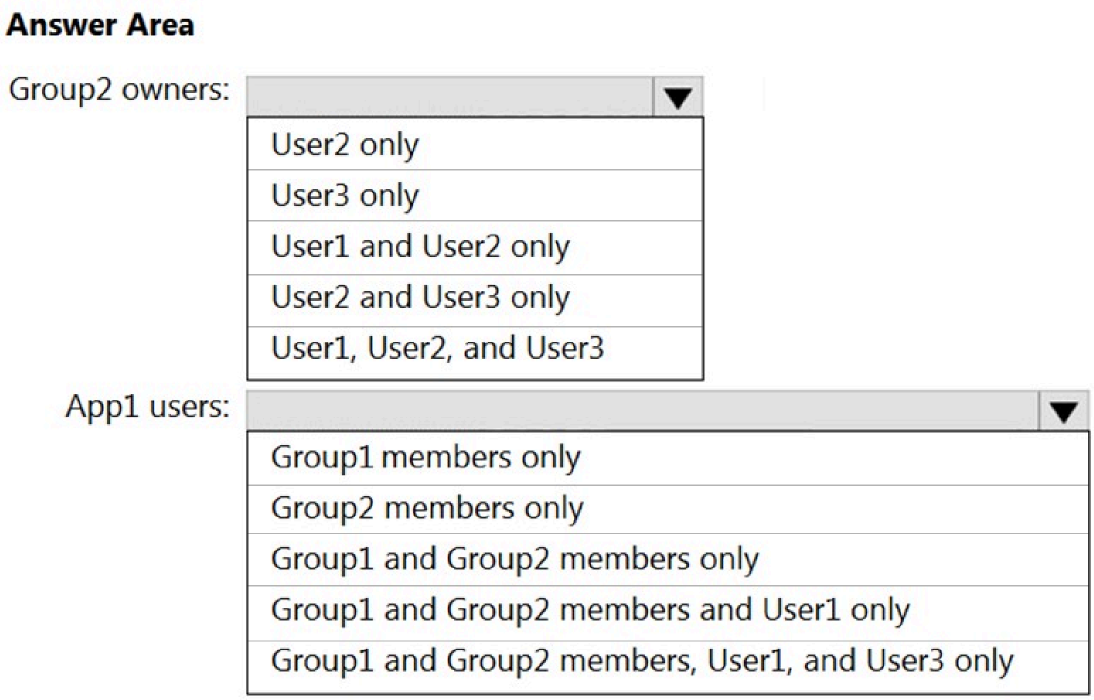
To which role should users be assigned in this application? ⓘ *Select a role: Default Access

User3 is configured to approve access to App1.

After you enable self-service application access for App1, who will be configured as the Group2 owner and who will be configured as the App1 users? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

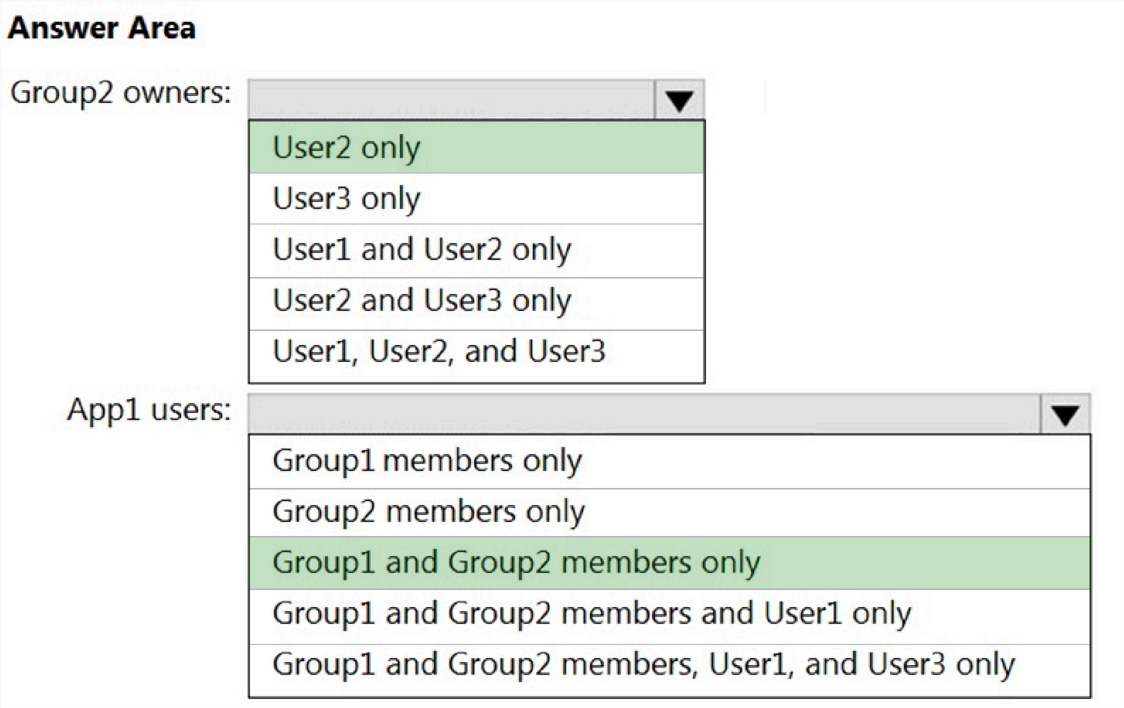
Group2 owners: ▼

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users: ▼

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Suggested Answer:



Answer Area

Group2 owners: ▼

- [✓ User2 only]
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users: ▼

- Group1 members only
- Group2 members only
- [✓ Group1 and Group2 members only]
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

⊟ **alanew** Highly Voted 3 years, 6 months ago

Tested in portal:

Group2 owners: User 3 Only

App1 users: Group 1 and Group 2 members only

upvoted 47 times

⊟ **MrPrasox** 3 years, 4 months ago

indeed, this is correct. Tested as well.

upvoted 1 times

⊟ **TiredofTesting** 3 years, 6 months ago

You are correct. For the 1st answer,

Under Self-Service:

When you selected a group 'To which group should assigned users be added', the owner will be replaced by the approver of this application. In this case, user 3.

Confirmed in the lab. It even tells you when you proceed to save the changes.

upvoted 12 times

Crawfork 3 years, 6 months ago

When you add User3 as the approver there is a dialog that says the approver will replace the owner of the group - verified in the Portal

upvoted 26 times

zellck Highly Voted 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 10 times

Ivan80 Most Recent 1 year, 5 months ago

In exam 1/28/24

upvoted 4 times

wardy1983 1 year, 7 months ago

Group2 owners: User 3 Only

App1 users: Group 1 and Group 2 members only

upvoted 1 times

TheProfessor 1 year, 9 months ago

Could any please explain why "App1 users: Group 1 and Group 2 members only"?

upvoted 2 times

pentium75 11 months ago

Group 1 already has access.

Group 2 was configured for self-service, so obviously it needs access too.

upvoted 1 times

STC007 1 year, 9 months ago

Because Group1 is configured as needed to access to Apps (as setting for App1) and Group2 is the group which can add users to group2. So

App1 user: group1 and group1 member only

upvoted 5 times

Troublemaker 1 year, 11 months ago

In Exam - 28/7/2023

upvoted 3 times

stepman 2 years, 2 months ago

I forgot what I chose, but this was On exam 4/27 with the new exam experience. No Sim or lab.

upvoted 6 times

majstor86 2 years, 3 months ago

Group2 owners: User 3 Only

App1 users: Group 1 and Group 2 members only

upvoted 3 times

F117A_Stealth 2 years, 7 months ago

Group2 owners: User 3 Only >>> (When you add User3 as the approver there is a dialog that says the approver will replace the owner of the group)

App1 users: Group 1 and Group 2 members only

upvoted 5 times

Muaamar_Alsayyad 2 years, 8 months ago

user 3 only

group1 and group 2 members only

upvoted 1 times

Diallo18 2 years, 8 months ago

In Exam 10/18/2022. One case study (6 Ques), no lab.

correct Ans

upvoted 3 times

ChrisPinas 2 years, 7 months ago

Did you take the exam online or on exam center? Thanks

upvoted 2 times

⊟ **BlackZeros** 2 years, 9 months ago

This was in exam September 15, 2022

upvoted 3 times

⊟ **ChrisPinas** 2 years, 7 months ago

Did you take the exam online or on exam center? Do you have any simulations/labs?

upvoted 1 times

⊟ **salmantarik** 3 years, 2 months ago

Test at Azure portal. user 3 is replaced by user 2 for self service configuration so my answer is
User 3 only and
App1 users as Group1 and Group2 members only.

upvoted 1 times

⊟ **Innovite** 3 years, 3 months ago

also confirmed in the lab..

upvoted 1 times

⊟ **Eltooth** 3 years, 3 months ago

User 3
Group 1 & 2 only

upvoted 1 times

⊟ **DANI0022** 3 years, 6 months ago

user 3

upvoted 2 times

Question #57 *Topic 2*

HOTSPOT -

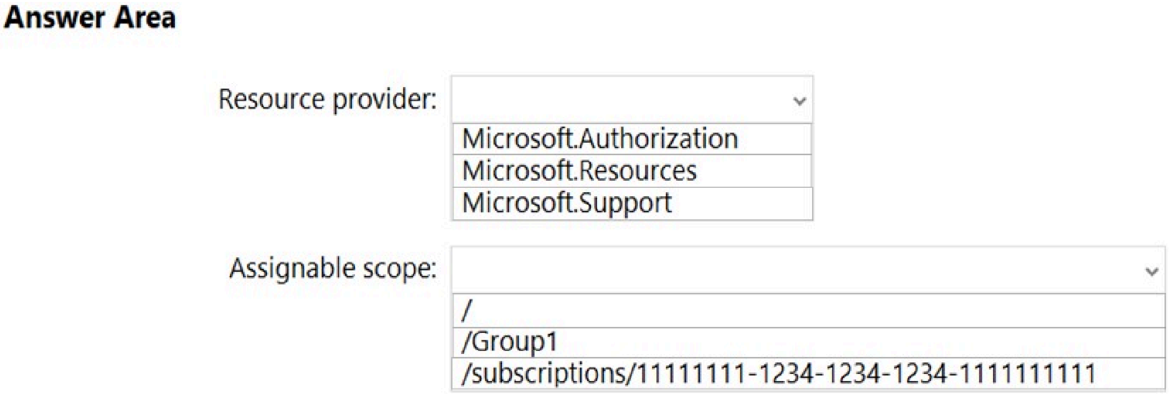
You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-
1111111111.

You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.

What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

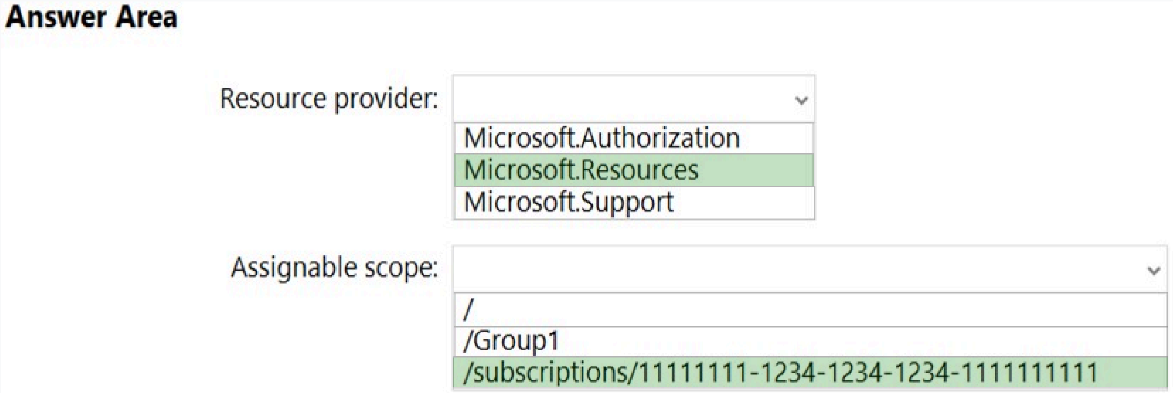


Answer Area

Resource provider:
- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.Support

Assignable scope:
- /
- /Group1
- /subscriptions/11111111-1234-1234-1234-1111111111

Suggested Answer:



Answer Area

Resource provider:
- Microsoft.Authorization
- [✓ Microsoft.Resources]
- Microsoft.Support

Assignable scope:
- /
- /Group1
- [✓ /subscriptions/11111111-1234-1234-1234-1111111111]

Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

NarenderSingh Highly Voted 3 years, 7 months ago

Assignable Scope is Management Group Now which is /Group1

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

On the Assignable scopes tab, you specify where your custom role is available for assignment, such as management group, subscriptions, or resource groups.

upvoted 25 times

asodataone 6 months, 3 weeks ago

Resource Provider: Microsoft.Resources

Assignable Scope: /providers/Microsoft.Management/managementGroups/Group1 Key Concepts:

Resource Provider: The resource provider for managing tags in Azure is Microsoft.Resources. Tags are a resource management feature provided by this provider, so your role should have permissions related to this resource provider.

Assignable Scope: The assignable scope should be the management group Group1, and it can include the subscriptions and resources within that management group, since the goal is to manage tags across all objects in Group1. Therefore, you would assign the scope to Group1 and ensure that it can cascade to all the resources inside Group1.

upvoted 1 times

ITFranz 6 months ago

The resource provider for managing tags in Azure is Microsoft.Resources. While this isn't explicitly stated in the search results, it can be inferred from the context:
Tags are a feature of Azure Resource Manager (ARM), which is part of the Microsoft.Resources namespace.
Tags can be applied to various Azure resources across different resource providers, but the underlying functionality for tag management is handled by Azure Resource Manager.
The search results mention using Azure Resource Manager JSON templates for tagging, which indicates that the tag management is part of the ARM functionality.
Tags in Azure can be managed through various methods, including:
Azure Portal
Azure PowerShell
Azure CLI
Azure Resource Manager templates
These methods all interact with the Microsoft.Resources provider to manage tags across different Azure resources and resource groups.

upvoted 1 times

TiredofTesting 3 years, 6 months ago

Concurred and tested. You can assign this to a subscription, management group or resource group.

upvoted 2 times

maxsh3 3 years, 2 months ago

Adding a management group to assignable scopes is currently in (preview).

upvoted 2 times

thienvupt Highly Voted 4 years ago

Correct Answer
Setting assignable scope to root scope ("/") is not supported. Currently, you cannot add a management group as an assignable scope.

upvoted 14 times

schpeter_091 Most Recent 8 months ago

From MS site: "You can't assign the custom role at the management group scope itself; however, you can assign the custom role at the scope of the subscriptions within the management group."
https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles

upvoted 2 times

410ns0 10 months, 3 weeks ago

*/Group1

upvoted 1 times

ITFranz 10 months, 4 weeks ago

To support the answer:
Resource provider:
https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources#required-access
There are two ways to get the required access to tag resources.
You can have write access to the Microsoft.Resources/tags resource type. This access lets you tag any resource, even if you don't have access to the resource itself
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes
On the Assignable scopes tab, you specify where your custom role is available for assignment, such as management group, subscriptions, or resource groups. Depending on how you chose to start, this tab might already list the scope where you opened the Access control (IAM) page.

upvoted 1 times

Jimmy500 11 months, 1 week ago

Hi guys, I think here answer will be as like this:
Box-1 Microsoft.Resources
Box-2 /subscription/id of subcsction.
Most of us mixed up with box2 in the second option of it with the /Group1.
Let tell why not (please refer here:https://learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview#scope-examples.
According to this in order to assign role to management group structure needs to be like this:
/providers/Microsoft.Management/managementGroups/marketing-group in our case in it should have been like this:

/providers/Microsoft.Management/managementGroups/Group1, that is why we need choose 3 rd option for Box-2 which is /subscriptions/id of subscription

upvoted 1 times

⊟ **pentium75** 11 months ago

We don't know which syntax is used here. "/Group1" is what we need to assign the permission to. Assigning it to a subscription will not apply it to 'all objects in Group1' as required, even if CURRENTLY there are no other subscriptions.

upvoted 1 times

⊟ **Adt3ster** 1 year, 6 months ago

Correct and tested. The right answer is resources provider and subscription level since if that was for MG level the name should be /providers/Microsoft.Management/managementGroups/Group1

upvoted 2 times

⊟ **wardy1983** 1 year, 7 months ago

Explanation:

Microsoft resourcews

Assignable Scope is Management Group Now which is /Group1

On the Assignable scopes tab, you specify where your custom role is available for assignment, such as management group, subscriptions, or resource groups.

upvoted 2 times

⊟ **wardy1983** 1 year, 7 months ago

Microsoft resourcews

Assignable Scope is Management Group Now which is /Group1

On the Assignable scopes tab, you specify where your custom role is available for assignment, such as management group, subscriptions, or resource groups.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignablescopes

upvoted 2 times

⊟ **[Removed]** 1 year, 7 months ago

Scope examples

Scope Example

Management group /providers/Microsoft.Management/managementGroups/marketing-group

Subscription /subscriptions/00000000-0000-0000-0000-000000000000

Resource group /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/Example-Storage-rg

upvoted 2 times

⊟ **ESAJRR** 1 year, 9 months ago

1. Microsfot.resources

2. Group?

upvoted 4 times

⊟ **_fvt** 1 year, 11 months ago

Seems that you can now assign custom roles to a Management group and it's not in Preview anymore. However you need to specify the resourceID, not the name (so it would look like /providers/Microsoft.Management/managementGroups/Group1).

https://docs.microsoft.com/en-us/azure/governance/management-groups/overview#azure-custom-role-definition-and-assignment

https://learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview#scope-examples

So the answer given is Right, you need to assign it to the Sub.

upvoted 2 times

⊟ **Troublemaker** 1 year, 11 months ago

In Exam - 28/7/2023

upvoted 1 times

⊟ **Holii** 2 years, 1 month ago

https://learn.microsoft.com/en-us/azure/templates/microsoft.resources/tags?pivots=deployment-language-bicep It can be either Management Scope (/Group1) or Subscription (/subscription)

Since the Management Group isn't fleshed out I am leaning on /subscription.

Otherwise the answer would follow a similar naming convention: (/providers/Microsoft.Management/managementGroups/Group1)
but instead it just states /Group1, rather than giving context that this actually is a Management Group.
upvoted 2 times

⊟ **zellck** 2 years, 1 month ago
1. Micosoft.Resources
2. /Group1

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources#required-access

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, subscription, and resource group scopes.
upvoted 12 times

⊟ **majstor86** 2 years, 3 months ago
1. Microsfot.resources
2. \group?
upvoted 3 times

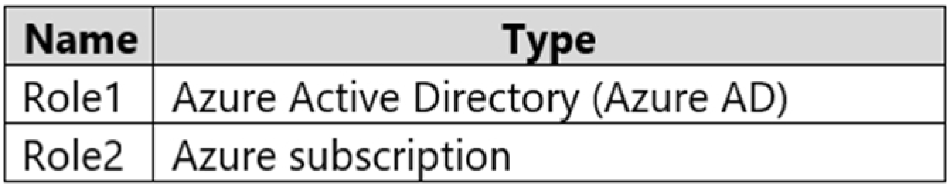
⊟ **Muaamar_Alsayyad** 2 years, 8 months ago
Microsfot.resources
\group

https://learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview
upvoted 4 times

Question #58 Topic 2

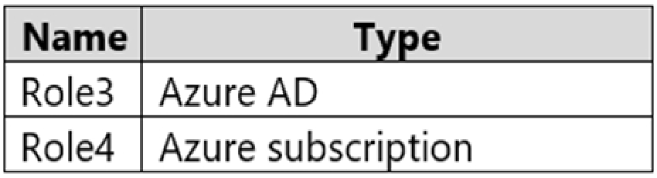
HOTSPOT -

You have an Azure subscription that contains the custom roles shown in the following table.



Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

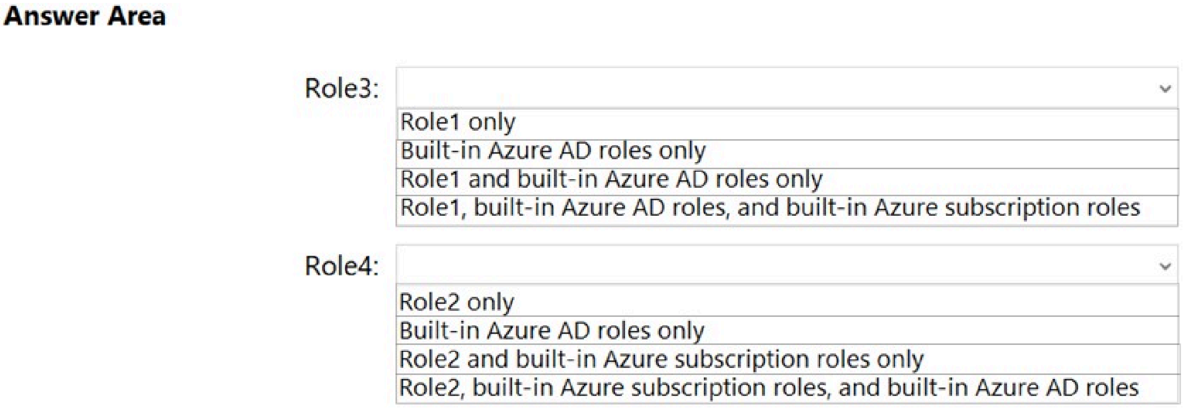


Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

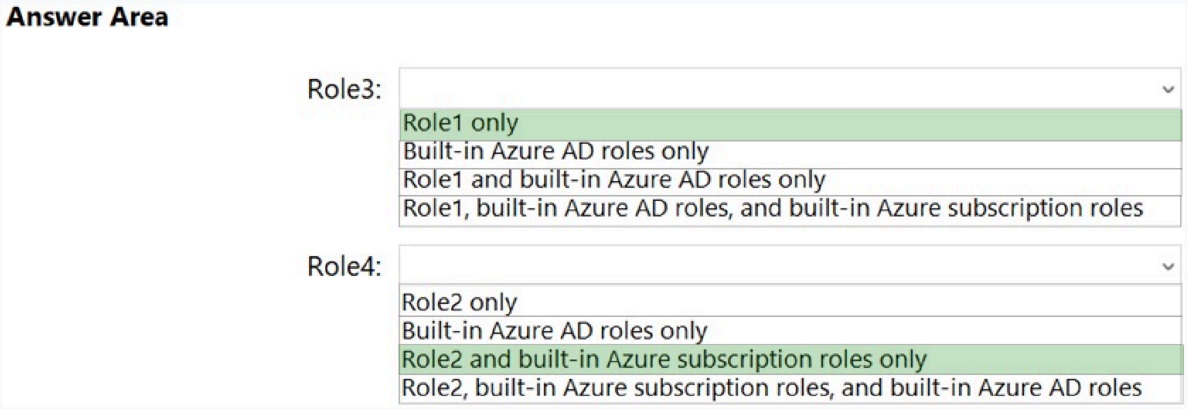


Answer Area

Role3:
- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:
- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Suggested Answer:



Answer Area

Role3:
- [✓ Role1 only]
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:
- Role2 only
- Built-in Azure AD roles only
- [✓ Role2 and built-in Azure subscription roles only]
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

rsharma007 Highly Voted 3 years, 10 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 55 times

vaaws 3 years, 10 months ago

Azure AD supports 2 types of roles definitions:

Built-in roles
Custom roles

Built-in roles are out of box roles that have a fixed set of permissions. These role definitions cannot be modified. There are many built-in roles that Azure AD supports, and the list is growing. To round off the edges and meet your sophisticated requirements, Azure AD also supports custom roles. Granting permission using custom Azure AD roles is a two-step process that involves creating a custom role definition and then assigning it using a role assignment. A custom role definition is a collection of permissions that you add from a preset list. These permissions are the same permissions used in the built-in roles.

REF: https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-overview

upvoted 5 times

⊟ **ITFranz** 5 months, 4 weeks ago

to support second answer.

built-in Azure subscriptions cannot be cloned directly. While you can create new subscriptions or move resources between subscriptions, there is no direct cloning functionality for built-in Azure subscriptions.

However, there are methods to achieve similar results:

Create a new subscription and manually recreate the resource structure.

Use Azure Resource Manager (ARM) templates to deploy resources consistently across subscriptions.

upvoted 1 times

⊟ **vaaws** 3 years, 10 months ago

Any REF URL than we cannot clone Built-in AD Roles?

upvoted 1 times

⊟ **STC007** 1 year, 9 months ago

Here you have : https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-overview

upvoted 1 times

⊟ **Daniel76** 3 years, 2 months ago

The purpose of cloning is to modify and customize the roles. Since a built-in role is out-of-the-box and cannot be modified, there is no point allowing user to clone it.

upvoted 1 times

⊟ **Ajdlfasudfo0** 2 years, 6 months ago

this explanation makes no sense since it would also apply to RBAC Resource roles

upvoted 4 times

⊟ **somenick** 2 years, 9 months ago

You can try it in the lab

upvoted 2 times

⊟ **stvsting** Highly Voted 3 years, 11 months ago

the answer is correct. test at the lab. you can clone only custome azure ad role or create from scratch.

upvoted 20 times

⊟ **scottyboy23** Most Recent 11 months, 2 weeks ago

on exam 20240715

upvoted 5 times

⊟ **Swaminathan** 1 year, 5 months ago

Role1 and 2 are custom roles. why can't role1 be cloned?

upvoted 1 times

⊟ **brooklyn510** 1 year, 5 months ago

On exam 1/2/24

upvoted 6 times

⊟ **Obama_boy** 1 year, 6 months ago

in exam 08/12/23

upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

Role3: Role1 only

Role4: Role 2 and built in Azure Subscription role only

upvoted 12 times

⊟ **samimshaikh** 2 years, 5 months ago

For AzureAD new custom role only can be created from "Clone from a custom role" and "Start from scratch" so answer if can be cloned only from the existing custom role which "Role1" for this case.

upvoted 1 times

⊟ **salmantarik** 2 years, 6 months ago

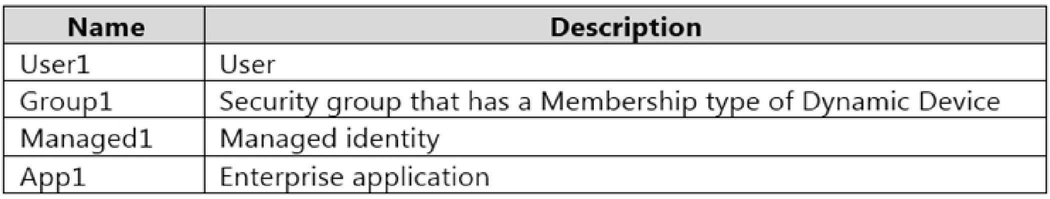
Correct answer. You can only clone Azure built in roles to create custom roles but you cant clone Azure AD roles.

upvoted 3 times

Question #59 Topic 2

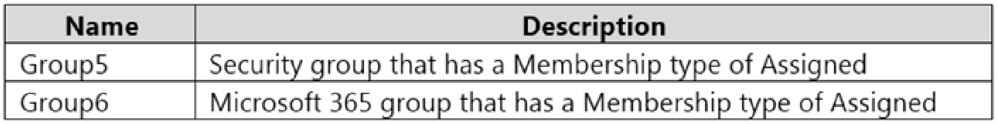
HOTSPOT -

You have an Azure subscription that contains the Azure Active Directory (Azure AD) resources shown in the following table.



Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

You create the groups shown in the following table.

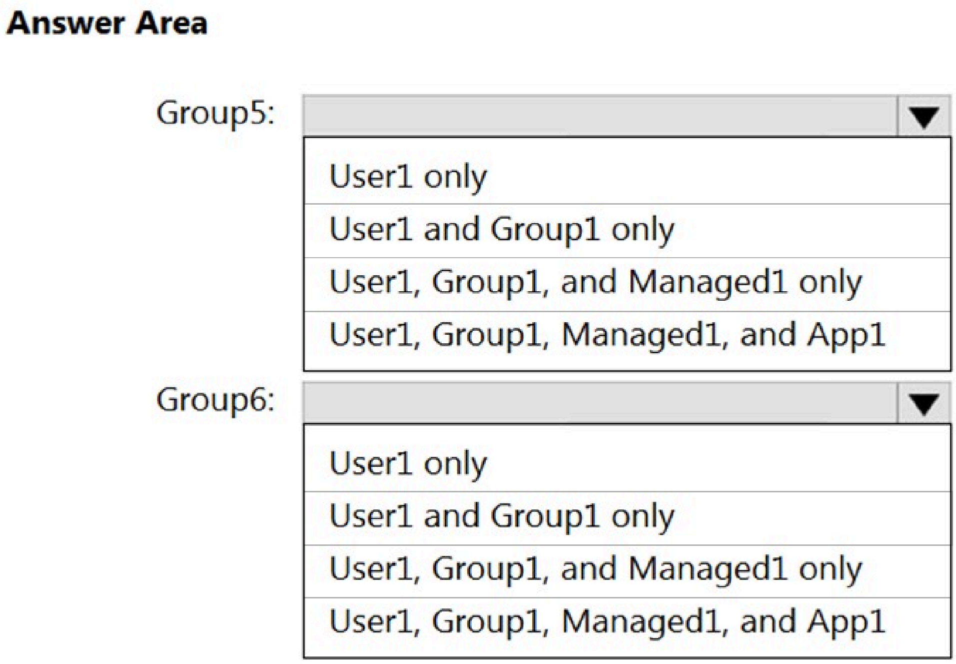


Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

Which resources can you add to Group5 and Group6? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

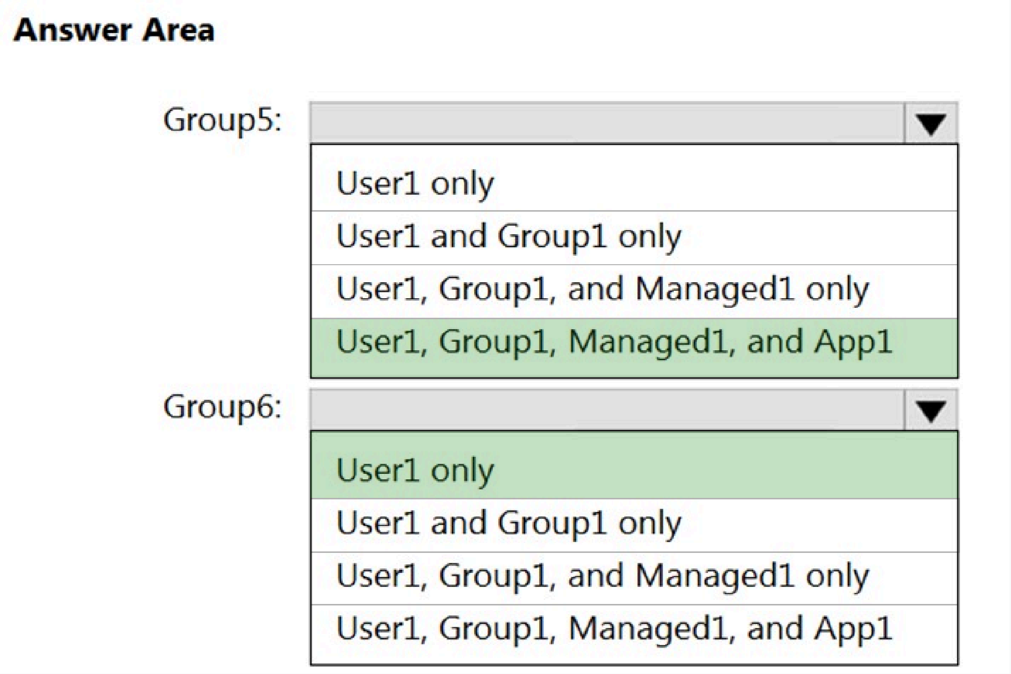


Answer Area

Group5:
- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Group6:
- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Suggested Answer:



Answer Area

Group5:
- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- [✓ User1, Group1, Managed1, and App1]

Group6:
- [✓ User1 only]
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

JBS Highly Voted 3 years, 8 months ago

Given answers are correct. For Group5, You can add enterprise applications to security groups. (Tested & Verified)
upvoted 45 times

orcnylmz Highly Voted 2 years, 8 months ago

Answer is
Group5: User1, Group1, Managed1
Group6: User1

Here is why:
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-learn-about-groups#group-types

Members of a security group can include users, devices, other groups, and service principals, which define access policy and permissions. Owners of a security group can include users and service principals.

Members of a Microsoft 365 group can only include users.
upvoted 13 times

ITFranz 5 months, 4 weeks ago

To support answer Group5.
you cannot add enterprise applications to a security group that has the membership type of "Assigned". Security groups are used to group users and devices, not applications. The relationship between security groups and enterprise applications works in the opposite direction:
Security groups (with assigned membership) can be added to enterprise applications for access control.
Users and devices can be assigned to security groups.
Enterprise applications can then use these security groups to manage access.
This approach allows for more efficient management of application access by grouping users and devices, rather than adding applications to groups. It's important to note that only security groups can be used for this purpose, and they cannot be nested when assigning to enterprise applications
upvoted 2 times

basak 1 year, 11 months ago

For Group 5 your answer is wrong. When an app is registered a service principal is created. according to your description service principle can be added in security group. Therefore, App1 also can be added.
upvoted 1 times

_fvt 1 year, 10 months ago

App1 is not an App Registration but an Enterprise Application. An Enterprise Application is a Service Principal.
So, answer is
Group5: User1, Group1, Managed1, App1
Group6: User1
upvoted 15 times

ca7859c Most Recent 1 month ago

Answer is correct

You can manage two types of groups in the Microsoft Entra admin center:
https://learn.microsoft.com/en-us/entra/fundamentals/concept-learn-about-groups

Security groups: Used to manage access to shared resources.

Members of a security group can include users, devices, service principals.
Groups can be members of other groups, sometimes known as nested groups. See note.
Users and service principals can be the owner of a security group.
Microsoft 365 groups: Provide collaboration opportunities.

Members of a Microsoft 365 group can only include users.
Users and service principals can be the owner of a Microsoft 365 group.
People outside of your organization can be members of a group.
For more information, see Learn about Microsoft 365 Groups.
upvoted 1 times

Jimmy500 11 months, 3 weeks ago

When we create managed identity does not matter user assigned and system assigned it registered as an enterprise application in our tenant and we can add the to them to the security groups. All in all, we can add user assigned, system assigned managed identities, service principals to the security groups as well as users and other security groups, we cannot add Microsoft 365 group to the security groups. From here we can say that for the Box-1 we can choose , User1,Group1,Manged1,App1(this is service principial as question says this has been registered in entra that is why we can add it as well).
For the box 2 we can only add User1, we cannot add Service principal, devices, security groups, managed identity to the Microsoft 365 group.
Answer will be like this:
Box-1 All
Box-2 only User1.
Regards!
Quick not also given answer is corret!
upvoted 5 times

Goke282 1 year, 3 months ago
In Azure, you cannot have a device and a user in the same security group. Dynamic groups in Azure Active Directory (Azure AD) can be created for devices or for users, but you can't create a rule that contains both users and devices. Device membership rules can reference only device attributes1. This means you would need to create separate groups for users and devices if you want to manage them dynamically based on their attributes.

If you need to manage devices and users together in some way, you might consider creating separate groups and then using Azure policies or other management tools to apply the necessary controls across those groups.

For the above reason, it can be concluded that the answer to Group5 is User1 Only.
upvoted 2 times

pentium75 11 months ago
"You can't create a rule that contains both users and devices" yeah but that has not been asked here. Security groups can contain other security groups. A security group with assigned membership can include users, service principals, managed identities, or other security groups.
upvoted 1 times

Goke282 1 year, 3 months ago
I think the answer is wrong for Group 5 because you cannot have devices and users in the same group. Therefore Group 1 cannot be in Group 5 as the others.
upvoted 1 times

pentium75 11 months ago
We cannot have "devices and users in the same group" but we can have multiple security groups (one with users, one with devices) in another security group.
upvoted 1 times

Obama_boy 1 year, 6 months ago
in exam 08/12/23
upvoted 3 times

[Removed] 1 year, 9 months ago
You cannot add AppRegistraion to a security group just tested in the lab no option to add to enterprise application is coming up in the list of members
upvoted 1 times

fireb 1 year, 9 months ago
App1 is an Enterprise Application, not an AppRegistration.
upvoted 3 times

Troublemaker 1 year, 11 months ago
In Exam - 28/7/2023
upvoted 2 times

zellck 2 years, 1 month ago
1. User1, Group1, Managed1, and App1
2. User1 only

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-learn-about-groups#group-types
- Security: Used to manage user and computer access to shared resources.
For example, you can create a security group so that all group members have the same set of security permissions. Members of a security group can

include users, devices, other groups, and service principals, which define access policy and permissions. Owners of a security group can include users and service principals.
- Microsoft 365: Provides collaboration opportunities by giving group members access to a shared mailbox, calendar, files, SharePoint sites, and more. This option also lets you give people outside of your organization access to the group. Members of a Microsoft 365 group can only include users. Owners of a Microsoft 365 group can include users and service principals.
upvoted 7 times

⊟ **majstor86** 2 years, 3 months ago
Correction for Group 5: User1, Group1, Managed1, App1
upvoted 2 times

⊟ **majstor86** 2 years, 3 months ago
Group5: User1, Group1, Managed1
Group6: User1
upvoted 2 times

⊟ **Amit3** 2 years, 9 months ago
# In EXAM - 01-Oct-2022
upvoted 4 times

⊟ **salmantarik** 3 years, 2 months ago
Security groups can be used for either devices or users, but Microsoft 365 Groups can be only user groups. Given answer is correct
upvoted 4 times

⊟ **siobhan1** 3 years, 3 months ago
# In exam today 03/12/2022
upvoted 4 times

⊟ **cfsxtuv33** 3 years, 5 months ago
Some extra info with an added link. After identifying the resource types of your resources, you must investigate if they can be moved, and the restrictions that are in place. Check your resource types against the move list below. The list shows whether each resource type can be moved between resource groups or between subscriptions: https://docs.microsoft.com/en-us/learn/modules/move-azure-resources-another-resource-group/4-assess-resources

For example, these resources can be moved:
Azure Storage accounts
Azure virtual machines
Azure virtual networks

These resources can't be moved:
Azure Active Directory domain services
Azure Backup vaults
Azure App Service gateways
upvoted 2 times

⊟ **HananS** 3 years, 6 months ago
Unfortunately, you cannot add an application as a member of Azure AD group.
https://stackoverflow.com/questions/47762262/add-aad-application-as-a-member-of-a-security-group
so the answer is user 1 ,managed1 and group 1 only for the first one
upvoted 2 times

⊟ **JL15546** 3 years, 5 months ago
Sorry HananS. I just tested it and it worked. So, yes, we an app can be added as a member of a AZ AD Security group.
Answer is correct.
upvoted 8 times

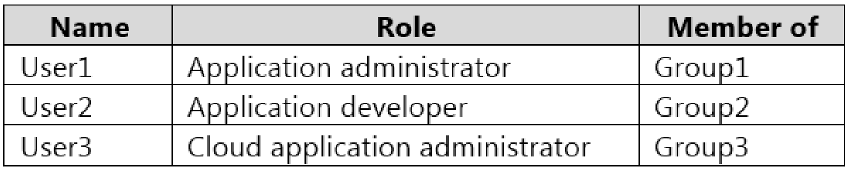
⊟ **OpsecDude** 2 years, 9 months ago
Just like JL15546 says, plus think of the app as a service principal to which roles can be assigned.
upvoted 1 times

Question #60

Topic 2

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.



Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

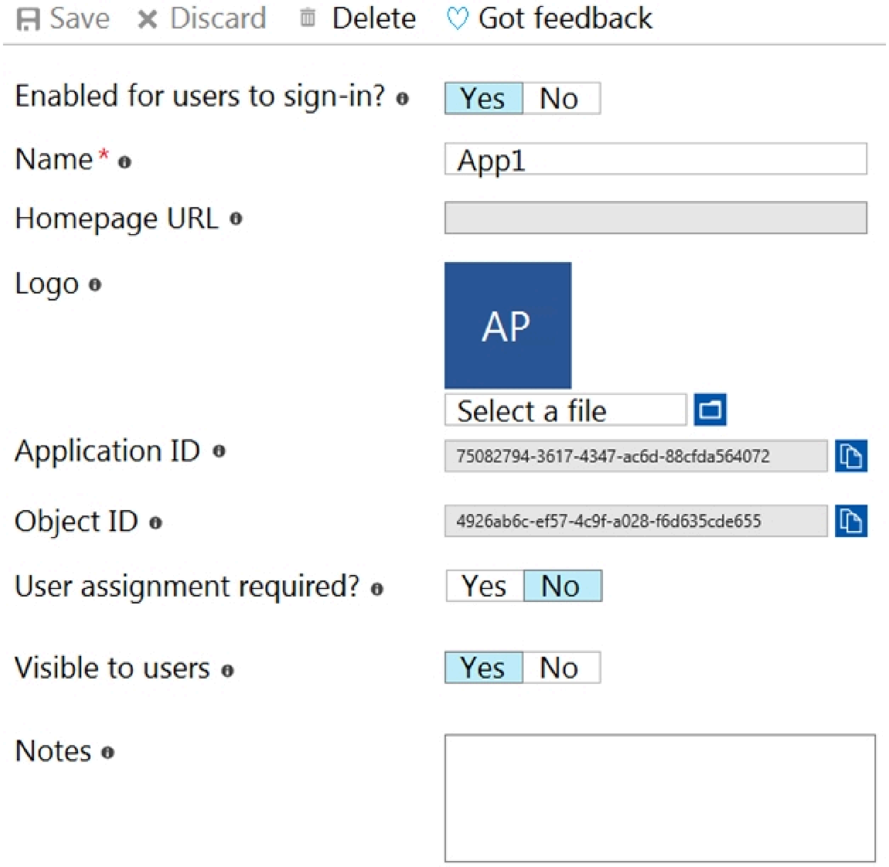
Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

✑ Owners: User1

✑ Users and groups: Group2

You configure the properties of App1 as shown in the following exhibit.



Enabled for users to sign-in? [✓ Yes] No

Name * App1

Homepage URL

Logo

Application ID 75082794-3617-4347-ac6d-88cfda564072

Object ID 4926ab6c-ef57-4c9f-a028-f6d635cde655

User assignment required? Yes [✓ No]

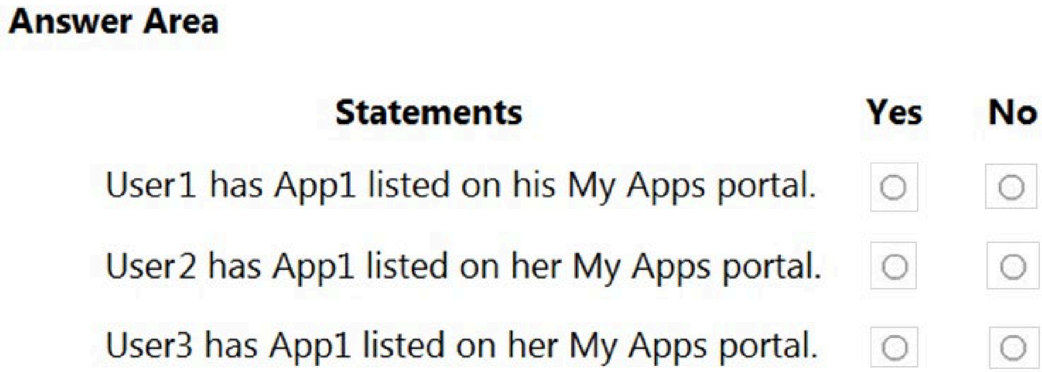
Visible to users [✓ Yes] No

Notes

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

NOTE: Each correct selection is worth one point.

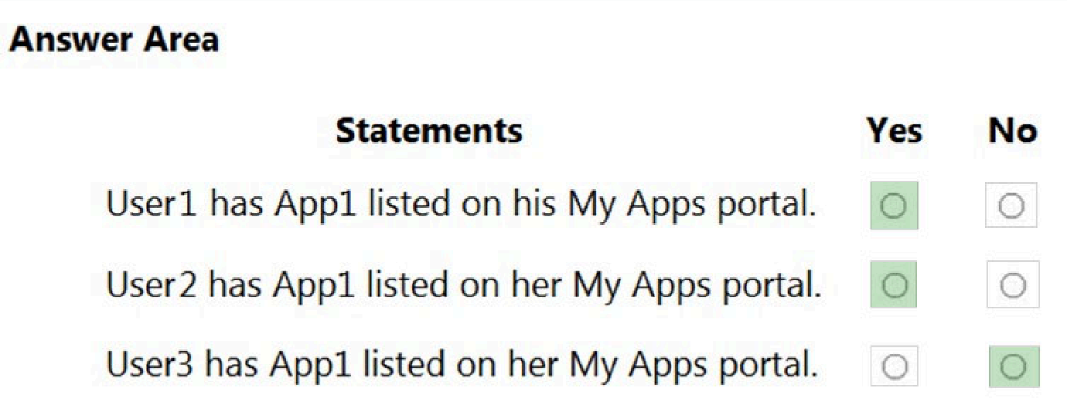
Hot Area:



Answer Area

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	○	○
User2 has App1 listed on her My Apps portal.	○	○
User3 has App1 listed on her My Apps portal.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	[✓ ○]	○
User2 has App1 listed on her My Apps portal.	[✓ ○]	○
User3 has App1 listed on her My Apps portal.	○	[✓ ○]

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

Joshing Highly Voted 3 years, 4 months ago

JSab is correct. No, Yes, No.

1. Owners don't see app in MyApps portal unless they are also assigned the App via group or user assignment. - No
2. User 2 is part of Group 2 so and the app is visible so will show in MyApps portal. - Yes
3. User 3 is in Group 3 that is a member of Group 2 but nested groups aren't supported in App assignments so only direct Group 2 membership will work. - No

upvoted 67 times

xRiot007 11 months, 2 weeks ago

User assignment is set to NO, so the explanation at point 1 does not apply.
Visible to users is set to Yes.
User 1 will see the app.

upvoted 3 times

pentium75 11 months ago

"User assignment required = No" means that users can access the app via its URL, but still they will not see it in "My apps" unless they are assigned as users.

upvoted 3 times

JSab Highly Voted 3 years, 6 months ago

No, Yes, No

upvoted 32 times

milan24_2000 3 years, 6 months ago

tested in the lab, owner dont get the app showing

upvoted 14 times

Jacky_YO 3 years, 3 months ago

My Answer : NO , YES , NO . Tested in the lab.
my app portal is https://myapps.microsoft.com/ , not EA or Apps display it .
user1 : signin to https://myapps.microsoft.com/ , No display App1.
user2 : signin to https://myapps.microsoft.com/ , YES display App1.
user3 : signin to https://myapps.microsoft.com/ , No display App1.

upvoted 6 times

Arvinn Most Recent 3 months, 1 week ago

Yes, Yes, Yes, since the app setting changed to visible to everyone and also user assignment not required.

upvoted 1 times

Jimmy500 11 months, 1 week ago

Answer for this question will be as No,Yes,No.
Keep in mind these thing if you are just an owner of application and your security principial does not seen in the Users and Groups then you will not see the application in myApps.
Nested groups do not supporting by myapps , means if you are member of nested group and added via it to the Users and Groups you will not see app in myApps.
If your security principial(user name) in listed under Users and Groups for the enterpise application's Users and Groups blade you will see the

application in the myapps portal.

Regards

upvoted 2 times

wardy1983 1 year, 8 months ago

1. Owners don't see app in MyApps portal unless they are also assigned the App via group or user assignment.- No

2. User 2 is part of Group 2 so and the app is visible so will show in MyApps portal. - Yes

3. User 3 is in Group 3 that is a member of Group 2 but nested groups aren't supported in App assignments so only direct Group 2 membership will work. - No

upvoted 4 times

Alster77 1 year, 11 months ago

question popped up in exam taken 24 July 2023

upvoted 6 times

zellck 2 years, 1 month ago

NYN is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivots=portal

When you assign a group to an application, only users in the group will have access. The assignment doesn't cascade to nested groups.

upvoted 2 times

Dannith 2 years, 3 months ago

As user assignment required is set to "no" and display in portal is "yes", surely the answer is YYY?

upvoted 1 times

majstor86 2 years, 3 months ago

NO

YES

NO

upvoted 2 times

samimshaikh 2 years, 5 months ago

NYN... TESTED

upvoted 1 times

sofieejo 2 years, 5 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 4 times

JohnBentass 2 years, 6 months ago

No,Yes,No

upvoted 2 times

edurakhan 2 years, 7 months ago

NO, YES, NOW - just tested!

upvoted 1 times

> **edurakhan** 2 years, 7 months ago
>
> NO, YES, NO :-)
>
> upvoted 2 times

shafqat 2 years, 9 months ago

No

Yes

NO : When you assign a group to an application, only users in the group will have access. The assignment does not cascade to nested groups.

upvoted 3 times

the_humanoid_typhoon 3 years, 2 months ago

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-service-limits-restrictions#:~:text=App%20role%20assignment%2C%20for%20both%20access%20and%20provisioning.%20Assigning%20groups%20to%20an%20app%20is%

upvoted 2 times

sieira 3 years, 4 months ago

Yes, Yes, No tested.the application portal https://myapplications.microsoft.com/ that is displayed for when you logon with user 3 is user 2's portal. Both user 2 and user 2 can access the application but user 3 cannot (because group 3 is nested in group 2)

upvoted 2 times

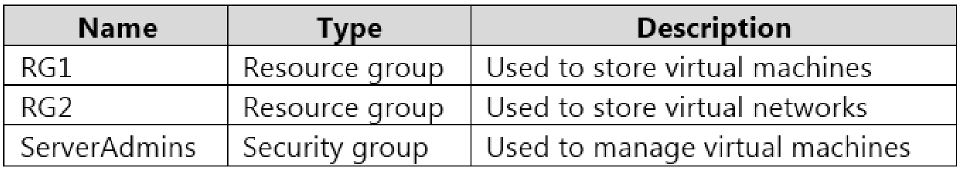
⊟ **Itzvaibhav** 3 years, 5 months ago

Is it Y-Y-Y ?

upvoted 3 times

Question #61 *Topic 2*

You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

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

✑ Create virtual machines in RG1 only.

✑ Connect the virtual machines to the existing virtual networks in RG2 only.

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a custom RBAC role for RG2

B. the Network Contributor role for RG2

C. the Contributor role for the subscription

D. a custom RBAC role for the subscription

E. the Network Contributor role for RG1

F. the Virtual Machine Contributor role for RG1

Suggested Answer: *AF*

Reference:

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

Community vote distribution

AF (79%) 10% 10%

Eltooth Highly Voted 3 years, 3 months ago

Selected Answer: AF

A. a custom RBAC role for RG2 - would provide least priv over RG2

B. the Network Contributor role for RG2 - provides too much priv over RG2

C. the Contributor role for the subscription - Cannot be C

D. a custom RBAC role for the subscription - to much permission

E. the Network Contributor role for RG1 - Cannot be E

F. the Virtual Machine Contributor role for RG1 - required to create VM's

Therefore A and F would provide least priv to perform tasks.

upvoted 17 times

machado 2 years, 2 months ago

How can D. be too much permission if it's custom and you can select scopes?

upvoted 2 times

in_da_cloud 2 years, 1 month ago

Because the scope is bigger than required - it would apply the permission on subscription instead of only RG.

upvoted 9 times

thienvupt Highly Voted 3 years, 8 months ago

BF for my choose

upvoted 8 times

xavi1 3 years, 8 months ago

not B, seems does not include virtual machine connection: https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor

upvoted 2 times

BillBaits 3 years, 8 months ago

For me this is part of Microsoft.Network/*
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/built-in-roles#network-contributor

So I think BF is correct
upvoted 2 times

pentium75 11 months ago
But Network Contributor can do all kinds of stuff, they are not supposed to do anything except connect VMs to existing networks
upvoted 1 times

Sabr_ Most Recent 2 months, 3 weeks ago
Selected Answer: AF
Exam question 6th April 2025
upvoted 1 times

Nhadipour 4 months, 3 weeks ago
Selected Answer: BF
Network Contributor is the most appropriate built-in role for this! grants enough necessary permissions to manage virtual networks within RG2.
While you could create custom roles, it's not necessary to violate the principle of least privilege. Built-in roles provide the required permissions.
upvoted 1 times

Tom_tank 4 months, 4 weeks ago
Selected Answer: BF
Virtual Machine Contributor role for RG1: This role will allow ServerAdmins to create and manage virtual machines in RG1.

Network Contributor role for RG2: This role will enable ServerAdmins to connect the virtual machines to the existing virtual networks in RG2.
upvoted 1 times

xRiot007 11 months, 2 weeks ago
Correct answers are :
A - a custom RBAC role for RG2, providing least privilege - any other answer/explanations are incorrect.
F - the virtual Machine Contributor on RG1 - this is the best option from the listed ones, any other answer is incorrect. An even better option than this would be a custom RBAC role on RG1.
upvoted 1 times

mrt007 1 year, 3 months ago
The correct answers are F. the Virtual Machine Contributor role for RG1 and B. the Network Contributor role for RG2.

Assigning the Virtual Machine Contributor role for RG1 will allow ServerAdmins to create virtual machines in RG1.

Assigning the Network Contributor role for RG2 will allow ServerAdmins to connect the virtual machines to the existing virtual networks in RG2
upvoted 3 times

CHIEF101H 1 year, 4 months ago
Selected Answer: AF
A. a custom RBAC role for RG2 - would provide least priv over RG2
&
F.the Virtual Machine Contributor role for RG1 - required to create VM's
upvoted 1 times

Ivan80 1 year, 5 months ago
In exam 1/28/24
upvoted 3 times

BigShot0 1 year, 9 months ago
Selected Answer: AF
Not B - Network Contributor does not have Microsoft.Network/networkInterfaces/*
upvoted 2 times

rameezali 1 year, 3 months ago
Although network contributor is not the right answer because it gives you way more permissions than to attach a NIC, but the role network contributor does have Microsoft.Network/*
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface?tabs=azure-portal#permissions

upvoted 1 times

_fvt 1 year, 10 months ago

Selected Answer: DF

You cannot create a VM without being able to attach it's network Interfaces to a VNet.
The only working option in definitive is:
D - A Custom role for attaching the network cards on the Subscription level,
F - VM contributor on RG1.

upvoted 1 times

pentium75 11 months ago

Wouldn't a custom role in RG2 allow you to attach your VM's network to a VNet?

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: AF

AF is the answer.

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 4 times

zellck 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 5 times

stepman 2 years, 2 months ago

I forgot what I chose, but this was On exam 4/27 with the new exam experience. No Sim or lab.

upvoted 3 times

tath 2 years, 6 months ago

need guidance for clearing az-500 exam

upvoted 1 times

Ajdlfasudfo0 2 years, 6 months ago

step one: learn
step two: pass exam
step three: profit

upvoted 18 times

chikorita 2 years, 4 months ago

step four: renew certification (REPEATTT)

upvoted 9 times

somenick 2 years, 9 months ago

Selected Answer: AF

B is not ok because it allows to create networks, support tickets, manage monitoring - so too much.

upvoted 3 times

Innovite 3 years, 3 months ago

Least priv.. so provided answer is right..

upvoted 3 times

starnb 3 years, 3 months ago

Selected Answer: BF

The correct answer is B and F

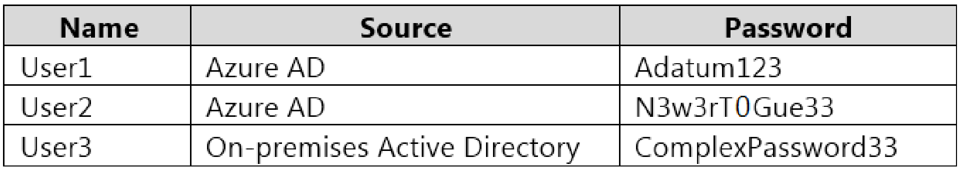
upvoted 2 times

Question #62 Topic 2

HOTSPOT -

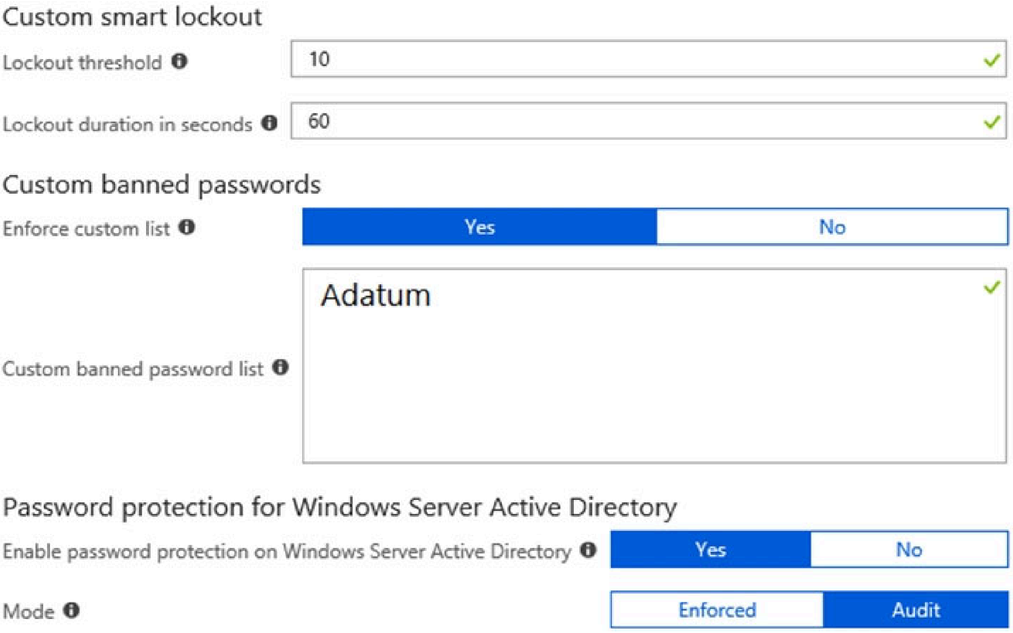
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).

The Azure AD tenant contains the users shown in the following table.



Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

You configure the Authentication methods `" Password Protection settings for adatum.com as shown in the following exhibit.



Custom smart lockout

Lockout threshold: 10 ✓

Lockout duration in seconds: 60 ✓

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list: Adatum ✓

Password protection for Windows Server Active Directory

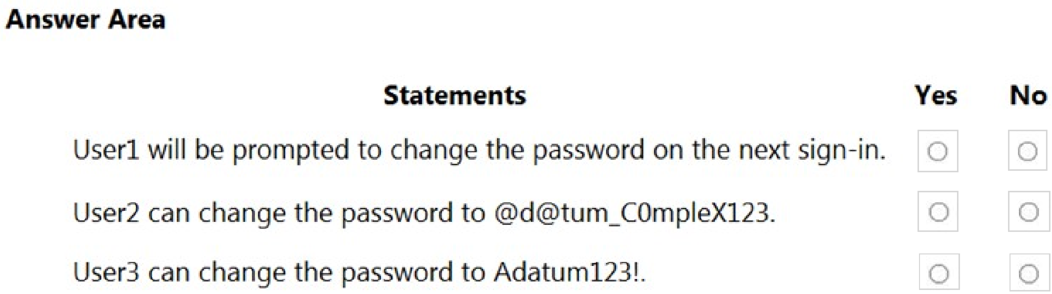
Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: Enforced [✓ Audit]

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

NOTE: Each correct selection is worth one point.

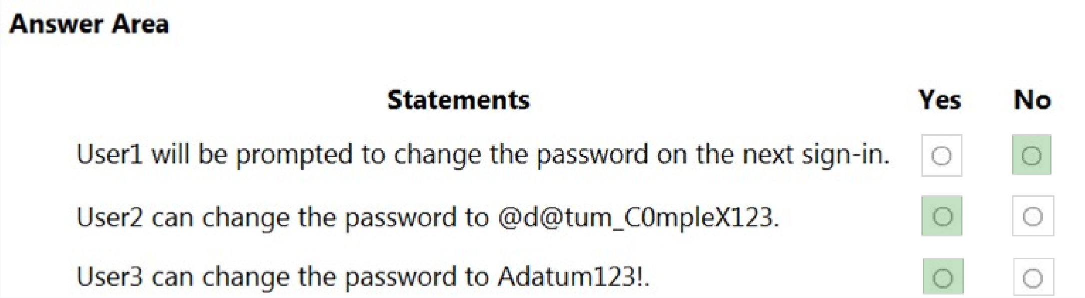
Hot Area:



Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	○
User2 can change the password to @d@tum_C0mpleX123.	○	○
User3 can change the password to Adatum123!.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	●
User2 can change the password to @d@tum_C0mpleX123.	●	○
User3 can change the password to Adatum123!.	●	○

Reference:

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

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

maylevi Highly Voted 3 years, 9 months ago

NO,YES,YES.

3)Audit mode

Audit mode is intended as a way to run the software in a "what if" mode. Each Azure AD Password Protection DC agent service evaluates an incoming password according to the currently active policy.

If the current policy is configured to be in audit mode, "bad" passwords result in event log messages but are processed and updated. This behavior is the only difference between audit and enforce mode. All other operations run the same.
upvoted 55 times

ConanBarb 2 years, 3 months ago

1 - No: Of course, nothing can evaluate existing passwords since they are stored hashed and not clear-text.

And it says here:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
"It is important to note that Azure AD Password Protection can only validate passwords during password change or set operations. Passwords that were accepted and stored in Active Directory prior to the deployment of Azure AD Password Protection will never be validated and will continue working as-is. Over time, all users and accounts will eventually start using Azure AD Password Protection-validated passwords as their existing passwords expire normally. Accounts configured with "password never expires" are exempt from this."

2 - No
"Enforce custom list" in effect. (The Audit mode is under the title sub-title "Password protection for Windows Server Active Directory" and applies only to that.)

Yes
Even though "Enforce custom list" is in effect, the subordinate setting for "Password protection for Windows Server Active Directory" is in Mode = Audit.
upvoted 23 times

ConanBarb 2 years, 3 months ago

And in fact, I tested case 2 in portal, and was denied password change due to banned words (had Mode = Audit)
upvoted 8 times

xavi1 3 years, 8 months ago

audit only applies to the local AD, not azure ad
upvoted 12 times

OpsecDude 2 years, 9 months ago

But Password protection is an AAD feature.
upvoted 1 times

Jacky_YO 3 years, 3 months ago

my Answer : No , Yes , Yes
upvoted 3 times

IvanIco 1 year, 8 months ago

and it's wrong
upvoted 2 times

Floweezy Highly Voted 3 years, 7 months ago

YES - User 1 is Azure AD hence his Adatum123 is now consider a bad password and must change it
NO - User 2 cannot change his password as suggested cause it contains a reference to Adatum (replacing A with @ will not bypass it)
YES - In audit mode so the policy does not enforce
upvoted 30 times

xRiot007 11 months, 2 weeks ago

Box 1 is No - In Audit mode when a bad password is used for login or changed into, an event is logged, but the change still happens.
upvoted 1 times

adamsca 3 years, 6 months ago

Why did you just Apply Audit mode to User3 and not User1 and User3? Because it's in audit mode policies will not be enforced so answers are NO, YES, YES.
upvoted 3 times

adamsca 3 years, 6 months ago

Correction: I meant to say...Why did you just Apply Audit mode to User3 and not User1 and User2?
upvoted 1 times

Naqsh27 3 years, 6 months ago

I think its because the audit only applies to on Prem Accounts which user 3 is.
It does not apply to the other cloud accounts. But i am not 100% sure.
upvoted 2 times

dzampar 3 years, 6 months ago
yes, right explanation
YES,NO,YES
upvoted 2 times

Patchfox 3 years, 5 months ago
I think it is NO NO YES. Because the documenation say nothing about current password evaluations. Only when the user will change or reset the password the evaluation will happen
upvoted 16 times

Patchfox 3 years, 5 months ago
Update: I tested it in lab. The behaviour is like I said.
upvoted 5 times

rooban 3 years, 4 months ago
1. NO. Password protection does not prompt a user to change the password during logon, it only works during a password change/reset.
2. YES. Policy is in Audit mode so no enforcement.
3. YES. Policy in Audit mode so no enforcement.
upvoted 13 times

Nickname01 2 years, 5 months ago
you are not correct, the audit mode is only for on-prem accounts and not for azure ad accounts. answer should be no no yes

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations
upvoted 1 times

MathiasC 1 year, 7 months ago
agree, N N Y
when "Enable password protection on Windows Server Active Directory" is set to "No", Mode options "Enforced" and "Audit" are greyed out.
upvoted 2 times

Tom_tank Most Recent 4 months, 4 weeks ago
1. User1: No, there's no information about a policy prompting a password change on next sign-in.
2. User2: No, "@da@tum_C0mpleX123" is not allowed because it contains "Adatum," which is on the banned passwords list.
3. User3: No, "Adatum123!" is not allowed for the same reason—it contains "Adatum."
upvoted 2 times

Srirupam 7 months, 2 weeks ago
No-No-Yes
upvoted 2 times

pentium75 11 months ago
NO (policy is only applied during password change)
NO (matches the banned password, audit mode is relevant only for AD)
YES (Audit mode is on for AD)
upvoted 2 times

JaridB 1 year, 2 months ago
Given that the policy is set to Audit mode, the enforcement of the custom banned password list is not active; instead, it will log any occurrences where a banned password would have been used if the policy were in Enforced mode.
1. User1 will be prompted to change the password on the next sign-in.
No. There is no indication that User1 is required to change their password on the next sign-in due to a password policy. Audit mode does not enforce password changes; it only logs events.
2. User2 can change the password to @d@tum_C0mpleX123.
Yes. In Audit mode, User2 would be able to change their password to this since the policy is not actively blocking the use of banned passwords but will log an event stating that this password would have been banned if the policy was in Enforced mode.
3. User3 can change the password to Adatum123.
Yes. Similar to User2, User3 would be able to change their password to Adatum123, and an event would be logged due to the policy being in Audit mode, not Enforced mode.

upvoted 2 times

⊟ **joegie00698** 1 year, 5 months ago

No : user is not changing password AND auditing is on

YES: password has more than 5 points after rules check

YES: same as above

Onprem password protection is also enabled and uses the global and custom lists also.

I assume that the necessairy components are installed on-prem as the option is activated

upvoted 1 times

⊟ **brooklyn510** 1 year, 5 months ago

On exam 1/2/24

upvoted 1 times

⊟ **[Removed]** 1 year, 6 months ago

If set to Enforce, users will be prevented from setting banned passwords and the attempt will be logged. If set to Audit, the attempt will only be logged. this is the explanation of Mode

We recommend that you start deployments in audit mode. Audit mode is the default initial setting, where passwords can continue to be set. Passwords that would be blocked are recorded in the event log. After you deploy the proxy servers and DC agents in audit mode, monitor the impact that the password policy will have on users when the policy is enforced.

During the audit stage, many organizations find that the following situations apply:

They need to improve existing operational processes to use more secure passwords.

Users often use unsecure passwords.

They need to inform users about the upcoming change in security enforcement, possible impact on them, and how to choose more secure passwords.

upvoted 1 times

⊟ **flafernan** 1 year, 6 months ago

N, Y, Y

upvoted 1 times

⊟ **PierreTang** 1 year, 6 months ago

Test on lab. N, N, N

upvoted 2 times

⊟ **TheProfessor** 1 year, 8 months ago

Correct answer. Policy is in Audit mode. It says " If set to Enforce, users will be prevented from setting banned passwords and the attempt will be logged. If set to Audit, the attempt will only be logged."

upvoted 1 times

⊟ **alopezme** 1 year, 9 months ago

YES NO YES

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-faq

Why is Azure AD still rejecting weak passwords even though I've configured the policy to be in Audit mode?

Audit mode is only supported in the on-premises Active Directory environment. Microsoft Entra ID is implicitly always in "enforce" mode when it evaluates passwords.

upvoted 1 times

⊟ **IvanIco** 1 year, 9 months ago

Since Adatum is banned word for password any possible version of it is banned as well so the answer is yes, no, no bcz @d@tum is counted in the banned list

upvoted 1 times

⊟ **TheProfessor** 1 year, 9 months ago

NO, NO, YES

upvoted 2 times

⊟ **MichaelD_NZ** 1 year, 10 months ago

Should be NO, NO, YES.

As per Authentication methods (Password Protection) Blade:

[QUOTE]

If set to Enforce, users will be prevented from setting banned passwords and the attempt will be logged. If set to Audit, the attempt will only be logged.

[END QUOTE]

upvoted 2 times

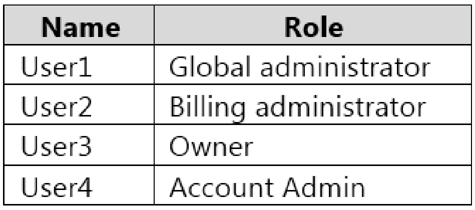
⊟ **Self_Study** 1 year, 10 months ago

On exam 7/8/23. Answers are correct.

upvoted 3 times

HOTSPOT -

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.



Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

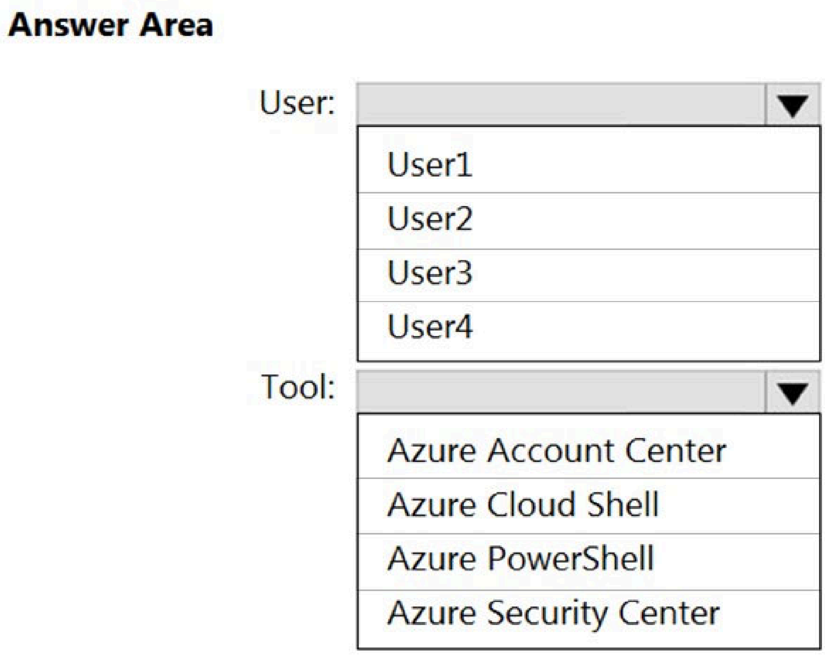
The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

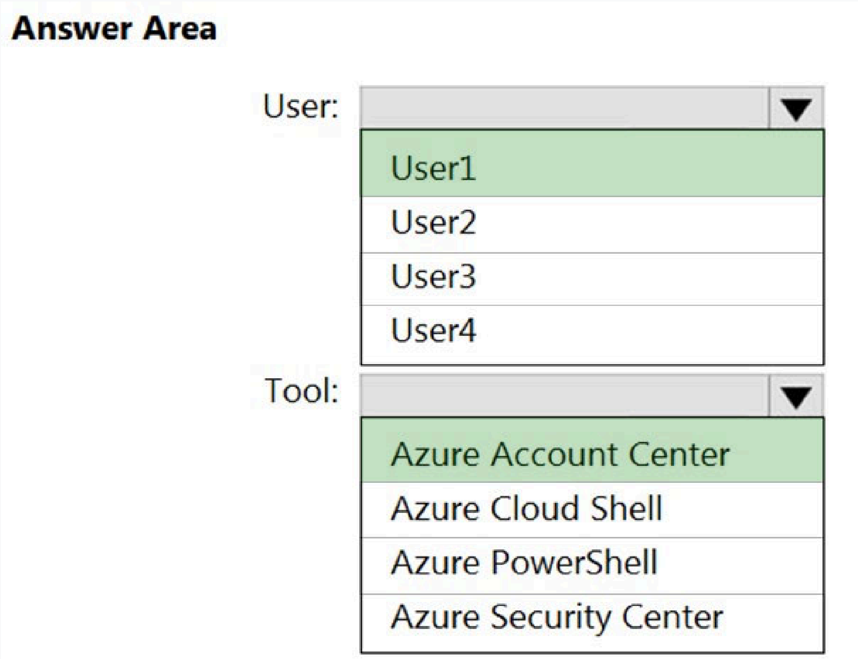


Answer Area

User:
- User1
- User2
- User3
- User4

Tool:
- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

Suggested Answer:



Answer Area

User:
- [✓ User1]
- User2
- User3
- User4

Tool:
- [✓ Azure Account Center]
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

Reference:

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

⊟ **Ikazimirs** Highly Voted 👍 3 years, 8 months ago

Can this be fixed please as this is a repeat question in first place and on the other question you have correct answer "Billing Administrator"

upvoted 104 times

> ⊟ **OpsecDude** 2 years, 9 months ago
>
> By now I think most of us know that only Billing admin can transfer ownership...but still yes: For the sake of those who paid contributor access, do fix this answer!
>
> upvoted 26 times
>
> > ⊟ **Malikusmanrasheed** 2 years, 1 month ago
> >
> > Does contributor access have less number of questions?
> >
> > upvoted 2 times

⊟ **markimsjm** Highly Voted 👍 3 years, 8 months ago

"Only the billing administrator of an account can transfer ownership of a subscription."

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

upvoted 26 times

⊟ **03b48e7** Most Recent ⏲ 1 month, 2 weeks ago

According to microsoft documentation it would be user4 who can transfer ownership.
“Only the account administrator of an account can transfer ownership of a subscription.”
I see that several are putting the Billing Administrator, but maybe that's how it was a while ago.

https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

upvoted 1 times

⊟ **Tom_tank** 4 months, 4 weeks ago

User : User 3
To transfer the ownership of Subscription1 to a new owner, the user who holds the Owner role can perform the transfer. In this case, User3 (U3) has the Owner role and is responsible for transferring ownership.
Tool: Azure Account Center

upvoted 1 times

⊟ **epomatti** 1 year, 6 months ago

I'm not buying exams in this platform anymore.

Maintenance of questions and answers here is garbage.

upvoted 12 times

> ⊟ **rooster90** 10 months, 1 week ago
>
> Hi, I think the same, what other pages you recommend?pls
>
> upvoted 1 times
>
> ⊟ **pentium75** 11 months ago
>
> The discussions are great. The "correct answers" and given explanations are BS.
>
> upvoted 1 times

⊟ **flafernan** 1 year, 6 months ago

1. User2-Billing Administrator
2. Azure Portal (Azure account center)

upvoted 5 times

⊟ **wardy1983** 1 year, 7 months ago

Explanation:
1. User2-Billing Administrator
2. Azure Portal (Azure account center)

upvoted 3 times

⊟ **ITFranz** 1 year, 7 months ago

Only the billing administrator of an account can transfer ownership of a subscription.
https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer
answer = user2

upvoted 1 times

wkm 1 year, 8 months ago

the correct answer "Billing Administrator"

https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

upvoted 1 times

wardy1983 1 year, 8 months ago

Only the billing administrator of an account can transfer ownership of a subscription.

upvoted 1 times

sommyo 1 year, 11 months ago

Correct answer is User 2 - Billing Admin

upvoted 2 times

zellck 2 years, 1 month ago

1. User2
2. Azure Account Center

https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

Only the billing administrator of an account can transfer ownership of a subscription.

upvoted 2 times

majstor86 2 years, 3 months ago

1. User2-Billing Administrator
2. Azure Portal (Azure account center)

upvoted 2 times

hitit 2 years, 5 months ago

I think Billing Administrator is correct.

upvoted 2 times

KTBL909 2 years, 7 months ago

I did contact yesterday the team and asked them to update the test they disagree said it is ok.

upvoted 3 times

aleksey_o 2 years, 7 months ago

Should be User2 - Azure Account Center

upvoted 2 times

somenick 2 years, 9 months ago

1) "Billing Administrator"

2) Azure Portal (as of Oct 2022 Account management has moved to Azure portal)

upvoted 10 times

> **CertShooter** 2 years, 6 months ago
>
> Agreed!
>
> upvoted 1 times

> **koreshio** 2 years, 8 months ago
>
> yes, this would be the correct answer now.
>
> upvoted 1 times

> **mangali84** 2 years, 8 months ago
>
> Hi Somenick , will be writing the examination in November do you care to share the documentation?
>
> upvoted 1 times
>
> > **somenick** 2 years, 8 months ago
> >
> > Just go to https://account.azure.com/Home/Redirect and you'll see the message
> >
> > upvoted 1 times

Question #64 *Topic 2*

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.
You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.
Which role should you assign to the PIM service principle?

A. Contributor

B. User Access Administrator

C. Managed Application Operator

D. Resource Policy Contributor

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Vikku30** Highly Voted 3 years, 5 months ago

The english of question is too confusing to understand. Who writes these questions

upvoted 53 times

⊟ **ITFranz** 3 months ago

In the way the question is written, creates more confusion, no because of the question itself, but the English wording they are using. I think questions must be very clear, and accurate to anyone and clearly explained, to avoid unfortunate situations and be fair with all the students trying to accomplish challenge on this test.

upvoted 1 times

⊟ **Fal991l** Highly Voted 2 years, 7 months ago

whoever figured out the proper answer must be a genius.

upvoted 12 times

⊟ **femzy** 1 year, 7 months ago

I didn't even answer it. My first approach was to come to the comments to see other people's logic towards answering this question.

upvoted 2 times

⊟ **JBAnalyst** Most Recent 6 months, 3 weeks ago

Selected Answer: B

The PIM service principal needs to have that role assigned to the user in order for it to function . The PIM service itself needs the role too

upvoted 2 times

⊟ **8de3321** 7 months ago

Selected Answer: D

This exact same question is in #113 Topic 2 (paid part of this website) and even this website has shown the answer mixed up compared to #63. This is so messed up. Guys if you are purchasing this questions from this website, do not blindly trust the answers. Know that only a few has purchased it and so the votes and discussion is significantly low. The answers are also messed up but you will get many more questions. If you are too good at finding answers yourself or want to prepare so badly then go for it otherwise it is absolutely a waste of money in my opinion.

upvoted 1 times

⊟ **ITFranz** 10 months, 3 weeks ago

The question states, A PIM user that is assigned the User Access Administrator (it already has it assigned).
To support the answer.
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-troubleshoot#access-to-azure-resources-denied
Access to Azure resources denied
Problem
As an active owner or user access administrator for an Azure resource, you are able to see your resource inside Privileged Identity Management but can't perform any actions such as making an eligible assignment or viewing a list of role assignments from the resource overview page. Any of these actions results in an authorization error.

Cause
This problem can happen when the User Access Administrator role for the PIM service principal was accidentally removed from the subscription. For the Privileged Identity Management service to be able to access Azure resources, the MS-PIM service principal should always have the User Access Administrator role role assigned.

upvoted 1 times

1dd60c0 3 months, 3 weeks ago

If it needs assigned why would it be possible to remove it?

upvoted 1 times

ESAJRR 1 year, 9 months ago

Selected Answer: B

B. User Access Administrator

upvoted 2 times

ErikPJordan 1 year, 9 months ago

Weird question.

upvoted 3 times

TheProfessor 1 year, 9 months ago

Selected Answer: B

This question was tricky. But answer B is correct answer.

upvoted 2 times

zellck 2 years, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-troubleshoot#access-to-azure-resources-denied
Assign the User Access Administrator role to the Privileged identity Management service principal name (MS–PIM) at the subscription level. This assignment should allow the Privileged identity Management service to access the Azure resources.

upvoted 7 times

Bentos2004 2 years, 2 months ago

Wow, very tricky

upvoted 1 times

Snaileyes 2 years, 2 months ago

Here's a current reference link: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-troubleshoot#access-to-azure-resources-denied

upvoted 2 times

majstor86 2 years, 3 months ago

B. User Access Administrator

upvoted 2 times

somenick 2 years, 9 months ago

The question is related to this article: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-troubleshoot
However I can not find MS-PIM service principal

upvoted 3 times

BP_lobster 3 years, 3 months ago

Selected Answer: B

Note the question is asking what role we should assign the SERVICE principle. The role mentioned in the question is assigned to a USER.

The question is confusingly worded, but the above distinction helped me answer it.

upvoted 6 times

DanHeg 3 years, 3 months ago

Very confusing to work out what it's asking for, as the answer is in the question but the question suggests it's not enough

upvoted 3 times

Patchfox 3 years, 5 months ago

Selected Answer: B

It's B

upvoted 1 times

⊟ **HananS** 3 years, 6 months ago

https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

The answer seems correct

upvoted 1 times

⊟ **cfsxtuv33** 3 years, 5 months ago

According to the link you provided I agree, the answer is correct.

upvoted 1 times

Question #65 Topic 2

You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role.
You purchase a cloud app named App1 and register App1 in Azure AD.
Admin1 reports that the option to enable token encryption for App1 is unavailable.
You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal.
What should you do?

A. Upload a certificate for App1.

B. Modify the API permissions of App1.

C. Add App1 as an enterprise application.

D. Assign Admin1 the Cloud application administrator role.

Suggested Answer: *C*
This is a tricky one because uploading a certificate is also required. However, the question states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application. When the app is added as an enterprise application, the Token Encryption option will be available.
Then you can upload the certificate.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption

Community vote distribution
A (55%) D (25%) C (20%)

asfgsertweg Highly Voted 3 years, 2 months ago
Don't understand as, if the app has been registered. It is an enterprise app !!!
upvoted 14 times

ConanBarb 2 years, 3 months ago
Yes, but the option is only available in portal for Enterprise Apps created as such from start:

"The Token encryption option is only available for SAML applications that have been set up from the Enterprise applications blade in the Azure portal, either from the Application Gallery or a Non-Gallery app. For other applications, this menu option is disabled."

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption?tabs=azure-portal

For plain App Registratrions you edit the application manifest under Manifest (see the same doc above).
"Set the value for the tokenEncryptionKeyId attribute."
upvoted 9 times

fonte Highly Voted 2 years, 6 months ago
Selected Answer: A
Created an app registration and it automatically appeared in the Enterprise Applications, so I would say the next thing is to configure the token encryption as per:
https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption?tabs=azure-portal
upvoted 8 times

ba1d9fc Most Recent 3 weeks, 4 days ago
Selected Answer: D
This is asking how Admin1 can enable the encryption. Assigning the relevant permission does this.
upvoted 1 times

ca7859c 1 month ago
Selected Answer: A
You will need a certificate

https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/howto-saml-token-encryption?tabs=azure-portal#configure-enterprise-application-saml-token-encryption

upvoted 1 times

cuongdo1793 1 month ago

Selected Answer: C

Final Answer: C. Add App1 as an enterprise application
Once it shows up under Enterprise Applications, Admin1 (as Application Developer) will be able to see the Token Encryption blade and proceed to upload the certificate.

upvoted 1 times

mmmyo 1 month, 3 weeks ago

Selected Answer: A

B. Modify API permissions of App1 – API permissions primarily control access and authorization, but they do not influence token encryption settings.

C. Add App1 as an enterprise application – Enterprise applications represent service principals of the registered app but are not a requirement for enabling token encryption.

D. Assign Admin1 the Cloud application administrator role – This role grants broader control over applications but is not directly tied to token encryption settings.

Since Admin1 needs the ability to enable token encryption, uploading a certificate will allow this functionality to be enabled in the Azure portal.

upvoted 2 times

randy0077 3 months ago

Selected Answer: D

although certificate is required but question is more about if admin1 has permissions: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/howto-saml-token-encryption?tabs=azure-portal#:~:text=SAML%20assertion%20data.-,Prerequisites,owner%20of%20the%20service%20principal,-Configure%20enterprise%20application

upvoted 1 times

stonwall12 4 months, 2 weeks ago

Selected Answer: A

Answer: A, Upload a certificate for App1

Reason: To enable token encryption for an application in Azure AD, you must first upload a certificate that will be used as the encryption key. Without a valid certificate uploaded to the application, the token encryption option remains unavailable, regardless of user permissions.

upvoted 2 times

ITFranz 4 months, 3 weeks ago

Selected Answer: D

To support the answer:
To enable Admin1 to enable token encryption for App1 in the Azure portal, you should assign Admin1 the Cloud Application Administrator role. Here's why:
1. The Application Developer role, which Admin1 currently has, is limited in its permissions. It primarily allows users to create application registrations and manage their own applications.
2. The Cloud Application Administrator role has more extensive permissions for managing enterprise applications, including the ability to manage all aspects of enterprise applications and application registrations.
3. The Cloud Application Administrator role grants the necessary permissions to configure advanced settings like token encryption for applications.
Answer = D

upvoted 1 times

Nhadipour 4 months, 3 weeks ago

Selected Answer: D

While uploading a certificate is a required step for token encryption, Admin1 currently does not have permission to do this. Admin1 needs the correct role to enable token encryption.

The Cloud Application Administrator role grants full control over enterprise applications and app registrations, including the ability to manage certificates and secrets, which is required to enable token encryption.

upvoted 2 times

SofiaLorean 4 months, 3 weeks ago

Selected Answer: D

To enable token encryption for an application in Azure AD, the Cloud Application Administrator or Global Administrator role is required

upvoted 1 times

sgomezsan 5 months ago

Selected Answer: D

To enable token encryption for App1, Admin1 needs to have one of the following roles: Cloud Application Administrator, Application Administrator, or owner of the service principal.
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/howto-saml-token-encryption?tabs=azure-portal

upvoted 1 times

waqqy 5 months, 2 weeks ago

Selected Answer: D

The correct solution is to assign Admin1 the Cloud Application Administrator role (Option D) because it grants the necessary permissions to manage application settings, including enabling token encryption. The other options either address different aspects of application management or do not provide the required permissions.

upvoted 1 times

Andreas_Czech 6 months, 4 weeks ago

Selected Answer: A

as the Microsoft Documentation:

To configure token encryption, you need to upload an X.509 certificate file that contains the public key to the Microsoft Entra application object that represents the application.

Reference-Link:
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/howto-saml-token-encryption?tabs=azure-portal

this points to A,
but ...: One of the following roles: Cloud Application Administrator, Application Administrator, or owner of the service principal.

Reference-Link:
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/howto-saml-token-encryption?tabs=azure-portal#prerequisites

which points to D.
I decided to choose A, but which is correct -> only MS knows

upvoted 1 times

Exam2us 7 months, 1 week ago

Correct answer is "D".
Assign Admin1 the Privileged Role Administrator or Global Administrator role temporarily to allow them to enable token encryption for App1 in the Azure portal. Once the configuration is complete, you can revoke the elevated permissions.

upvoted 1 times

Srirupam 7 months, 2 weeks ago

Correct Answer: A. Upload a certificate for App1
Token encryption in Azure AD requires the application to have a certificate uploaded. This certificate is used to encrypt the tokens issued to the app. Without a certificate uploaded, the option to enable token encryption will not be available in the Azure portal.
B. API permissions are unrelated to enabling token encryption. They are used to define what APIs the app can access.
C. Registering an app and adding it as an enterprise application are separate processes. While this step might be part of integrating an app, it does not affect token encryption settings.
D. The Application developer role already allows Admin1 to manage app registrations. The inability to enable token encryption is not due to permissions but the lack of a certificate uploaded to the application.

upvoted 1 times

codeunit 8 months, 2 weeks ago

To ensure that Admin1 can enable token encryption for App1, you should assign Admin1 either the Application Administrator or the Cloud Application Administrator role. These roles allow the user to manage all aspects of application registration and configuration, including enabling token encryption.

In summary:
* Assign the Application Administrator or Cloud Application Administrator role to Admin1.
* Admin1 will then be able to enable token encryption for App1 in the Azure portal.

upvoted 1 times

Question #66 *Topic 2*

You plan to deploy an app that will modify the properties of Azure Active Directory (Azure AD) users by using Microsoft Graph.
You need to ensure that the app can access Azure AD.
What should you configure first?

A. an app registration

B. an external identity

C. a custom role-based access control (RBAC) role

D. an Azure AD Application Proxy

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

Community vote distribution
A (100%)

o2091 Highly Voted 👍 3 years ago
it seems correct
upvoted 9 times

Patchfox Highly Voted 👍 2 years, 11 months ago
Correct Answer
upvoted 5 times

waqqy Most Recent ⊙ 5 months, 2 weeks ago
Selected Answer: A
Correct Answer
upvoted 1 times

brooklyn510 11 months, 4 weeks ago
On exam 1/2/24
upvoted 4 times

ESAJRR 1 year, 3 months ago
Selected Answer: A
A. an app registration
upvoted 1 times

majstor86 1 year, 10 months ago
Selected Answer: A
A. an app registration
upvoted 2 times

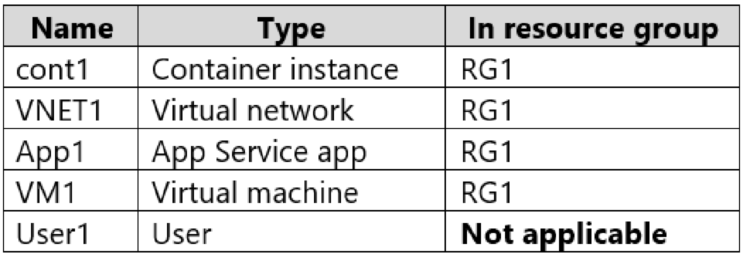
F117A_Stealth 2 years, 1 month ago
Selected Answer: A
App reg
upvoted 2 times

wizardoX 2 years, 11 months ago
Correct, just create a service principal under App Registration
upvoted 4 times

Question #67 *Topic 2*

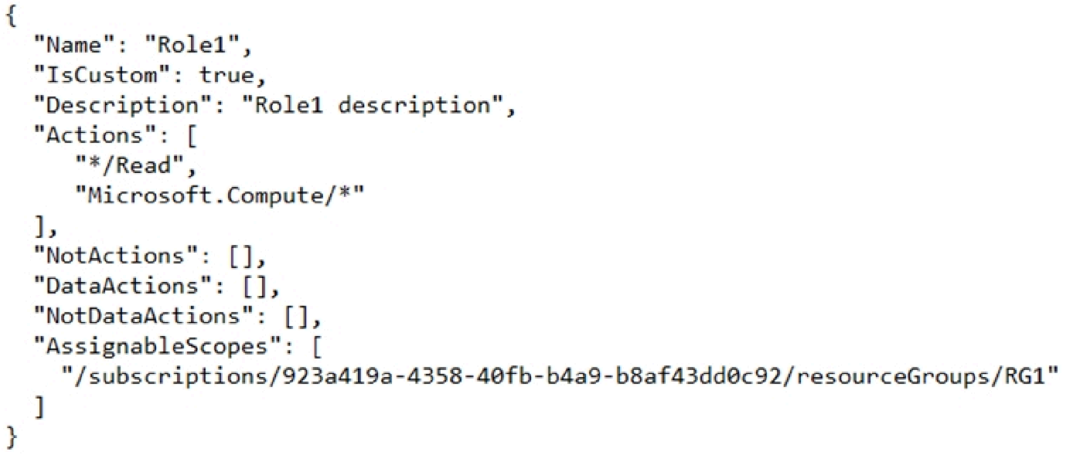
HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.



Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	**Not applicable**

You create a custom RBAC role in Subscription1 by using the following JSON file.



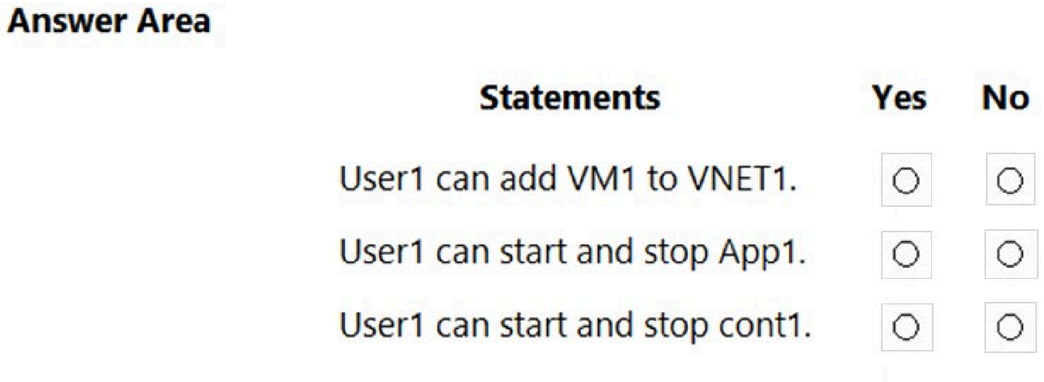
```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
     "*/Read",
     "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

You assign Role1 to User1 on RG1.

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

NOTE: Each correct selection is worth one point.

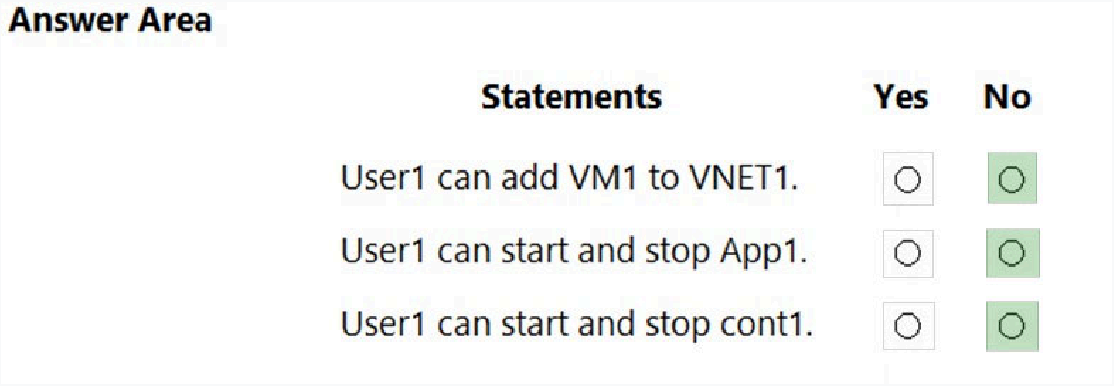
Hot Area:



Answer Area

Statements	Yes	No
User1 can add VM1 to VNET1.	○	○
User1 can start and stop App1.	○	○
User1 can start and stop cont1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can add VM1 to VNET1.	○	[✓ ○]
User1 can start and stop App1.	○	[✓ ○]
User1 can start and stop cont1.	○	[✓ ○]

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute

Eltooth Highly Voted 3 years, 3 months ago

NO NO NO

upvoted 21 times

slimjago 2 years, 6 months ago

what about this? https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#actions

upvoted 2 times

stepman 2 years, 2 months ago

I chose this NNN and this was On exam 4/27 with the new exam experience. No Sim or lab.

upvoted 14 times

wsrudmen Highly Voted 2 years, 8 months ago

It's correct. NO NO NO

*/Read ==> User1 can read anything

Micrososft.Compute/* ==> doesn't provide anything. It will will reference all resourceTypes but without action

Reminder on action format: {Company}.{ProviderName}/{resourceType}/{action}

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions

upvoted 12 times

koreshio 2 years, 8 months ago

no. see this: https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#actions

Microsoft.Compute/* --> "Grants access to all actions for all resource types in the Microsoft.Compute resource provider."

upvoted 5 times

koreshio 2 years, 8 months ago

but overall, its seems: No, No, No. as you've stated:

Permissions on Microsoft.Compute are here:

https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute

upvoted 3 times

SofiaLorean Most Recent 3 months, 3 weeks ago

No, No, No.

upvoted 1 times

codeunit 8 months, 2 weeks ago

User1 can add VM1 to VNET1.

No: Adding a virtual machine to a virtual network requires permissions beyond read access, such as Microsoft.Network/virtualNetworks/*. The custom role only includes Microsoft.Compute/*, which does not cover virtual network modifications.

User1 can start and stop App1.

No: App1 is an App Service app, which is not a Microsoft.Compute resource. Starting and stopping App Services requires permissions on Microsoft.Web resources, which are not included in the role.

User1 can start and stop cont1.

No: cont1 is a Container instance, which falls under Microsoft.ContainerInstance. The custom role does not include permissions for container instances, only Microsoft.Compute/*.

upvoted 7 times

shadad 8 months ago

well done!

what i like on this site is the discussion part only. make understand why right answers is right answers and why wrong is wrong is wrong. we are here not to answer blindly like other sites dumps but to know why. Thank you.

upvoted 3 times

pentium75 11 months ago

No - user does not have any network permissions (= he cannot do anything with VNET1)

No - "Microsoft.Compute" provider is not including app service

No - "Microsoft.Compute" provider is not including containers

upvoted 1 times

danielgil 1 year, 7 months ago

YES, NO, NO

*/read -> Grants access to read actions for all resource types of all Azure resource providers.

Microsoft.Compute/* -> Grants access to all actions for all resource types in the Microsoft.Compute resource provider.

User can create virtual machines because they can perform any action for VMs, and read VNet to attach it to the VM.

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#actions

upvoted 2 times

bob_sez 1 year, 7 months ago

You need additional permission for creating VM cause you have to assign the VM to a subnet and that is not possible without a network specific permission.

upvoted 2 times

xxavimr 1 year, 7 months ago

Ok, it is all NO's because that custom role has a bad format. Action format is {Company}.{ProviderName}/{resourceType}/{action} where action is *, read, write, action or delete. We miss ResorceType or ProviderName.
Tested and it does not allowed to save it

upvoted 4 times

xxavimr 1 year, 7 months ago

I do not get the respond. Adding Microsoft.Compute/*, it is including Microsoft.Compute/virtualMachines/read Get the properties of a virtual machine
Microsoft.Compute/virtualMachines/write Creates a new virtual machine or updates an existing virtual machine
Microsoft.Compute/virtualMachines/delete Deletes the virtual machine
Microsoft.Compute/virtualMachines/start/action

So, we may start and create a new VM

upvoted 3 times

Obama_boy 1 year, 6 months ago

I agree with you, the answer to whether user1 can add VM1 to VNET1 should be YES

upvoted 1 times

[Removed] 1 year, 7 months ago

Tested in the Lab NO NO NO

upvoted 3 times

TheProfessor 1 year, 8 months ago

Why the second option is NO?

Microsoft.Compute/virtualMachines/* Perform all virtual machine actions including create, update, delete, start, restart, and power off virtual machines. Execute scripts on virtual machines.

upvoted 1 times

sadsad 1 year, 8 months ago

*/read allows read access to all resource types across all resource providers in Azure.
Microsoft.Compute/* allows all actions for all resource types specifically within the Microsoft.Compute resource provider.
If a user is assigned this custom role, they will have read access to all resource types across all resource providers (due to */read) and full access (read, write, delete, etc.) to all resource types within the Microsoft.Compute resource provider.

For example, if this user tries to interact with a virtual machine (which is part of the Microsoft.Compute resource provider), they will have full control (create, update, delete, etc.) over that virtual machine because of the second action. For resources in other resource providers, they would only have read access.

upvoted 2 times

sadsad 1 year, 8 months ago

So Yes / Yes /Yes due to Microsoft.Compute/*

upvoted 3 times

ubiquituz 1 year, 7 months ago

the options are not for vms, you can not configure vnet1, start app1 and container1 with ms.compute/*...

upvoted 1 times

ESAJRR 1 year, 9 months ago

It's correct. NO NO NO

upvoted 1 times

BigShot0 1 year, 9 months ago

No - VNET - You need Microsoft.Network/networkInterfaces/*
Yes - Start Machine - That is included in Microsoft.Compute/virtualMachines/*
No - Container - Would be under the Microsoft.ContainerService/*

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

upvoted 7 times

adminpack 1 year, 9 months ago

For the first question, I think this is missing and that;s why it is a NO. Microsoft.Network/networkInterfaces/write Creates a network interface or updates an existing network interface.

upvoted 1 times

ServerBrain 1 year, 11 months ago

No No No, read is only read..

upvoted 1 times

Troublemaker 1 year, 11 months ago

In Exam - 28/7/2023

upvoted 1 times

Malikusmanrasheed 2 years ago

Not sure why everyone is saying user only has read access to VNET1

User 1 is assigned Role 1 on Rg1 which contains VNET1

User 1 has read permission to everything in RG1
User 1 has all access to Microsoft.Compute in RG1 which includes
Microsoft.Compute/virtualMachines/write Creates a new virtual machine or updates an existing virtual machine
Hence
1.Yes

2. No - - > no such permissions are granted.

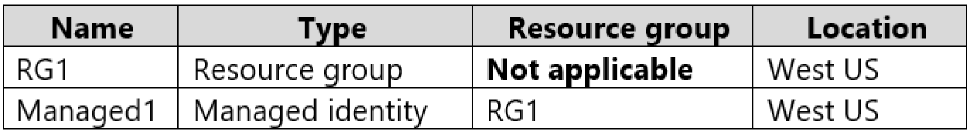
3. No - - > as others have mentioned. Container is a different resource provider, its not a part of Microsoft.Compute.

upvoted 2 times

Question #68 Topic 2

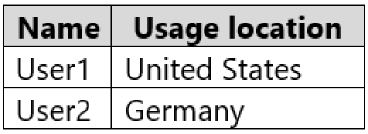
HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.



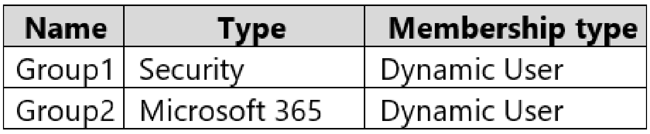
Name	Type	Resource group	Location
RG1	Resource group	**Not applicable**	West US
Managed1	Managed identity	RG1	West US

The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



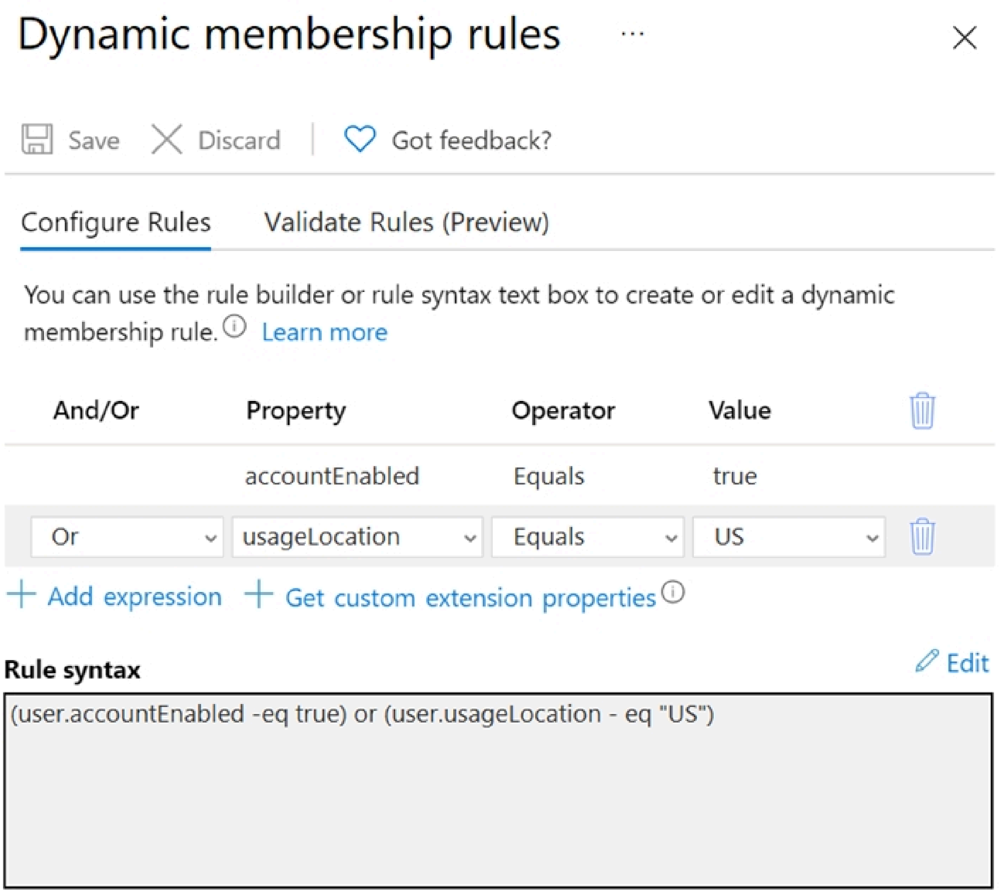
Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.



Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.



Dynamic membership rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

And/Or	Property	Operator	Value
	accountEnabled	Equals	true
Or	usageLocation	Equals	US

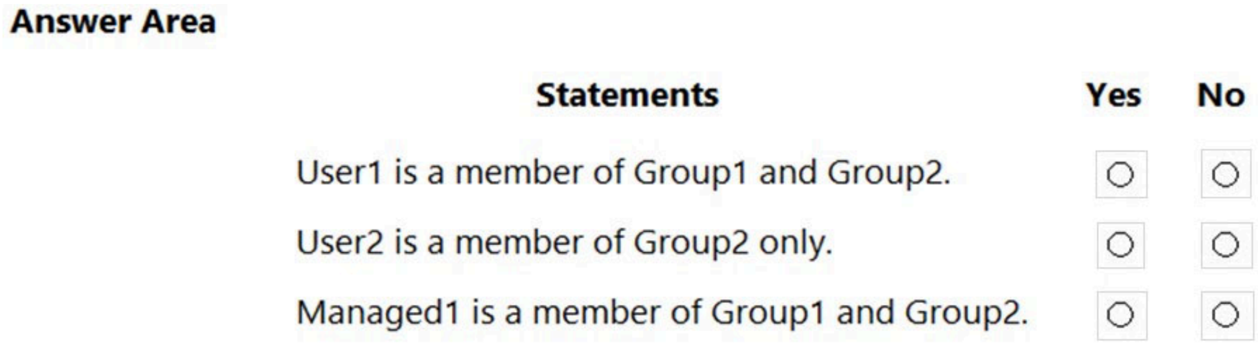
Rule syntax

(user.accountEnabled -eq true) or (user.usageLocation - eq "US")

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

NOTE: Each correct selection is worth one point.

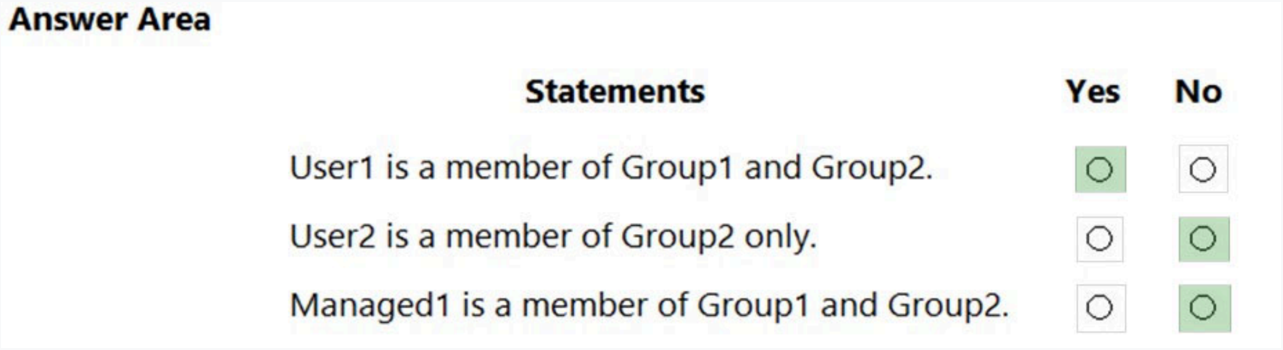
Hot Area:



Answer Area

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 is a member of Group1 and Group2.	[✓ ○]	○
User2 is a member of Group2 only.	○	[✓ ○]
Managed1 is a member of Group1 and Group2.	○	[✓ ○]

Reference:

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

alanew Highly Voted 3 years, 6 months ago

tested, right answer

upvoted 23 times

zellck Highly Voted 2 years, 1 month ago

Gotten this in May 2023 exam.

upvoted 11 times

pentium75 Most Recent 11 months ago

Yes - usageLocation is US

No - we don't know if User2 is enabled, but he's either member of both groups or none

No - Managed Identity not member of M365 groups

upvoted 2 times

bxlin 1 year, 1 month ago

User1 is a member of Group1 and Group2

User2 is a member of Group1 and Group2

upvoted 2 times

Nikeshkj078 1 year, 2 months ago

Y N N

Y - Dynamic Memebership rule will add User1 and user2 to both group as criteria is Account enabled or location is US.

N - Dynamic Memebership rule will add User1 and user2 to both group as criteria is Account enabled or location is US.

N - Additing Managed idenitity to M365 Group i.e. Group 2 is not supported. we can only add managed identity to Group1

upvoted 4 times

Ivan80 1 year, 5 months ago

In exam 1/28/24

upvoted 6 times

Catlyn 1 year, 9 months ago

Got this in Aug 2023 exam

upvoted 6 times

heatfan900 1 year, 10 months ago

Y, N, N

Only USER 1 meets the Rule settings because they are in the U.S.

upvoted 5 times

_fvt 1 year, 11 months ago

Y,N,N, I agree, but what if the last point was just Managed1 being a member of Group1 ?

Will a Service Principal be evaluated by a Dynamic Membership rule and possibly be added (to a Security Group as M365 only supports users) ?

upvoted 1 times

madmax1 2 years ago

where does it state the members of group 2? this question is confusing

upvoted 3 times

⊟ **stepman** 2 years, 2 months ago

I forgot what I chose, but this was On exam 4/27 with the new exam experience. No Sim or lab.

upvoted 3 times

⊟ **majstor86** 2 years, 3 months ago

YES
NO
NO

upvoted 2 times

⊟ **ltjones12** 2 years, 5 months ago

Y, Y, N....accountEnabled = True OR

upvoted 3 times

⊟ **Holii** 2 years, 1 month ago

This would still be Yes/No/No. User2 is a part of Group1 and Group2 the same as User1...
It asks "Group2 only"

upvoted 4 times

⊟ **mung** 2 years, 7 months ago

Nobody knows why Box 3 is no?
I

upvoted 2 times

⊟ **Ajdlfasudfo0** 2 years, 6 months ago

mircosoft 365 groups don't support managed identities

upvoted 22 times

⊟ **Jhill777** 2 years, 7 months ago

YNN
Says "or" not "and". Location means nothing.

upvoted 2 times

⊟ **F117A_Stealth** 2 years, 7 months ago

YNN

Simple

upvoted 1 times

⊟ **Siblark** 2 years, 8 months ago

In Exam Oct-05-2022

upvoted 5 times

Question #69 *Topic 2*

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.
You create a new Azure subscription.
You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription.
You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts.
What should you do fist?

A. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.

B. Configure the Azure AD tenant used by the new subscription to use federated authentication.

C. Change the Azure AD tenant used by the new subscription.

D. Configure a second instance of Azure AD Connect.

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **[Removed]** Highly Voted 👍 3 years, 6 months ago

We need to assign the Subscription on the tenant

upvoted 13 times

⊟ **Sujeeth** Highly Voted 👍 1 year, 9 months ago

C, When you create a new Azure subscription, it is associated with an Azure AD tenant. If the synced on-premises user accounts cannot be assigned roles in the new subscription, it might be because the Azure AD tenant associated with the new subscription is not the same as the one you've been synchronizing with using Azure AD Connect. Changing the Azure AD tenant to match the one you've been synchronizing with will allow you to assign roles to synced user accounts correctly.

upvoted 12 times

⊟ **Nhadipour** Most Recent 🕘 5 months ago

Selected Answer: C

To assign roles to synced on-premises user accounts in the new subscription, the subscription must use the same Azure AD tenant as the one where those accounts exist.
If the synced on-premises user accounts belong to a different Azure AD tenant than the one used by the new subscription, those accounts cannot be assigned roles in the subscription.

upvoted 1 times

⊟ **waqqy** 5 months, 2 weeks ago

Selected Answer: D

Option C: Change the Azure AD tenant used by the new subscription means switching to a different Azure AD tenant. This would not solve the issue because the new tenant would not have the synced on-premises user accounts from your original Azure AD tenant.

The correct approach is to ensure that the new subscription recognizes the synced user accounts from your existing Azure AD tenant. This is achieved by:

Option D: Configure a second instance of Azure AD Connect. This ensures that the new subscription is properly synced with the on-premises Active Directory, allowing the user accounts to be assigned roles.

upvoted 1 times

⊟ **ESAJRR** 1 year, 9 months ago

Selected Answer: C

C. Change the Azure AD tenant used by the new subscription.

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/role-based-access-control/transfer-subscription

upvoted 4 times

majstor86 2 years, 3 months ago

Selected Answer: C

C. Change the Azure AD tenant used by the new subscription.

upvoted 1 times

F117A_Stealth 2 years, 7 months ago

Selected Answer: C

C - Correct

upvoted 1 times

Balamani1 2 years, 8 months ago

Selected Answer: C

Answer is correct

upvoted 1 times

JakeCallham 2 years, 9 months ago

Selected Answer: C

You create a new Azure subscription. Hence you need to assign. These questions something are tricky. Go over every answer and try to backtrack if it triggers an earlier statement.

upvoted 5 times

OpsecDude 2 years, 9 months ago

Yeah, so it should be "Assign" because change implies that you will transfer ownership or something alike.

upvoted 3 times

helenwonderland 2 years, 10 months ago

someone please explain

upvoted 1 times

JakeCallham 2 years, 9 months ago

You create a new Azure subscription. Hence you need to assign. These questions something are tricky. Go over every answer and try to backtrack if it triggers an earlier statement.

upvoted 5 times

CatoFong 2 years, 9 months ago

Jake is correct

upvoted 1 times

ParabJWalia_123 3 years, 2 months ago

I didn't understand this

upvoted 5 times

pentium75 11 months ago

You must link the new Azure subscription to your existing Azure AD tenant.

upvoted 1 times

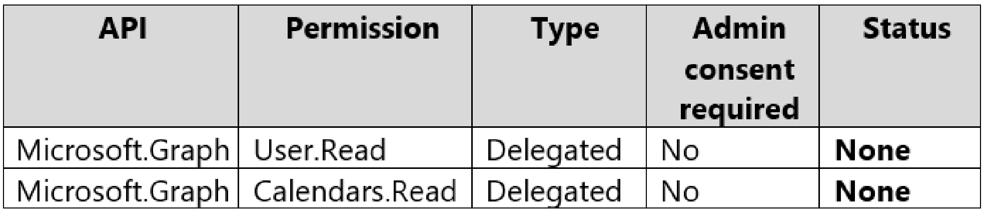
Patchfox 3 years, 5 months ago

Answer is correct

upvoted 4 times

Question #70 Topic 2

You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.



API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	**None**
Microsoft.Graph	Calendars.Read	Delegated	No	**None**

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege.

What should you do?

A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.

B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.

C. Select Grant admin consent.

D. Add new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

Suggested Answer: *A*

Reference:

https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions

Community vote distribution

B (69%) A (31%)

BillBaits Highly Voted 3 years, 6 months ago

Selected Answer: B

Answer: B

The question is about reading and writing ALL user calendars. Delegated permissions only works for the logged in user.

https://docs.microsoft.com/en-us/graph/permissions-reference#application-permissions-8

upvoted 36 times

LeDefatman 3 years, 6 months ago

@BillBaits,

I think you did not fully understand the documentation on this:|

Permission Display String Description Admin Consent Required Microsoft Account supported

Calendars.ReadWrite Have full access to user calendars Allows the app to create, read, update, and delete events in user calendars. No Yes

upvoted 1 times

BayaliJihad 2 years, 2 months ago

@BillBaits, it's says "he solution must use the principle of least privilege". So Delgated permissions is the correct answer

upvoted 2 times

Vikku30 3 years, 5 months ago

Why B. Delegated permissions would be required on user behalf so that basis the scope of permissions the app1 is allowed to schedule the meetings as per user's calendar. Application permission are used by the application native processes , daemons etc. So I don't think so that B is correct option. Option A is correct here.

upvoted 7 times

pentium75 11 months ago

It clearly says that the application must be able to read ALL user calendars. With delegated permission, it can only read the calendars that the user who uses it has access to.

upvoted 1 times

jore041 Highly Voted 2 years, 8 months ago

Selected Answer: A

A appears to be the correct answer here.

Delegated Calendars.ReadWrite ===Have full access to user calendars and it Allows the app to create, read, update, and delete events in user calendars.

Application Calendars.ReadWrite === Read and write calendars in all mailboxes. Allows the app to create, read, update, and delete events of all calendars without a signed-in user.

upvoted 8 times

lili 2 years, 4 months ago

Since it is asking for principle of at least privilege then logically Delegate permission is the right one

upvoted 1 times

Sabr_ Most Recent 2 months, 3 weeks ago

Selected Answer: B

Exam question 6th April 2025

upvoted 1 times

randy0077 3 months ago

Selected Answer: B

B is correct ans: https://learn.microsoft.com/en-us/graph/permissions-reference#application-permissions-8:~:text=Read%20and%20write%20calendars%20in%20all%20mailboxes

upvoted 1 times

shanrajesh 4 months, 2 weeks ago

Selected Answer: B

In Exam 07-Feb-2025

52 Questions (5 Case Studies Questions) No Simulation

95% Questions came from exam topics only Kudos to you guys

upvoted 1 times

fregs 3 months ago

lovely

upvoted 1 times

pentium75 11 months ago

Selected Answer: B

It clearly says that the application must be able to read ALL user calendars. With delegated permission, it can only read the calendars that the user who uses it has access to. Yes, we must follow the principle of least privilege, but delegated permission would give less privilege than required.

upvoted 1 times

workhard 11 months, 2 weeks ago

Selected Answer: B

In order to comply with the principle of least priviledge requirement: "Administrators can configure application access policy to limit app access to specific mailboxes and not to all the mailboxes in the organization, even if the app has been granted the Calendars.ReadWrite application permission." https://learn.microsoft.com/en-us/graph/permissions-reference#calendarsreadwrite

upvoted 2 times

xRiot007 11 months, 2 weeks ago

A - delegated perm to ReadWrite is least privilege. We want only specific users using the app to be able to make appointments.

upvoted 1 times

93b98ea 11 months, 3 weeks ago

Answer: B

Delegated permission would require you granting a user that access as well which is not less priv. If our goal is to let app write/read cal and do it with least priv, we want to only grant the app permission to it and not give it to a user to then delegate.

upvoted 1 times

Dimitrios 1 year, 2 months ago

Delegated permissions: Also called scopes, allow the application to act on behalf of the signed-in user.

Application permissions: Also called app roles, allow the app to access data on its own, without a signed-in user.

upvoted 1 times

Ivan80 1 year, 5 months ago

In exam 1/28/24

upvoted 5 times

cris_exam 1 year, 5 months ago

Ahh, tricky one.

Hmm, after some 20 min reading and some 15 min testing in a lab, I got to the below conclusion.

So, "need to read and change/create events in calendar for ALL users" - the easy way out is to go with the App role (which would be choice B).

Buut, the least privileged access would be to have Delegated role, which would still be able to read/create those calendar events for all users, but it's going to be un-behalf of the user (having the access limitations of the user - if the user should have any) which is more secure - aka least privileged concept.

These 2 articles are covering the topic well:
https://learn.microsoft.com/en-us/graph/auth/auth-concepts#microsoft-graph-permissions

https://learn.microsoft.com/en-us/graph/permissions-overview?tabs=http

Soo, I would go with A here (Delegated role), based on the above reasoning, but take it with a grain of salt, I may be wrong, I hope I'm not cuz that's what I am gonna chose if this question pops up. :D

upvoted 2 times

⊟ **da** 1 year, 5 months ago

answer: A

upvoted 1 times

⊟ **[Removed]** 1 year, 6 months ago

Calendars.ReadWrite

Allows the app to create, read, update, and delete events of all calendars without a signed-in user.

upvoted 1 times

⊟ **[Removed]** 1 year, 6 months ago

This was in application permissions

upvoted 1 times

⊟ **Obama_boy** 1 year, 6 months ago

Selected Answer: B

To ensure that App1 can read all user calendars and create appointments, while adhering to the principle of least privilege, you should:

A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.

This permission allows the application to read and write to user calendars as the signed-in user, without needing more privileged permissions than necessary. Application permissions would grant the app access without a user context and are typically used for background services or daemons, which is not adhering to the principle of least privilege in this context.

upvoted 1 times

⊟ **wardy1983** 1 year, 7 months ago

Answer: B
Explanation:
Answer: BThe question is about reading and writing ALL user calendars. Delegated permissions only works for the logged in user.
https://docs.microsoft.com/en-us/graph/permissions-reference#application-permissions-8
Here you'll find very good explanation about these two types of permissions:https://learn.microsoft.com/en- us/graph/permissions-overview?tabs=http

upvoted 1 times

⊟ **flafernan** 1 year, 7 months ago

Selected Answer: B

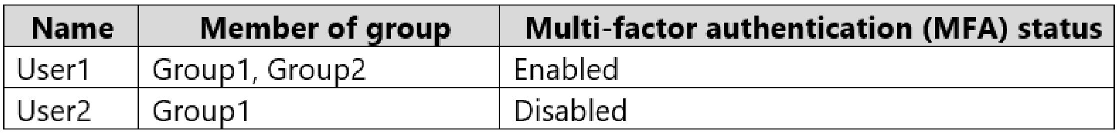
Option (A) "Add a new delegated API permission for Microsoft.Graph Calendars.ReadWrite" does not allow the application to read and write to all users' calendars, which is a requirement of the question, as the delegated permissions apply only to the context of an authenticated user. Therefore, the correct option to satisfy the read and write requirement for all users' calendars is option (B) "Add a new application API permission for Microsoft.Graph Calendars.ReadWrite".

upvoted 2 times

Question #71 Topic 2

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	Member of group	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

✑ Assignments: Include Group1, exclude Group2

✑ Conditions: Sign-in risk level: Low and above

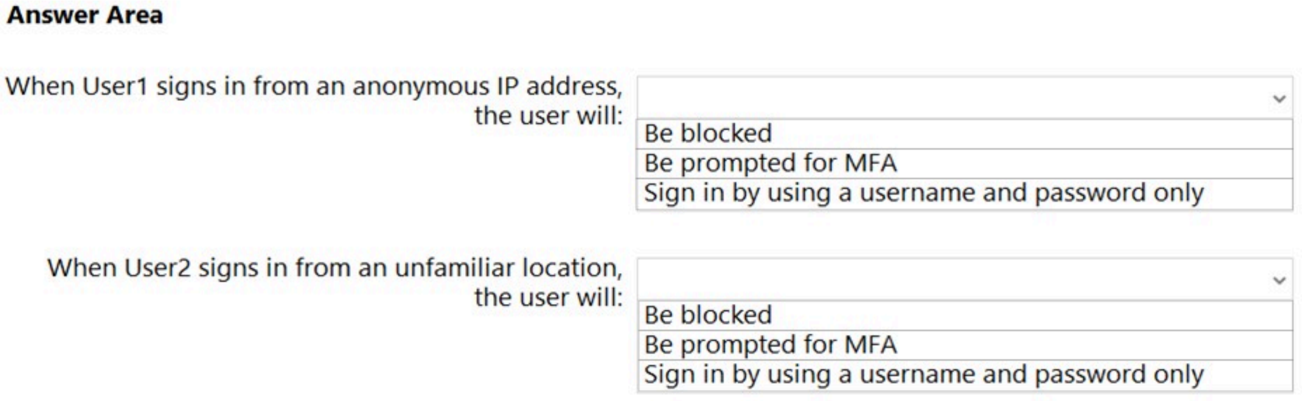
✑ Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

What should you identify for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

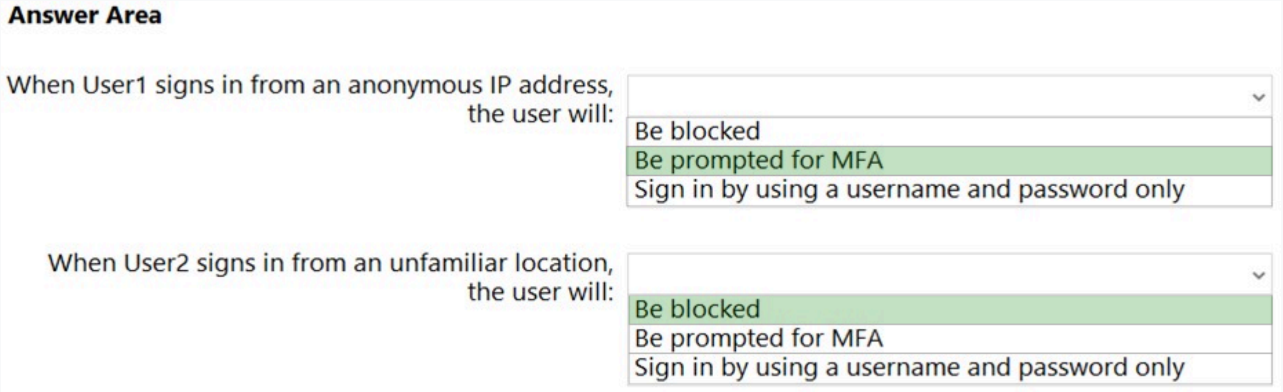
When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

Suggested Answer:



Answer Area

When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- [✓ Be prompted for MFA]
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

Reference:

http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/ https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Pitch09 Highly Voted 3 years, 6 months ago

User1 - is excluded but user1 MFA is Enabled

Exclusion will take precedence. Ans: MFA will be prompted

User2 - is include and user meet the above threshold for sign-in risk level: low and above therefor user account will be blocked.

Note: If you target this policy to a user that hasn't registered for MFA. Their access will be blocked

Ans: Be blocked

upvoted 44 times

luzzo 3 years, 5 months ago

User1 - should be Excluded... MFA is only Enabled and not Enforced

upvoted 5 times

ruscomike 11 months, 3 weeks ago

enabled meand that he/she have to challenge MFA but has not been already configured the mfa method. after that the status become enforced

upvoted 2 times

monob25889 3 years, 6 months ago

User1: Exclusion will take precedence. The MFA will NOT be prompted.

upvoted 7 times

koreshio 2 years, 8 months ago

correct, they should be asked to set up MFA due to 'Enabled' (but not 'Enforced' state), but should be able to log in with username and pass but without MFA

upvoted 6 times

Alster77 1 year, 11 months ago

in exam taken 24 July 2023

upvoted 8 times

basak 1 year, 10 months ago

1. user 1 will be prompted for sign-up MFA (exclusion is applied)

2. user 2 will be applied policy. however, since user2 MFA is disabled hw will not be able login and will be blocked. a user should prior sign-up MFA to act conditional access policy.

upvoted 3 times

Nik9059 Highly Voted 3 years, 6 months ago

I think in both the cases the user will be prompted for MFA

upvoted 23 times

mansc3wth1s 3 years, 4 months ago

MFA Disabled/Enabled on these questions do matter if they are already meeting remediation conditions. They would have to have enforced MFA already by this point.

Because User1 is in Group1 and Group2 the user is then Excluded period. They're free to login with user and pass at this point. MFA is not enabled and no other policy to fallback on that we know of.

upvoted 4 times

[Removed] 3 years, 5 months ago

Wrong as user 2 must register for Azure AD MFA for remediation as its disabled

upvoted 1 times

Nhadipour Most Recent 4 months, 3 weeks ago

User1: "Sign in by using a username and password only."

User2: “Be blocked”

upvoted 1 times

randy0077 3 months ago

You are missing the point here, MFA is already enabled so regardless of policy applies or not MFA will be triggered.

upvoted 2 times

schpeter_091 7 months, 1 week ago

User 1 has to use(setup) an MFA, regardless to his group membership, since MFA is enabled. If MFA was disabled, user wouldn't be blocked because of the exclusion.

upvoted 1 times

shadad 8 months ago

User1 = Excluded Yes but the MFA is enabled and enable mean it will prompt him but he still can skip it setup to use his user name as its not enforced. The question is asking about the prompting MFA then we need to answer that part (enforced will prompt and he must use it).

User 2 = Need to use MFA but its not enabled so he will be blocked.

upvoted 1 times

pentium75 11 months ago

User1 - will be prompted to set up MFA, but can log in without MFA (he is excluded from the policy)

User2 - will be blocked (he has not enrolled in MFA and can't do that during a risky signin)

upvoted 2 times

ivann2010 1 year, 3 months ago

We are talking about "Identity Protection" and not "Conditional Access". Answer for me is: "Sing in by using.....", because MFA is activated, it does not show you the MFA PROMP, it gives you the option to configure it or do it later, if you say do it later you go straight in. Regarding the second, it will force you to configure MFA although it does not change the user's status.

upvoted 3 times

brooklyn510 1 year, 5 months ago

On exam 1/2/24

upvoted 4 times

[Removed] 1 year, 6 months ago

I have tested this in the Lab
When User has MFA enabled it will prompt for MFA
When User has MFA disabled it will still prompt for MFA if the user is required to do MFA.

upvoted 4 times

pentium75 11 months ago

But User2 has not registered for MFA yet. And he can't register it during a risky logon that requires MFA, thus he is blocked.

upvoted 1 times

AZ5002023 1 year, 6 months ago

enabled does not mean enforced
so i think box 1 user name and pass
box 2 : blocked

upvoted 3 times

wardy1983 1 year, 7 months ago

User1 - is excluded but user1 MFA is Enabled
Exclusion will take precedence. Ans: MFA will be prompted
User2 - is include and user meet the above threshold for sign-in risk level: low and above therefor user account will be blocked.
Note: If you target this policy to a user that hasn't registered for MFA. Their access will be blocked
Ans: Be blocked
Reference:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-accesspolicies/
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identityprotection-policies https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/conceptidentity-protection-risks

upvoted 2 times

flafernan 1 year, 7 months ago

If you create a mandatory MFA policy and explicitly exclude USER1 from that policy, but USER1 already has MFA enabled on their account, they will not be affected by the policy. This is because the explicit deletion of the MFA policy should override the policy, allowing USER1 to continue using their multi-factor authentication as usual. The opt-out policy is more specific and will take priority over the MFA mandatory policy. Therefore, USER1 will be able to authenticate without any problems using MFA.

upvoted 1 times

Troublemaker 1 year, 11 months ago

In Exam - 28/7/2023

upvoted 3 times

Hillary_Innocent 2 years ago

user 1 is excluded in this policy since exclude takes precedence. therefore user one will be blocked.

upvoted 1 times

Anarchira 2 years ago

User1, Sign in by using a username and paswword only

Not affected cuz is excluded and :

If a user has MFA configured as enabled but not forced, they are not obligated to configure and use MFA. In this case, the user can choose to sign in using only their username and password without using MFA.

Having MFA enabled but not forced means that users are recommended or encouraged to use MFA to add an additional layer of security to their account, but they are not required to do so. Users have the option to configure and use MFA if they wish, but it is not imposed as a mandatory requirement.

User2, be blocked cuz is affected and dont have mfa

upvoted 5 times

zellck 2 years, 1 month ago

1. Be prompted for MFA
2. Be blocked

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#risk-remediation
Users must register for Azure AD MFA before they face a situation requiring remediation. Users not registered are blocked and require administrator intervention.

upvoted 2 times

Alexbz 2 years, 2 months ago

Both will be promoted for MFA. If MFA is disabled for a user and an access policy force it for login user with MFA disabled status won't be blocked, they will be prompted to set the MFA upon login.

upvoted 3 times

Question #72 *Topic 2*

HOTSPOT -

You have an Azure subscription that contains an Azure SQL database named SQL1.

You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

✑ Provide App1 with access to SQL1 without storing a password.

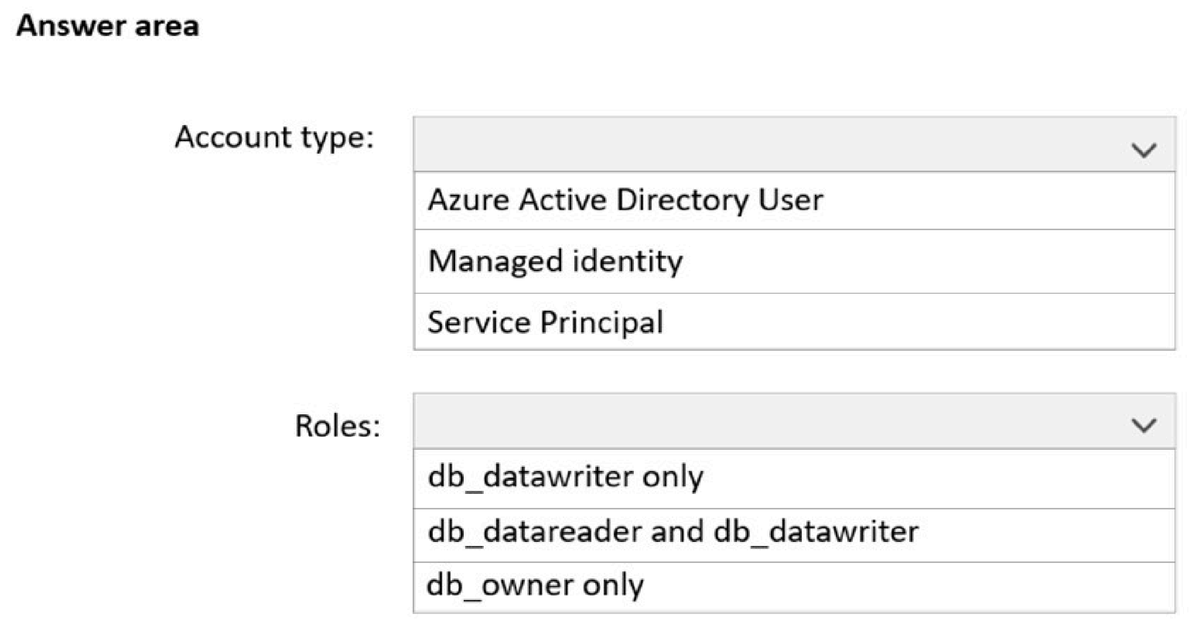
✑ Use the principle of least privilege.

✑ Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

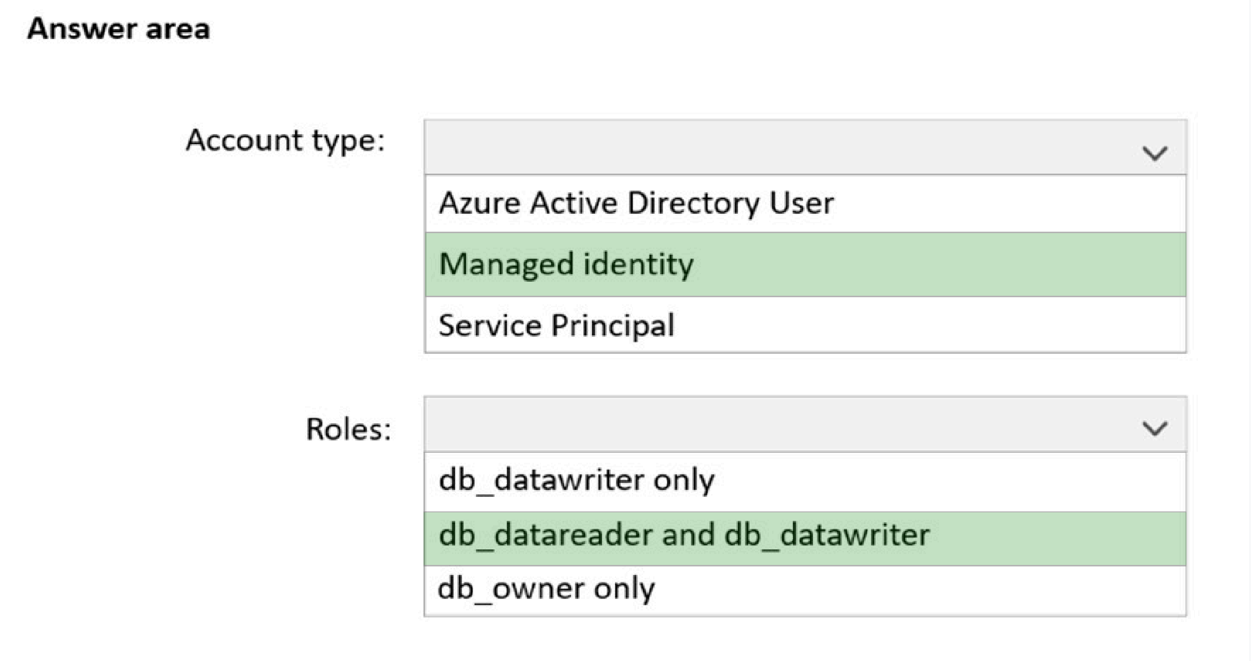


Answer area

Account type:
- Azure Active Directory User
- Managed identity
- Service Principal

Roles:
- db_datawriter only
- db_datareader and db_datawriter
- db_owner only

Suggested Answer:



Answer area

Account type:
- Azure Active Directory User
- [✓ Managed identity]
- Service Principal

Roles:
- db_datawriter only
- [✓ db_datareader and db_datawriter]
- db_owner only

Reference:

https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet

⊟ zellck Highly Voted 2 years, 1 month ago

1. Managed identity
2. db_datareader and db_datawriter

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview
A common challenge for developers is the management of secrets, credentials, certificates, and keys used to secure communication between services. Managed identities eliminate the need for developers to manage these credentials.

While developers can securely store the secrets in Azure Key Vault, services need a way to access Azure Key Vault. Managed identities provide an automatically managed identity in Azure Active Directory (Azure AD) for applications to use when connecting to resources that support Azure AD authentication. Applications can use managed identities to obtain Azure AD tokens without having to manage any credentials.
upvoted 16 times

zellck 2 years, 1 month ago
https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver16#fixed-database-roles
- db_datawriter
Members of the db_datawriter fixed database role can add, delete, or change data in all user tables. In most use cases this role will be combined with db_datareader membership to allow reading the data that is to be modified.
- db_datareader
Members of the db_datareader fixed database role can read all data from all user tables and views. User objects can exist in any schema except sys and INFORMATION_SCHEMA.
upvoted 5 times

flafernan Highly Voted 1 year, 7 months ago
You can use a Service Principal to grant an application access to Azure resources, including SQL databases. However, when granting read and write access to a SQL database, it is generally safer to use Managed Identities when the application is running on a virtual machine or an Azure service. Managed Identities are an easier and more secure way to grant access to Azure resources because they don't require you to manually manage secrets or credentials.

Service Principals are typically used when you need to grant access to external applications or services that are not hosted in Azure. When it comes to internal Azure applications and services, Managed Identities are a more direct and secure option. Therefore, using a Managed Identity would be the most appropriate option to meet the criteria of not storing passwords, using the principle of least privilege, and minimizing administrative effort in the context of internal Azure resources.
upvoted 12 times

Sabr_ Most Recent 2 months, 3 weeks ago
Exam question 6th April 2025
upvoted 1 times

subrat10 1 year ago
The answer of question 1 should be "Service principal" as the question explicitly says Minimize administrative effort.
upvoted 2 times

xRiot007 11 months, 2 weeks ago
FYI, managed identity is a type of service principal used when we don't want to pass credentials around, so question 1 is MI.
upvoted 3 times

brooklyn510 1 year, 5 months ago
On exam 1/2/24
upvoted 7 times

Troublemaker 1 year, 11 months ago
In Exam - 28/7/2023
upvoted 8 times

Johnvic 2 years, 2 months ago
Exam.6 case studies. 3 true/false questions. 47 multiple questions and no simulations. Alot of new questions thats not up here
upvoted 2 times

icebw22 2 years, 3 months ago
Correct, Managed identity because db need to see who is the request coming from.
Managed identity = identity for the app
upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

Account Type = Managed Identity

Roles = db_datareader and db_datawriter

upvoted 2 times

⊟ **sofieejo** 2 years, 5 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 3 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

Members of the db_datawriter fixed database role can add, delete, or change data in all user tables. In most use cases this role will be combined with db_datareader membership to allow reading the data that is to be modified.

https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver16

upvoted 1 times

⊟ **F117A_Stealth** 2 years, 7 months ago

Correct!

Account Type = Managed Identity

Roles = db_datareader and db_datawriter

upvoted 2 times

⊟ **Kelly8023** 2 years, 8 months ago

Correct answers

upvoted 1 times

⊟ **Siblark** 2 years, 8 months ago

In Exam Oct 05, 2022

upvoted 2 times

⊟ **Amit3** 2 years, 9 months ago

# In EXAM - 01-Oct-2022

upvoted 2 times

⊟ **Mic8888** 3 years, 2 months ago

correct answers

upvoted 2 times

Question #73 *Topic 2*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

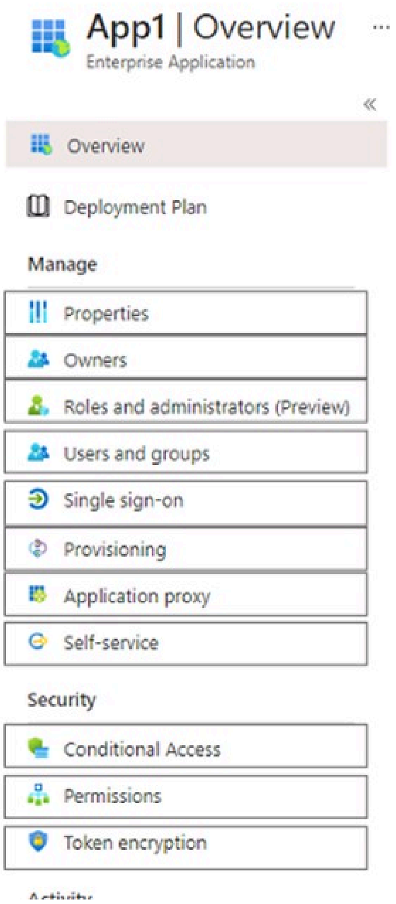
You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

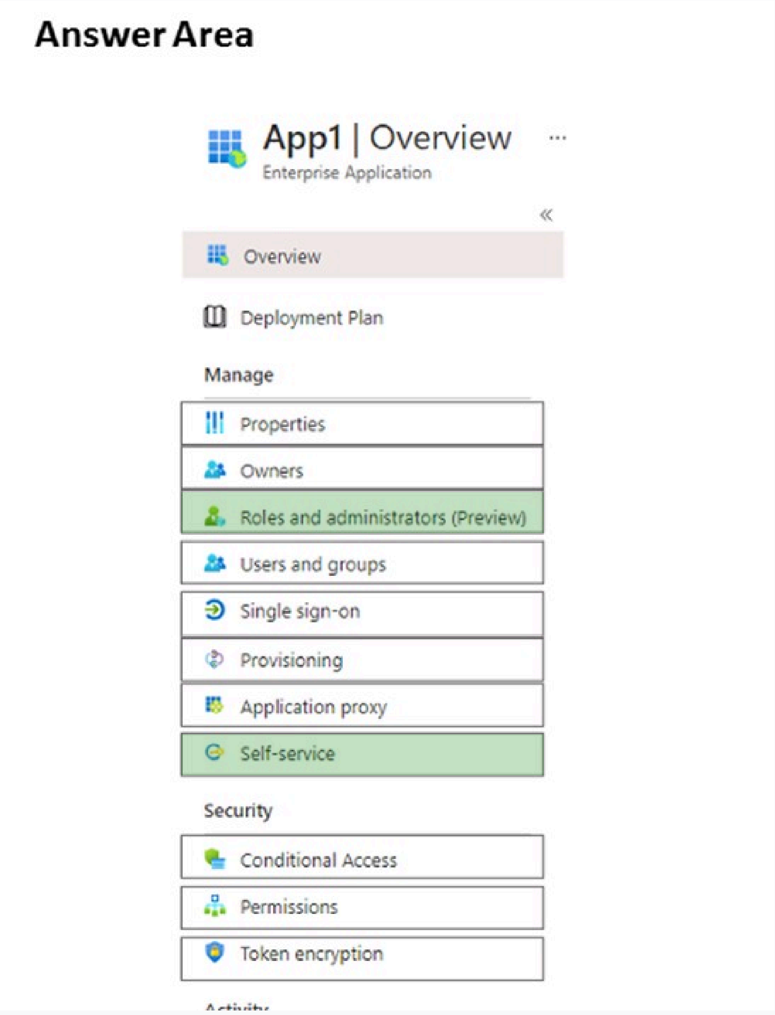
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Suggested Answer:



Answer Area

App1 | Overview ···

Enterprise Application

Box 1: Roles and administrators -

Here you will find Role1 and be able to assign User1 to the role.

Box 2: Self Service -

Under Self Service, there is an option to ג€Allow users to request access to this applicationג€.

ParabJWalia_123 Highly Voted 3 years, 2 months ago

Answer is wrong

I tried it manually on a lab, Roles and Administrators is limited only to a few builtin AD roles

I think the answer should be

1. Users and Groups for User1
2. Self-service for User2

upvoted 39 times

[Removed] 1 year, 6 months ago

This is the correct answer

upvoted 1 times

ITFranz 10 months, 3 weeks ago

Do you have the steps a link to support it?

I found this.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/custom-enterprise-apps#create-a-new-custom-role

Assign the role to a user using the Microsoft Entra admin center

Sign in to the Microsoft Entra admin center as at least a Privileged Role Administrator.

Browse to Identity > Roles & admins > Roles & admins.

Select the Manage user and group assignments role.

upvoted 1 times

Ajdlfasudfo0 2 years, 6 months ago

correct

upvoted 2 times

⊟ **OpsecDude** 2 years, 9 months ago

You are right, I took the bother of creating a custom App Role and all I could do with it is assign it to a group (already added to the app) from Users and Groups

upvoted 4 times

⊟ **geuser** Highly Voted 2 years, 9 months ago

The selected answers are correct. You can create a custom App Role (if you have appropriate licensing) and add it via Roles and Administrators.
https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps#create-a-new-custom-role

upvoted 12 times

⊟ **somenick** 2 years, 9 months ago

Agree. Tested in the lab. You can assign a role to the user via Roles and Administrators

upvoted 4 times

⊟ **Sinemorec2024** Most Recent 2 months, 1 week ago

On exam 07.04.2025

upvoted 1 times

⊟ **walcv** 4 months, 1 week ago

To grant Role1 to User1, you assign them that role in the app’s Users and groups blade.
To allow User2 to request access, you enable and configure the app’s Self-service settings.

upvoted 1 times

⊟ **schpeter_091** 7 months, 1 week ago

I checked it in an app, what is under users and groups. I can select a user, but under "select a role" I can only see 'default access'. How can I add a custom role then? (Default access option cannot be mofified)

upvoted 1 times

⊟ **codeunit** 8 months, 2 weeks ago

To assign Role1 to User1 and enable User2 to request access to App1, you need to modify the following settings in the App1 enterprise application configuration:

Roles and Administrators:
This setting is where you can assign Role1 to User1. Navigate to the "Roles and Administrators" section and assign the specific app role (Role1) to User1.

Self-service:
This setting allows you to enable User2 to request access to the application. By configuring self-service settings, you can enable users to request access to App1 directly from the Azure AD portal.

upvoted 1 times

⊟ **pentium75** 11 months ago

"An app-specific role" is created in under "App roles" the app registration. Users are assigned their app roles under "Users and Groups".

Thus: Users and Groups, and Self-service.

upvoted 1 times

⊟ **bob_sez** 1 year, 7 months ago

If the custom role is created in Azure Entra, you can assign that role from Roles and Administrators blade.
If the custom role is created in Azure, you cannot see that role in Roles and Admin and hence cannot assign it.
The question doesnt explicitly mention where the role is created, but since the question is explicitly mentioning that we have Azure AD, its assumed that they are talking acount the role created in Azure AD and not Azure.
With this understanding, I would think the given answers are correct.

upvoted 5 times

⊟ **pentium75** 11 months ago

It is neither an Entra role nor an Azure role, it is "an app-specific role" created in the app registration. Users are assigned their roles under "Users and Groups".

upvoted 1 times

⊟ **TheProfessor** 1 year, 8 months ago

Given answer are correct since the question mentioned about custom role. However, in order to add custom role, P1 or P2 license is required. Below from the Azure dashboard -

"To create custom roles, your organization needs Microsoft Entra ID Premium P1 or P2".

upvoted 1 times

pentium75 11 months ago

This is about about Azure AD roles, we have "an app-specific role" created in the app registration.

upvoted 1 times

wardy1983 1 year, 8 months ago

Box 1:users and groups

Box 2: Self Service -

Under Self Service, there is an option to Allow users to request access to this application.

upvoted 1 times

zellck 2 years, 1 month ago

1. Roles and administrators
2. Self-service

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access#enable-self-service-application-access-to-allow-users-to-find-their-own-applications

Self-service application access is a great way to allow users to self-discover applications, and optionally allow the business group to approve access to those applications. For password single-sign on applications, you can also allow the business group to manage the credentials assigned to those users from their own My Apps portal.

upvoted 2 times

xRiot007 11 months, 2 weeks ago

The question is poorly worded. "App-specific role" means nothing. It is not clear if the custom role is an AD (Entra) role and an RBAC role.

upvoted 1 times

pentium75 11 months ago

It IS clear. It is "an app-specific role" created under "App roles" in the app registration. NOT an Azure AD role, NOT an RBAC role.

upvoted 1 times

majstor86 2 years, 3 months ago

Roles and administrators-assign Role1 to User1

Self service-enable User2 to request access to App1

upvoted 2 times

JohnBentass 2 years, 6 months ago

1. Users and Groups for User1
2. Self-service for User2

upvoted 1 times

F117A_Stealth 2 years, 7 months ago

The selected answers are correct.

upvoted 1 times

Kelly8023 2 years, 8 months ago

Vote for users and groups for #1 since Roles and Administrators section still in preview [As shown in screenshot]

upvoted 1 times

AzureJobsTillRetire 2 years, 5 months ago

It is not in preview anymore.

upvoted 1 times

CatoFong 2 years, 9 months ago

Agreed with Parab.

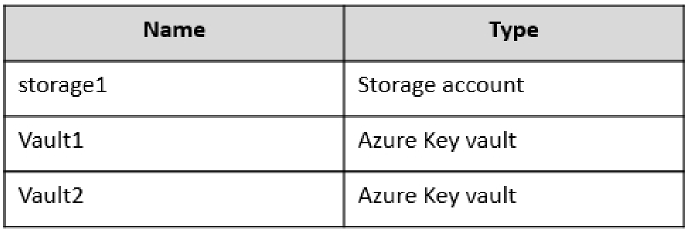
User 1 - Users and Groups

User 2 - Self-service

upvoted 2 times

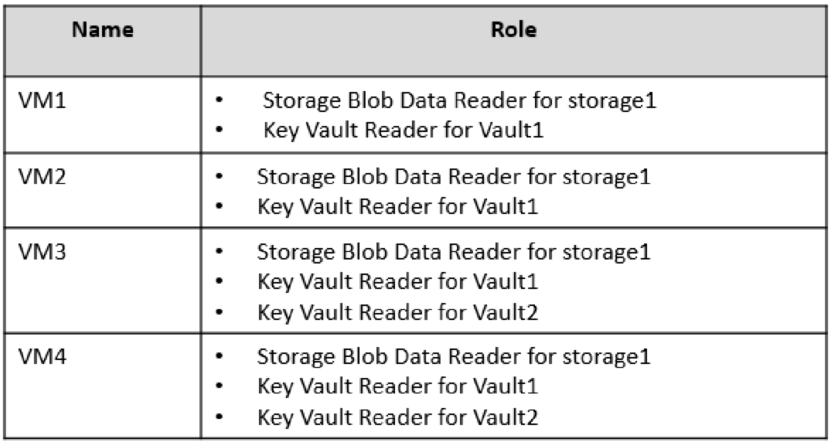
Question #74 *Topic 2*

You have an Azure subscription that contains the resources shown in the following table.



Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.



Name	Role
VM1	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM2	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM3	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2
VM4	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

✑ Assign each virtual machine the required roles.

✑ Use the principle of least privilege.

What is the minimum number of managed identities required?

A. 1

B. 2

C. 3

D. 4

Suggested Answer: *B*

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Community vote distribution

B (86%) 14%

ltjones12 Highly Voted 2 years ago

If it's a system assigned managed id, it can only be tied to one resource. If you use a user assigned managed ID, it can be tied to multiple resources. Since there are 2 separate policies required, you can assign a user assigned managed ID for each policies. B is correct

upvoted 11 times

matt3p3 Most Recent 11 months, 3 weeks ago

Selected Answer: B

definitely B

upvoted 1 times

flafernan 1 year ago

Selected Answer: B

B - An Azure Managed Identity can be associated with resources including virtual machines, Azure functions, etc. Therefore, it is possible to have a single Managed Identity linked to multiple virtual machines or other resources within Azure.

upvoted 2 times

JunetGoyal 1 year, 2 months ago

4, Managed Identity can tie to on resource only

upvoted 1 times

heatfan900 1 year, 4 months ago

YOU CREATE ONE USER-ASSIGNED MI FOR VM 1 AND VM 2 AND ANOTHER FOR VM 3 AND VM4. THIS WAY VM 1 AND VM2 DO NOT HAVE ACCESS KEY VAULT 2.

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#managed-identity-types
- User-assigned.
You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more Azure Resources.

upvoted 2 times

icebw22 1 year, 9 months ago

Correct, only two needed

VM1 and VM2, same permission, and vm3 and vm4 same as well therefore only need 2

upvoted 1 times

majstor86 1 year, 10 months ago

Selected Answer: B

B. 2 managed identities

upvoted 1 times

F117A_Stealth 2 years, 1 month ago

Selected Answer: B

Just 2 is required.

upvoted 3 times

Te2ya 2 years, 2 months ago

As this table explained, Managed ID can not be shared multiple resources. So 4 Managed ID should be the answer

upvoted 2 times

> **arseyam** 2 years, 2 months ago
>
> You really need to read about manager identities again.
>
> upvoted 5 times
>
> **Ajdlfasudfo0** 2 years ago
>
> Satz mit X, das war wohl nix
>
> upvoted 1 times

wsrudmen 2 years, 2 months ago

Selected Answer: B

Correct

upvoted 1 times

somenick 2 years, 2 months ago

Selected Answer: B

Pre-create 2 MIs with required permissions and then assign a user-assigned managed identity to existing VMs.

upvoted 1 times

domtopics 2 years, 3 months ago

Selected Answer: B

Two are needed.

upvoted 1 times

queenbea 2 years, 3 months ago

I belive the answer is 2

upvoted 1 times

Amit3 2 years, 3 months ago

Given Answer is correct

upvoted 1 times

JakeCallham 2 years, 3 months ago

Selected Answer: A

I disagree. I could create one managed identity and use that for both settings. I would not do it in real world, but it's possible. We dont need two MI, In keayvult you can add a MI for a specific role and also use that same MI for a role in storage account. So answer is wrong imho.

upvoted 2 times

JakeCallham 2 years, 3 months ago

i take it back, its two indeed, if you add one, it would automatically have acces to the others. Answer is correct

upvoted 5 times

Armanas 2 years, 3 months ago

Which Answer is correctt? Your answer or Exam Topics??

upvoted 1 times

JakeCallham 2 years, 3 months ago

Exam topic, the answer of 2 is correct.

upvoted 2 times

You_can_call_me_X 2 years, 3 months ago

exam topics answer

upvoted 1 times

Henry56351 2 years, 8 months ago

Correct ans

upvoted 2 times

Question #75 *Topic 2*

SIMULATION -

You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group.

The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

1. Sign in to the Azure portal.
2. Browse to Resource Groups.
3. Select the RG1lod12345678 resource group.
4. Select Access control (IAM).
5. Select Add > role assignment.
6. Select Virtual Machine Contributor (you can filter the list of available roles by typing 'virtual' in the search box) then click Next.
7. Select the +Select members option and select user2-12345678 then click the Select button.
8. Click the Review + assign button twice.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current

gbx077 Highly Voted 1 year, 9 months ago

# Exam Question March 24, 2023

upvoted 11 times

twinkl 1 year, 9 months ago

Any lab?

upvoted 4 times

Drummer Most Recent 6 months, 4 weeks ago

Correct Answer:

See the explanation below.

1. Sign in to the Azure portal.
2. Browse to Resource Groups.
3. Select the RG1lod12345678 resource group.
4. Select Access control (IAM).
5. Select Add > role assignment.
6. Select Virtual Machine Contributor (you can filter the list of available roles by typing 'virtual' in the search box) then click Next.
7. Select the +Select members option and select user2-12345678 then click the Select button.
8. Click the Review + assign button twice.

upvoted 3 times

ErikPJordan 1 year, 3 months ago

tested in lab?? This is a lab question

upvoted 1 times

Paruns 1 year, 8 months ago

Did you get lab questions in March 24 2023 exam

upvoted 2 times

F117A_Stealth 2 years, 1 month ago

correct - tested

upvoted 1 times

Kelly8023 2 years, 2 months ago

correct solution

upvoted 1 times

somenick 2 years, 2 months ago

Correct solution

upvoted 1 times

⊟ **Amit3** 2 years, 3 months ago

Given solution is correct, tested in Lab.

upvoted 1 times

Question #76 *Topic 2*

SIMULATION -

You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com. The new directory must contain a new user named user1@12345678.onmicrosoft.com.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

The first step is to create the Azure Active Directory tenant.

1. Sign in to the Azure portal.
2. From the Azure portal menu, select Azure Active Directory.
3. On the overview page, select Manage tenants.
4. Select +Create.
5. On the Basics tab, select Azure Active Directory.
6. Select Next: Configuration to move on to the Configuration tab.
7. For Organization name, enter 12345678.
8. For the Initial domain name, enter 12345678.
9. Leave the Country/Region as the default.

The next step is to create the user.

1. From the Azure portal menu, select Azure Active Directory.
2. Select Users then select New user.
3. Enter User1 in the User name and Name fields.
4. Leave the default option of Auto-generate password.
5. Click the Create button.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

gbx077 Highly Voted 👍 9 months, 1 week ago

# Exam Question March 24, 2023

upvoted 7 times

Prii02 Most Recent 9 months, 2 weeks ago

we have stimulation questions in examination? am taking this saturday

upvoted 1 times

ltjones12 1 year ago

Should the "initial domain name" be onmicrosoft.com instead of 12345678?

upvoted 2 times

F117A_Stealth 1 year, 1 month ago

Correct - Tested

upvoted 1 times

Kelly8023 1 year, 2 months ago

Tested in lab, correct solution

upvoted 2 times

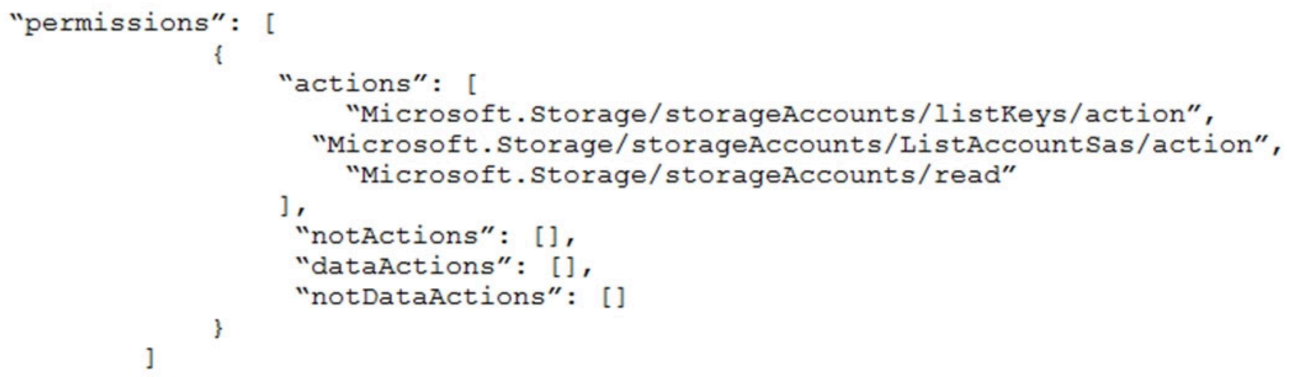
Question #77 *Topic 2*

HOTSPOT -

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.

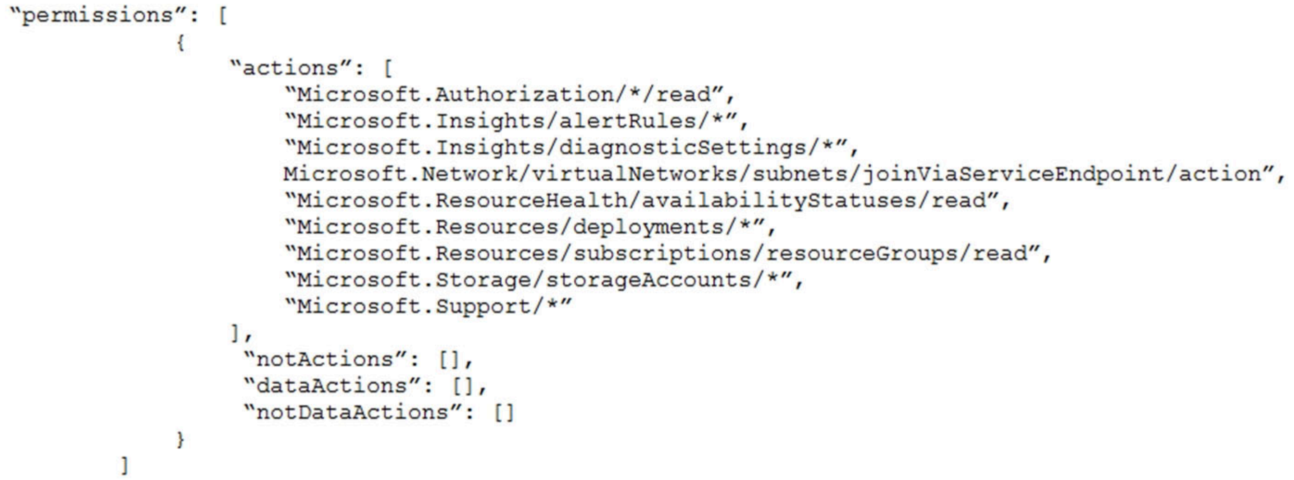
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.



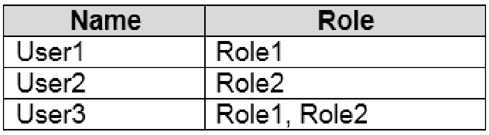
```
“permissions”: [
            {
                “actions”: [
                    “Microsoft.Storage/storageAccounts/listKeys/action”,
                  “Microsoft.Storage/storageAccounts/ListAccountSas/action”,
                    “Microsoft.Storage/storageAccounts/read”
                ],
                 “notActions”: [],
                 “dataActions”: [],
                 “notDataActions”: []
            }
        ]
```

The permissions for Role2 are shown in the following JSON code.



```
“permissions”: [
            {
                “actions”: [
                    “Microsoft.Authorization/*/read”,
                    “Microsoft.Insights/alertRules/*”,
                    “Microsoft.Insights/diagnosticSettings/*”,
                    Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action”,
                    “Microsoft.ResourceHealth/availabilityStatuses/read”,
                    “Microsoft.Resources/deployments/*”,
                    “Microsoft.Resources/subscriptions/resourceGroups/read”,
                    “Microsoft.Storage/storageAccounts/*”,
                    “Microsoft.Support/*”
                ],
                 “notActions”: [],
                 “dataActions”: [],
                 “notDataActions”: []
            }
        ]
```

You assign the roles to the users shown in the following table.

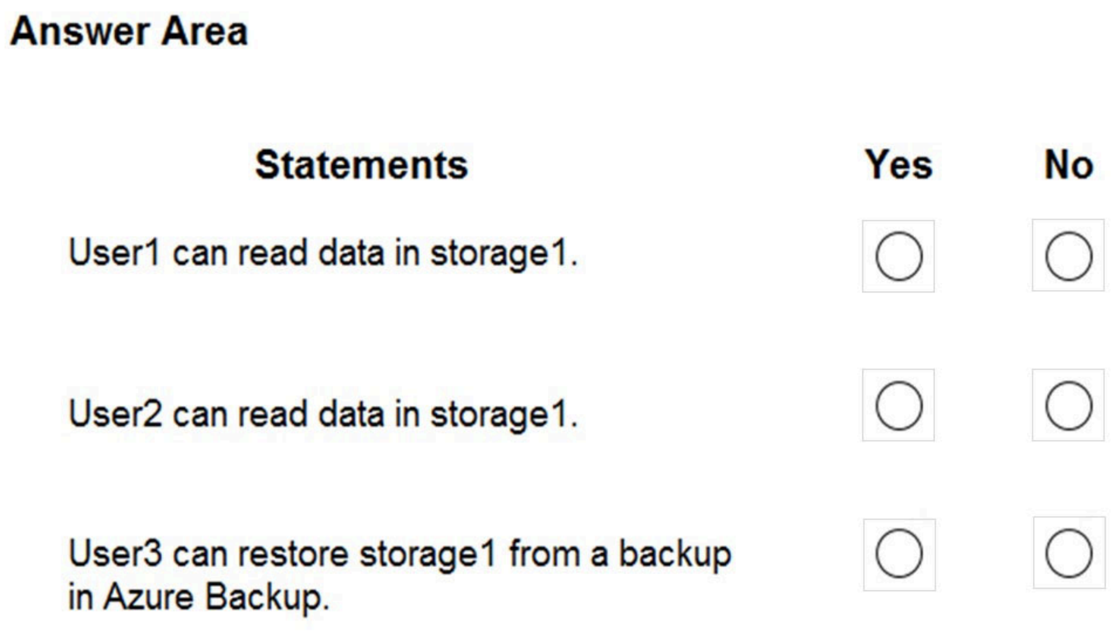


Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

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

NOTE: Each correct selection is worth one point.

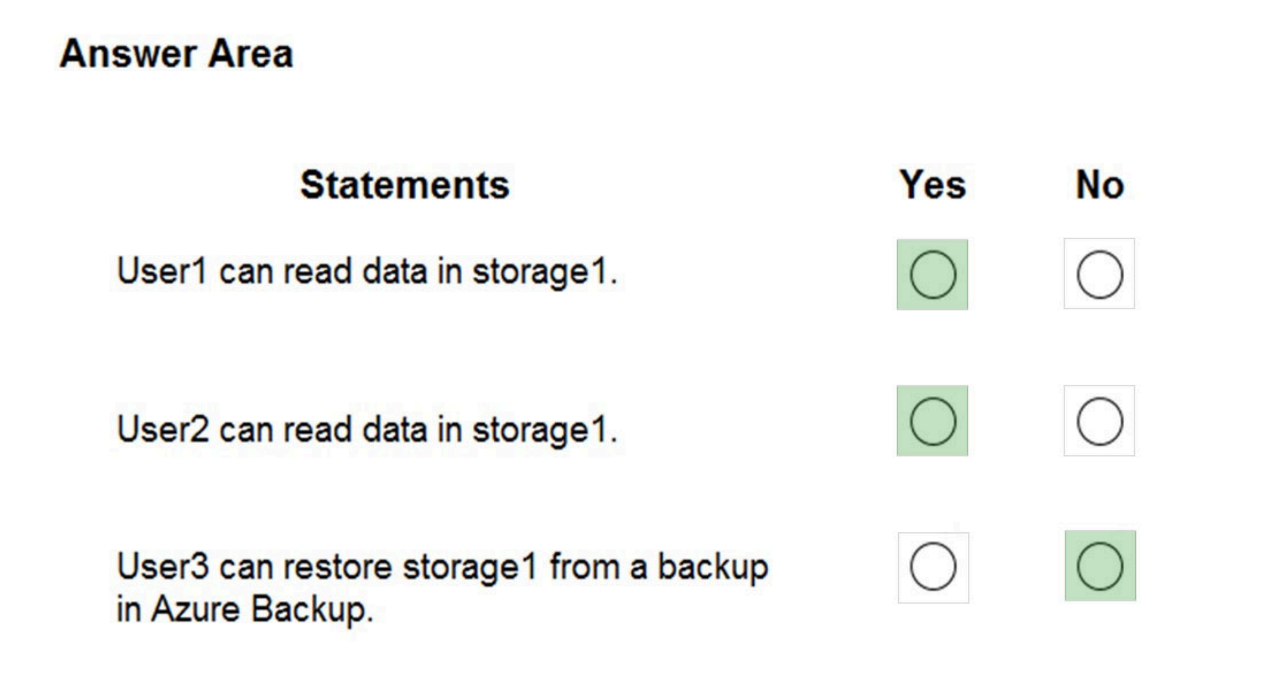
Hot Area:



Answer Area

Statements	Yes	No
User1 can read data in storage1.	○	○
User2 can read data in storage1.	○	○
User3 can restore storage1 from a backup in Azure Backup.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can read data in storage1.	[✓ ○]	○
User2 can read data in storage1.	[✓ ○]	○
User3 can restore storage1 from a backup in Azure Backup.	○	[✓ ○]

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

damtrx Highly Voted 2 years, 10 months ago

User 1 can't read the Storage because Microsoft.Storage/storageAccounts/read will allow him just to LIST the storage accounts

User 2 HAS the option to do whatever he want on the storage account so he can read the data.

User 3 can't access Azure backup because the provider is not enabled in the Access Policy

upvoted 34 times

Hot_156 3 months, 3 weeks ago

LAB!!!

N - User1 cannot read data

Y - User2 can see the container and File shares tabs and open the files.

N/Y - I was not able to test this but based on the perms and Gemini, this is possible

upvoted 2 times

jorgesoma 1 year ago

Correct. NYN

upvoted 1 times

juandmi 2 years, 5 months ago

No - No - No

because User 2 has no dataActions defined, so he cannot read any data

upvoted 11 times

juandmi 2 years, 5 months ago

I need to correct myself. No - No - Yes

User 3 is able to perform restores with Microsoft.Storage/storageAccounts/*

upvoted 6 times

juandmi 2 years, 5 months ago

I'm correcting myself again. data access with Key and SAS will work for user1 and user2.

And I think Microsoft.RecoveryServices/ is not needed for user3 https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-account-backup-contributor

So: YES - YES -YES

upvoted 5 times

chikorita 2 years, 4 months ago

bro, take a break, have a coffee, then comment

please dont confuse other :(

upvoted 63 times

saturation97 2 years, 2 months ago

Definitely take a break but please....NO coffee.

upvoted 22 times

damtrx 2 years, 10 months ago

Correction. User 3 has the option to do restore :

Microsoft.Storage/storageAccounts/restoreBlobRanges/action - Restore blob ranges to the state of the specified time

upvoted 8 times

Ga__ium Highly Voted 👍 2 years, 9 months ago

I assume that "dataactions" is not set, so data cannot be read.

upvoted 25 times

Jimmy500 1 year ago

Correct , all should has been

no,no,no

upvoted 1 times

orcnylmz 2 years, 8 months ago

Agreed. I think No - No - No

https://learn.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access?tabs=portal

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-blob-data-reader

upvoted 5 times

koreshio 2 years, 8 months ago

yup, without "datactions" allowed, they should not be able to read blob data. The roles specify "actions" only which are control-plane actions and not data-plane actions.

upvoted 6 times

ca7859c Most Recent ⊙ 1 month ago

NYN

User1 Permission:

Microsoft.Storage/storageAccounts/read

Returns the list of storage accounts or gets the properties for the specified storage account. (list of storage accounts/properties, not actual data. Storage Data reader at least is needed)

User2 /* (full permissions)

User3 doesn't jave the permissions for backup
Microsoft.RecoveryServices/Vaults/backupJobs/*
upvoted 1 times

randy0077 3 months ago
NNN no data action to read storage data.
upvoted 1 times

Hot_156 4 months, 2 weeks ago
actions vs. dataActions - Revisited (and Corrected):

actions: Control plane. Managing the resource itself (create, delete, modify settings, list keys). Microsoft.Storage/storageAccounts/read lets you see that a storage account exists and view its properties, but NOT its contents.
dataActions: Data plane. Accessing the data within the resource (blobs, queues, tables, files). You need dataActions to read the actual data (blobs, files, etc.) within a storage account.
Role1: Has no dataActions. User1 can see the storage account exists and list its keys, but cannot read any blob, file, queue, or table data.

Role2: Has Microsoft.Storage/storageAccounts/* under actions. This is a broad control plane permission. It allows User2 to manage the storage account (change settings, etc.), and see it exist. Crucially, Role2 lacks any dataActions permissions. So it CANNOT read data.

User3: Inherits the permissions of both roles. Still has no permissions in the dataActions.
upvoted 3 times

schpeter_091 7 months, 1 week ago
Microsoft.Storage/storageAccounts/* : Create and manage storage accounts
Microsoft.Storage/storageAccounts/read: Returns the list of storage accounts or gets the properties for the specified storage account.
to read blobs' data user should have: 'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read' --> Return a blob or a list of blobs.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage
upvoted 1 times

codeunit 8 months, 2 weeks ago
User1 can read data in storage1.
Yes: User1 is assigned Role1, which allows Microsoft.Storage/storageAccounts/read, granting read access to storage account metadata but not to blobs/files themselves directly.

User2 can read data in storage1.
Yes: User2 is assigned Role2, which has Microsoft.Storage/storageAccounts/* permissions, providing access to read data within the storage account, including blobs and files.

User3 can restore storage1 from a backup in Azure Backup.
No: Neither Role1 nor Role2 provide permissions to restore storage accounts from Azure Backup, as there are no permissions related to Azure Backup specifically.
upvoted 2 times

xRiot007 11 months, 2 weeks ago
I really hate these question. User1 can read data. What exactly is DATA? If we are talking about storage account properties, sure, he can read that. If we are talking about blobs and files, he can't.
upvoted 2 times

RaphaelG 1 year, 1 month ago
I'm going through the storage account documentation and there is an interesting piece of information "If a role includes Microsoft.Storage/storageAccounts/listKeys/action, then a user to whom that role is assigned can access data in the storage account [...]".
Therefore, to me, it actually is:
1. Yes (explicit)
2. Yes (via Microsoft.Storage/storageAccounts/*)
3. No (no backup permissions)
upvoted 1 times

xRiot007 11 months, 2 weeks ago
I saw that phrasing too and it's confusing the F out of me. Microsoft should define their roles better because this thing literally looks like a hack.
upvoted 1 times

az2022 1 year, 1 month ago

No, Yes, No

upvoted 1 times

kevgen33091 1 year, 1 month ago

Y-Y-N

The answer is correct. The description of role 2 is 'Storage Account Contributor' which cannot play backup restore action.

Storage Account Contributor: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#storage-account-contributor
Storage Account Backup Contributor: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage#storage-account-backup-contributor

upvoted 1 times

chema77 9 months ago

Y-Y-Y imho.

Restoring both managed and unmanaged disks will work with Storage Account Contributor permissions

https://learn.microsoft.com/en-us/azure/backup/backup-rbac-rs-vault

upvoted 1 times

bob_sez 1 year, 7 months ago

Role1 has more than just read, it also has ListAccountSas/Action and ListKeys/Action which allows read/write access to data within the storage account:
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader-and-data-access

Dont just get hung up on just the read permission in that role.

upvoted 2 times

xxavimr 1 year, 7 months ago

The respond is correct surprisingly. The role 1 is a built-in role called "Reader and Data Access".
https://www.azadvertizer.net/azrolesadvertizer/c12c1c16-33a1-487b-954d-41c89c60f349.html

With Microsoft.Storage/storageAccounts/ListAccountSas/action permission, you may get SAS and do read/write operations.
If you see this link, https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles and look for "Reader and Data Access" role, you see its definition.

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.

The second box is also yes as it has an asterisk for storageaccount

YES, YES, NO

upvoted 2 times

wardy1983 1 year, 7 months ago

Explanation:
USER 1 = Microsoft.Storage/storageAccounts/read= Returns the list of storage accounts or gets the
properties for the specified storage account
user 2 = wildcards (*) so YES
user 3= not defined Microsoft.Storage/storageAccounts/restoreBlobRanges/action

upvoted 3 times

wardy1983 1 year, 7 months ago

Explanation:
USER 1 = Microsoft.Storage/storageAccounts/read= Returns the list of storage accounts or gets the properties for the specified storage account
user 2 = wildcards (*) so YES
user 3= not defined Microsoft.Storage/storageAccounts/restoreBlobRanges/action

upvoted 1 times

flafernan 1 year, 7 months ago

The "Microsoft.Storage/storageAccounts/*/" attribute in a role assignment applies to Azure Storage and provides access to all containers and blobs within all storage accounts in the specified scope.
However, it does not provide access to, for example, Azure Backup and does not automatically grant the ability to restore backups from Azure Backup. To grant permissions to restore backups from Azure Backup, you must meet the correct role in the specific scope. Be careful not to get confused.
upvoted 1 times

TheProfessor 1 year, 8 months ago
Why User 3 can not restore a back up even having the permission Microsoft.Storage/storageAccounts/*

This is the permission of built-in "storage-account-backup-contributor" role.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#storage-account-backup-contributor
upvoted 2 times

Question #78 *Topic 2*

You have an Azure subscription that contains a storage account named storage1 and two web apps named app1 and app2.
Both apps will write data to storage1.
You need to ensure that each app can read only the data that it has written.
What should you do?

A. Provide each app with a system-assigned identity and configure storage1 to use Azure AD User account authentication.

B. Provide each app with a separate Storage account key and configure the app to send the key with each request.

C. Provide each app with a user-managed identity and configure storage1 to use Azure AD User account authentication.

D. Provide each app with a unique Base64-encoded AES-256 encryption key and configure the app to send the key with each request.

Suggested Answer: *C*
A user-assigned identity is a standalone Azure resource that can be assigned to your app. An app can have multiple user-assigned identities.
Incorrect:
Not A: A system-assigned identity is tied to your application and is deleted if your app is deleted. An app can only have one system-assigned identity.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity

Community vote distribution
D (49%) A (24%) C (22%) 6%

MattM70 Highly Voted 👍 2 years, 10 months ago
I think the answer is D. Can make use of "Encryption Scopes".
https://docs.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview
upvoted 13 times

flafernan Highly Voted 👍 1 year, 7 months ago
Selected Answer: C
The question can be seen as having two complementary answers. Answer C (provide each application with a managed identity and configure storage1 to use Azure AD authentication) is the essential part of the solution to ensure that each application can securely authenticate itself and access data. However, answer D (giving each application an encryption key) is also an important part of the solution because encryption helps ensure that only the application that wrote the data can read it.

Therefore, both answers C and D are complementary and together form a comprehensive solution to meet the requirements of the question. Microsoft's official answer seems to focus more on the managed identity part (answer C), but the community also highlights the importance of encryption (answer D), which is valid for ensuring data security.
upvoted 10 times

mmmyo Most Recent 🕘 1 month, 3 weeks ago
Selected Answer: C
✅ User-assigned managed identities allow explicit role-based access control (RBAC) for each app. ✅ Using Azure AD authentication for Storage1 enables fine-grained permissions, ensuring each app can read only its own data. ✅ Managed identities prevent the need to store credentials in the app and ensure secure authentication.
upvoted 1 times

westlifeteki 2 months, 3 weeks ago
Selected Answer: D
The question means app1 can just read app1's data in storage1, and do not read app2's data in storage1. Also app2. So if use mamaged id , that can read data of both app.
upvoted 1 times

golitech 4 months, 4 weeks ago
Selected Answer: A
Explanation: Azure AD authentication with system-assigned identities enables you to manage access without storing credentials. You can assign appropriate roles to each app's managed identity to control access to resources like storage accounts.
Correct approach: This is the best option. By using system-assigned identities, you can grant each app permissions to access only its own data in the

storage account using Azure RBAC (Role-Based Access Control). You would assign each app access to its data in the storage account based on the identity of the app.

This approach allows each app to access only the data it wrote to the storage account, leveraging Azure AD authentication with system-assigned identities.

upvoted 3 times

waqqy 5 months ago

Selected Answer: C

While encryption keys (Option D) are critical for protecting data, they do not address access control or the specific requirement that apps can only access their own data. Therefore, Option C is the correct and practical solution.

upvoted 1 times

codeunit 8 months, 2 weeks ago

By using system-assigned identities, each app (app1 and app2) will have its own identity in Azure AD.

You can then configure RBAC on storage1 to grant each app specific permissions on the data it has written.

Azure AD User account authentication allows you to precisely control access to storage resources, which ensures that app1 can only access its own data, and the same for app2.

The other options are not ideal for this requirement:
B. Using separate storage account keys does not provide isolation at the data level within the same storage account.
C. User-managed identities are an alternative, but system-assigned identities are more streamlined for individual resources as they automatically manage lifecycle and permissions.
D. Base64-encoded AES-256 encryption keys are related to encryption, not to access control and isolation of data per app.

upvoted 1 times

rahmatellah 10 months, 2 weeks ago

Selected Answer: A

i choose the answer A, it's more safer than C, and chatgpt/copilot also choose the answer A

upvoted 3 times

Pavel019846457 10 months, 4 weeks ago

Selected Answer: A

Answer by Copilot and I can agree with it. System-managed identity is the preferable way.
"To ensure that each app can read only the data it has written to the storage account, you should:

A. Provide each app with a system-assigned identity and configure storage1 to use Azure AD User account authentication.

This approach leverages Azure AD for authentication and authorization, allowing you to set up role-based access control (RBAC) policies that restrict each app's access to only its own data. System-assigned identities are managed by Azure, making it easier to handle credentials securely."

upvoted 3 times

Jimmy500 1 year ago

I think user and system assigned managed identities can be used question more likely asking about encryption scopes which is possible with option D, technically A and C also work and they are same and both can be used in this scope but question does not say will both application use same blob to write data or not , if it will use same blob then with system assigned and user assigned managed identities will be useless because let's say both app1 and app2 write data into blob1 which is inside storage1 , if we use managed identity then when will grant access to identity it will automatically have access both data which is inside this is not going to work . In this scenario and even separate blob scenario we can use encryption scope which will allow apps read data that it is written by specific app.

upvoted 1 times

Pamban 1 year, 1 month ago

Selected Answer: D

Answer is D.. below is the explanation

Clients making requests against Azure Blob storage can provide an AES-256 encryption key to encrypt that blob on a write operation. Subsequent requests to read or write to the blob must include the same key. Including the encryption key on the request provides granular control over encryption settings for Blob storage operations. Customer-provided keys can be stored in Azure Key Vault or in another key store.

https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-customer-provided-keys

upvoted 2 times

emartiy 1 year, 2 months ago

Selected Answer: D

based on the question, both apps can reach same StorageAccount with may full permissions (read-write). Let them only read data they written is giving them Base64-encoded AES-256 encryption key. So, App1 can't read App2's created files without correct Base64-encoded AES-256 encryption key.

I also asked this to copilot and AI corrected itself after my feedback :)

"You are correct! I apologize for the oversight. The option to provide each app with a unique Base64-encoded AES-256 encryption key indeed aligns with the goal of ensuring that each app can read only the data it has written to storage1. By using unique encryption keys, you can achieve fine-grained control over data access, allowing each app to access only its own data within the storage account. Thank you for pointing that out! "

upvoted 2 times

mrt007 1 year, 3 months ago

The correct answer is C. Provide each app with a user-managed identity and configure storage1 to use Azure AD User account authentication.

Azure Active Directory (Azure AD) authentication is a mechanism of connecting to Azure Storage by using identities defined in Azure AD. It allows you to use a user-managed identity for your apps, which provides a managed identity for Azure resources. By assigning a managed identity to your apps, you can authenticate to any service that supports Azure AD authentication without having any credentials in your code.

upvoted 1 times

wingcheuk 1 year, 5 months ago

Selected Answer: C

Why many people here voted D? Encrypt the data never used for to control the access right. C makes more sense as we can use RBAC (with user's MI) to grant the required access.

upvoted 2 times

xRiot007 11 months, 2 weeks ago

This is not control plane, it's data plane.

Inside the same storage, on the same blob container, 2 apps write, but each app can only read the content it has written itself.

upvoted 1 times

wardy1983 1 year, 7 months ago

Answer: D

Explanation:

https://docs.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview

"Encryption scopess enable you to manage encryption with a key that is scoped to a container or an individual blob. You can use encryption scopes to create secure boundaries between data that resides in the same storage account but belongs to different customers."

upvoted 2 times

TheProfessor 1 year, 9 months ago

Selected Answer: D

Encryption scopes enable you to manage encryption with a key that is scoped to a container or an individual blob. You can use encryption scopes to create secure boundaries between data that resides in the same storage account but belongs to different customers.

upvoted 2 times

alfaAzure 1 year, 10 months ago

Selected Answer: B

Letter B.

Option B is the correct approach to ensure that each app can read only the data it has written to the storage account. By providing each app with a separate Storage account key and configuring the app to send the key with each request, you're essentially implementing per-app authentication and authorization for accessing the storage account.

upvoted 2 times

Question #79 *Topic 2*

You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1.

User1 attempts to access share1 from a Windows 10 device by using SMB.

Which type of token will Azure Files use to authorize the request?

A. OAuth 2.0

B. JSON Web Token (JWT)

C. SAML

D. Kerberos

Suggested Answer: *D*

Azure Filesג€‰supports identity-based authentication over Server Message Block (SMB) throughג€‰two types of Domain Services: on-premises Active Directory Domain

Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Supported scenarios and restrictions include:

Supports Kerberos authentication with AD with AES 256 encryption (recommended) and RC4-HMAC.

Note: Kerberos is an authentication protocol that is used to verify the identity of a user or host.

Reference:

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable

Community vote distribution

D (100%)

Self_Study Highly Voted 1 year, 4 months ago

Selected Answer: D

On exam 7/8/23. Answers are correct.

upvoted 6 times

Forex19 Most Recent 1 month, 3 weeks ago

Selected Answer: D

# 09/may/2025

upvoted 1 times

brooklyn510 11 months, 4 weeks ago

On exam 1/2/24

upvoted 3 times

shako 11 months, 2 weeks ago

ARE THERE LABS ?

upvoted 1 times

Obama_boy 1 year ago

in exam 08/12/23

upvoted 2 times

tweleve 1 year, 2 months ago

in exam 13 Oct

upvoted 4 times

zellck 1 year, 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#azure-ad-kerberos-for-hybrid-identities

upvoted 3 times

majstor86 1 year, 10 months ago

Selected Answer: D

D. Kerberos

upvoted 2 times

salmantarik 1 year, 12 months ago

Selected Answer: D

D is correct

upvoted 1 times

F117A_Stealth 2 years, 1 month ago

Selected Answer: D

Kerberos

upvoted 1 times

wshamroukh 2 years, 1 month ago

Selected Answer: D

answer d

upvoted 1 times

lahl 2 years, 2 months ago

In exam 31st Oct 2022

upvoted 1 times

Amit3 2 years, 3 months ago

# In EXAM - 01-Oct-2022

upvoted 4 times

Kelly8023 2 years, 3 months ago

Answer is correct

upvoted 3 times

Question #80 Topic 2

DRAG DROP

-

You have an Azure subscription.

You plan to create two custom roles named Role1 and Role2.

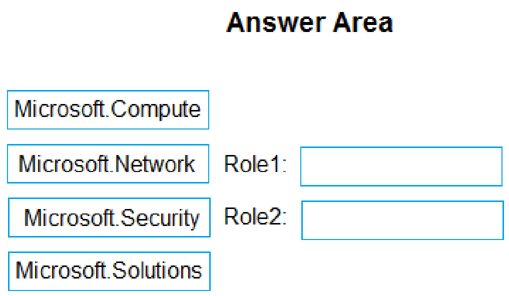
The custom roles will be used to perform the following tasks:

• Members of Role1 will manage application security groups.
• Members of Role2 will manage Azure Bastion.

You need to add permissions to the custom roles.

Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider may be used, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer Area

Microsoft.Compute

Microsoft.Network

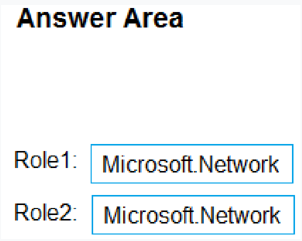
Microsoft.Security

Microsoft.Solutions

Role1:

Role2:

Suggested Answer:



Answer Area

Role1: Microsoft.Network

Role2: Microsoft.Network

Seelearndo Highly Voted 2 years, 5 months ago

Answer is correct: Microsoft.Network, Microsoft.Network

For Bastion: https://learn.microsoft.com/en-us/azure/templates/microsoft.network/bastionhosts

For ASGs: https://learn.microsoft.com/en-us/rest/api/virtualnetwork/application-security-groups/create-or-update?tabs=HTTP

upvoted 29 times

MS_KoolaidMan 2 years, 2 months ago

Thanks, @Seelearndo!

I appreciate it when people back-up their answers with Microsoft Documentation. :)

upvoted 5 times

zellck Highly Voted 2 years, 2 months ago

1. Microsoft.Network
2. Microsoft.Network

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers

Microsoft.Network

- Azure Bastion
- Virtual Network

upvoted 8 times

zellck 2 years, 2 months ago

https://learn.microsoft.com/en-us/azure/templates/microsoft.network/applicationsecuritygroups?pivots=deployment-language-bicep

https://learn.microsoft.com/en-us/azure/templates/microsoft.network/bastionhosts?pivots=deployment-language-bicep

upvoted 2 times

schpeter_091 Most Recent 7 months, 1 week ago

supporting the Bastion part:

Microsoft.Network/bastionHosts creates the bastion host.

Microsoft.Network/virtualNetworks creates a virtual network.

Microsoft.Network/virtualNetworks/subnets creates the subnet.

Microsoft Network/networkSecurityGroups controls the NSG settings.

Microsoft.Network/publicIpAddresses specifies the public IP address value for the bastion host.

reference:

https://learn.microsoft.com/en-us/azure/bastion/quickstart-host-arm-template#review-the-template

upvoted 1 times

brooklyn510 1 year, 5 months ago

In exam 1/2/24

upvoted 3 times

majstor86 2 years, 3 months ago

Microsoft.Network -Members of Role1 will manage application security groups (ASGs).

Microsoft.Network -Members of Role2 will manage Azure Bastion.

upvoted 4 times

Question #81 *Topic 2*

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.

You plan to implement Azure Active Directory (Azure AD) Identity Protection.

You need to ensure that you can configure a user risk policy and a sign-in risk policy.

What should you do first?

A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.

B. Register all users for Azure Multi-Factor Authentication (MFA).

C. Enable security defaults for Azure Active Directory.

D. Enable enhanced security features in Microsoft Defender for Cloud.

Suggested Answer: *A*

Community vote distribution

A (100%)

AzureJobsTillRetire Highly Voted 👍 1 year, 11 months ago

Selected Answer: A

Repeat question of Question #52Topic 2

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

upvoted 11 times

golitech Most Recent 🕘 4 months, 4 weeks ago

Selected Answer: A

Identity Protection is supported in plan 2.

upvoted 1 times

wingcheuk 11 months, 3 weeks ago

Answer is A.

See self-explanation from Azure Portal:

Microsoft Entra ID Protection is an IT admin's solution to prevent, detect, and remediate identity risks in an organization. Microsoft Entra ID P2 edition (available with EMS E5 subscription) is needed to use Microsoft Entra ID Protection.

If you are not a Microsoft Entra ID P2 edition subscriber, you can view limited Microsoft Entra ID security reports at Microsoft Entra ID > Security.

upvoted 1 times

yonie 1 year ago

Selected Answer: A

Risk-based policies require access to Identity Protection, which is a Microsoft Entra ID P2 feature

https://learn.microsoft.com/en-us/entra/fundamentals/licensing#microsoft-entra-conditional-access

upvoted 2 times

fireb 1 year, 3 months ago

Selected Answer: A

A is correct.

upvoted 2 times

zellck 1 year, 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#license-requirements

Using Identity Protection requires Azure AD Premium P2 licenses.

upvoted 3 times

⊟ **majstor86** 1 year, 10 months ago

Selected Answer: A

A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.

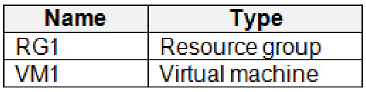
upvoted 4 times

Question #82 Topic 2

HOTSPOT

-

You have an Azure subscription that contains the resources shown in the following table.



Name	Type
RG1	Resource group
VM1	Virtual machine

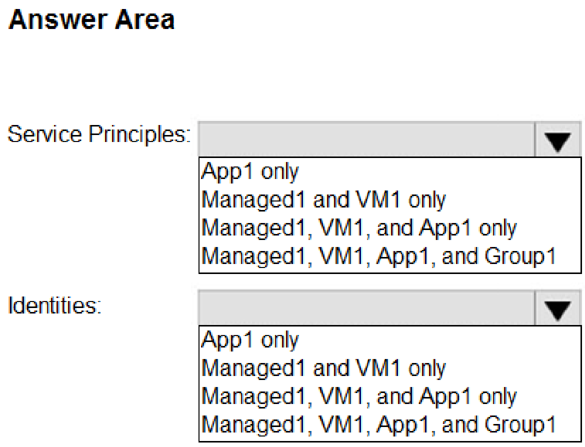
You perform the following tasks:

- Create a managed identity named Managed1.
- Create a Microsoft 365 group named Group1.
- Register an enterprise application named App1.
- Enable a system-assigned managed identity for VM1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1.

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

NOTE: Each correct selection is worth one point.

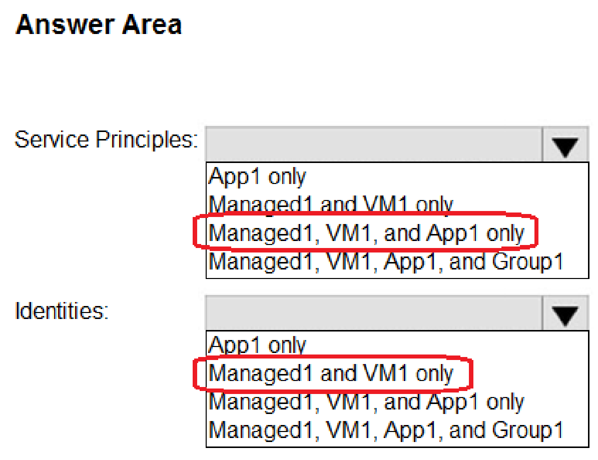


Answer Area

Service Principles:
App1 only
Managed1 and VM1 only
Managed1, VM1, and App1 only
Managed1, VM1, App1, and Group1

Identities:
App1 only
Managed1 and VM1 only
Managed1, VM1, and App1 only
Managed1, VM1, App1, and Group1

Suggested Answer:



Answer Area

Service Principles:
App1 only
Managed1 and VM1 only
[✓ Managed1, VM1, and App1 only]
Managed1, VM1, App1, and Group1

Identities:
App1 only
[✓ Managed1 and VM1 only]
Managed1, VM1, and App1 only
Managed1, VM1, App1, and Group1

undecided Highly Voted 2 years, 5 months ago

Tested in the Portal; second answer looks to be incorrect.

Service Principals: Managed1, VM1, and App1 only

Identities: Managed1, VM1, App1, and Group1

upvoted 31 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

I agree that Group1 can. I tested in lab as well. I created a Microsoft 365 group and I found that it appears in the select member list.
I'm not too sure about App1 service principle though. I registered an app and its service principle does not show up in the select member list. I might have done my lab wrong though.
But I will choose undecided's answer when I go to exam.

upvoted 2 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

anyway, there is not an option for Manager1, VM1 and Group1 only for box 2, hence the answer for the second box must be all

upvoted 1 times

⊟ **zellck** Highly Voted 2 years, 2 months ago

1. Managed1, VM1 and App1 only
2. Managed1, VM1, App1 and Group1

https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals#service-principal-object
There are three types of service principal:
- Application - The type of service principal is the local representation, or application instance, of a global application object in a single tenant or directory.
- Managed identity - This type of service principal is used to represent a managed identity. Managed identities eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to resources that support Azure AD authentication.
- Legacy - This type of service principal represents a legacy app, which is an app created before app registrations were introduced or an app created through legacy experiences.

upvoted 12 times

⊟ **zellck** 2 years, 2 months ago

https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-role-assignments-to-groups-work
To assign a role to a group, you must create a new security or Microsoft 365 group with the isAssignableToRole property set to true. In the Azure portal, you set the Azure AD roles can be assigned to the group option to Yes. Either way, you can then assign one or more Azure AD roles to the group in the same way as you assign roles to users.

upvoted 3 times

⊟ **Nhadipour** Most Recent 4 months, 3 weeks ago

Service Principals: Managed1, VM1, and App1 only
Identities: Managed1, VM1, and App1 only

Azure RBAC roles (Reader) cannot be assigned to Microsoft 365 Groups directly. RBAC roles are assigned to Azure AD users, service principals, and managed identities.

upvoted 3 times

⊟ **golitech** 4 months, 4 weeks ago

Service Principals Created:
Managed1 (The service principal representing the managed identity you created)
App1 (The service principal for the registered enterprise application)
VM1 (The service principal representing the system-assigned managed identity for VM1)

Identities That Can Be Assigned the Reader Role for RG1:
Managed1 (The managed identity you created for a service can be assigned the Reader role for RG1).
App1 (The service principal for the enterprise application can also be assigned the Reader role).
VM1 (The system-assigned managed identity of the VM can be assigned the Reader role).
However, Group1 cannot directly be assigned the Reader role unless it is configured with roles that map to a service principal (e.g., using Azure AD groups for access control). In this case, Group1 does not directly have a service principal for role assignment purposes in RG1.

upvoted 2 times

⊟ **Jimmy500** 1 year ago

Look guys, do not reply please here until you do not know question. In the first question it asks which service principial creating keep in mind this will happen when we will create app registration. So the first one will be App1 only. For the second one it asks which identity can be asked as a reader role Grouup1 can not as it is MS365 group, but we can asssign it for Managed identity, Service Principial and VM1 as it has system assigned managed idetity.

Answer:

App1 only

Managed1,VM1, App1 only

upvoted 2 times

⊟ **Jimmy500** 11 months, 3 weeks ago

I am so sorry guys, my first answer is wrong let me correct my mistake.

When we create managed identity does not matter system or user assigned we can see the service principial for them in the Entra Id, if search with the id of managed identity we will see that also when we register application we also will see on service pricipial under enterprice applications in the first box besides Group creation we will see principial creation in other 3 cases which means given answer for the first box is correct.

For the second box we should choose all of them as we can also assign role to Microsoft 365 groups as well, we can not assign role to the nested groups , please keep this in your mind as well for the other question.Once again sorry for my first answer.

upvoted 4 times

⊟ **NICKTON81** 1 year, 3 months ago

Service Principals: Managed1, VM1, and App1 only

Identities: Managed1, VM1, and App1 only

PS: You can't assign Reader role for RG1 using MS365 groups.

upvoted 2 times

⊟ **wardy1983** 1 year, 7 months ago

Explanation:

Service Principals: Managed1, VM1, and App1 only

Identities: Managed1, VM1, App1, and Group1

upvoted 2 times

⊟ **flafernan** 1 year, 7 months ago

SERVICE PRINCIPLES:

Managed1, VM1 and App1 only

IDENTITIES (Identities):

Managed1 and VM1 only

Explanation:

Managed1 is a managed identity that you created.

VM1, when having a managed identity enabled, also generates a Service Principal to represent a VM in Azure AD.

App1, being a registered enterprise application, is associated with a Service Principal.

Microsoft 365 Group1 does not generate Service Principal and is not directly related to this configuration.

Only Managed1, VM1 and App1 have Service Principals associated with them. Although Managed1 and VM1 have managed identities, Group1 does not fall into the Service Principals or Identities categories in this context.

upvoted 1 times

⊟ **TheProfessor** 1 year, 8 months ago

When you go to assign role, you have to select either 1) user, group or service principle or 2) Managed Identity.

So Identities: Managed1, VM1, App1, and Group1

upvoted 1 times

⊟ **tweleve** 1 year, 8 months ago

in exam 13 Oct

upvoted 3 times

⊟ **nox2447** 1 year, 9 months ago

Pretty sure it is:

Service Principals: App1 only

and

Identities: Managed1, VM1

Identities and Service Principal are not the same.

Imo this questions tests whether you know that SP is created during App creation and how the differ from managed identities.

upvoted 4 times

[Removed] 2 years, 3 months ago

currently, when you select members for an RG, there is a radio button for either "User, group, or service principal" or "Managed identity" that determines how the view is filtered. You are allowed to add a mix of both

upvoted 2 times

majstor86 2 years, 3 months ago

Service Principals: Managed1, VM1, and App1 only

Identities: Managed1, VM1, App1, and Group1

Service principals:

https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals#service-principal-obje

Identity:

https://devblogs.microsoft.com/devops/demystifying-service-principals-managed-identities/

upvoted 7 times

sofieejo 2 years, 5 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 3 times

mskott 2 years, 5 months ago

Managed identity and service principal are two different types of 'identities'

It should be:

Service Principal: App1 only

Identities:

Managed1 (user assigned identity), VM1 (which has system assigned identity), App1 (service principal)only

upvoted 4 times

AzureJobsTillRetire 2 years, 5 months ago

There are three types of service principal:

Application

Managed identity

Legacy

https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals#service-principal-object

upvoted 4 times

Ajdlfasudfo0 2 years, 5 months ago

answer seems to be correct;

https://stackoverflow.com/questions/47762262/add-aad-application-as-a-member-of-a-security-group

upvoted 4 times

Question #83 Topic 2

HOTSPOT

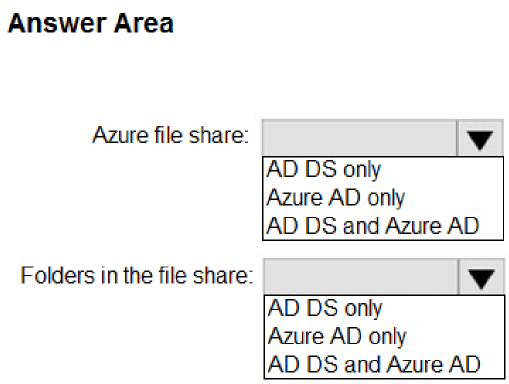
-

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You plan to create an Azure file share that will contain folders and files.

Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

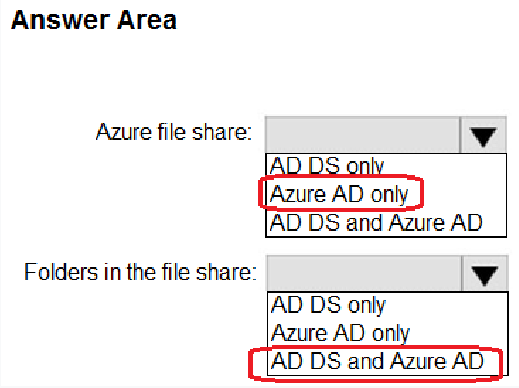


Answer Area

Azure file share: ▼
AD DS only
Azure AD only
AD DS and Azure AD

Folders in the file share: ▼
AD DS only
Azure AD only
AD DS and Azure AD

Suggested Answer:



Answer Area

Azure file share: ▼
AD DS only
[✓ Azure AD only]
AD DS and Azure AD

Folders in the file share: ▼
AD DS only
Azure AD only
[✓ AD DS and Azure AD]

Nick66 Highly Voted 2 years, 5 months ago

Box1 and Box2: AD DS Only

Azure Files supports identity-based authentication for Windows file shares over Server Message Block (SMB) using the Kerberos authentication protocol through the following three methods:

- On-premises Active Directory Domain Services (AD DS)
- Azure Active Directory Domain Services (Azure AD DS)
- Azure Active Directory (Azure AD) Kerberos for hybrid user identities

Note

Azure Files supports authentication for Azure AD DS with full or partial (scoped) synchronization with Azure AD. For environments with scoped synchronization present, administrators should be aware that Azure Files only honors Azure RBAC role assignments granted to principals that are synchronized. Role assignments granted to identities not synchronized from Azure AD to Azure AD DS will be ignored by the Azure Files service.

upvoted 26 times

stepman 2 years, 2 months ago

I chose this. On exam 4/27. the new exam experience. No Sim or lab.

upvoted 14 times

Tweety1972 2 years, 2 months ago

Share-level permissions on Azure file shares are configured for Azure Active Directory (Azure AD) users, groups, or service principals, while directory and file-level permissions are enforced using Windows access control lists (ACLs).

upvoted 4 times

⊟ **undecided** Highly Voted 2 years, 5 months ago

As per https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#how-it-works, I believe:

Box 1: Azure AD only (same as how for on-prem AD it's Azure AD)
Box 2: AD DS only (same as how for on-prem AD it's AD DS)

upvoted 16 times

⊟ **ca7859c** Most Recent 1 month ago

Answer is correct

Entra ID at share level and AD DS at file level

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions?tabs=azure-portal#choose-how-to-assign-share-level-permissions

Share-level permissions on Azure file shares are configured for Microsoft Entra users, groups, or service principals, while directory and file-level permissions are enforced using Windows access control lists (ACLs). You must assign share-level permissions to the Microsoft Entra identity representing the user, group, or service principal that should have access.

upvoted 1 times

⊟ **ca7859c** 1 month ago

1st Entra ID
2nd AD DS & Entra ID at file level*
\sorry for the typo

upvoted 1 times

⊟ **golitech** 4 months, 4 weeks ago

For Azure File Share:
Answer: AD DS only
This is because Azure Files (when using SMB protocol) supports Active Directory Domain Services (AD DS) authentication for assigning permissions to the Azure file share itself. Azure AD is not directly used for managing file share-level permissions in this context.

For Folder in the File Share:
Answer: Both
Permissions for folders within the Azure file share can be managed using either Azure AD or AD DS, depending on your configuration:

Azure AD can be used if the file share is configured for Azure AD authentication.
AD DS can be used if the file share is configured for AD DS authentication.
Thus, both Azure AD and AD DS can be used for folder-level permissions, depending on the authentication method chosen.

upvoted 2 times

⊟ **cerifyme85** 9 months ago

1. Azure Ad and Azure ADDs
2. Azure AD only

upvoted 1 times

⊟ **pentium75** 11 months ago

To me it's unclear what "identity store" is supposed to mean. However, there's this sentence in the documentation:

"None of the authentication methods support assigning share-level permissions to computer accounts (machine accounts) using Azure RBAC, because computer accounts can't be synced to an identity in Microsoft Entra ID. If you want to allow a computer account to access Azure file shares using identity-based authentication, use a default share-level permission or consider using a service logon account instead."

This indicates that share-level permissions are somehow using Entra ID while folder-level permissions are using AD/ADDS. So I'd say first answer is "Azure AD only".

upvoted 2 times

⊟ **Alex1405** 1 year ago

To correctly assign permissions to an Azure file share and the folders within the share, considering an environment that syncs with an Active Directory Domain Services (AD DS) domain, you need to choose the appropriate identity store. The correct answers are:

Azure file share:

AD DS only: Azure Files supports identity-based authentication over SMB (Server Message Block) by integrating with AD DS. This allows you to use on-premises AD DS to authenticate and authorize users for accessing Azure file shares.
Folders in the file share:

AD DS only: Since the Azure file share is integrated with AD DS for authentication and authorization, the permissions for folders within the file share will also rely on AD DS.
So the correct options are:

For the Azure file share: AD DS only
For folders in the file share: AD DS only
upvoted 2 times

Ivan80 1 year, 5 months ago
In exam 1/28/24
upvoted 2 times

brooklyn510 1 year, 5 months ago
On exam 1/2/24
upvoted 3 times

shako 1 year, 5 months ago
No Sim or lab ?
upvoted 1 times

Obama_boy 1 year, 6 months ago
in exam 08/12/23
upvoted 1 times

ubiquituz 1 year, 7 months ago
box1: ad ds and azure ad (microsoft entra)
box2: ad ds and azure ad (microsoft entra)
https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview
https://techcommunity.microsoft.com/t5/azure-storage-blog/general-availability-introducing-azure-ad-support-for-azure/ba-p/3826733
upvoted 7 times

wardy1983 1 year, 8 months ago
box1: AD DS only
The selected Azure AD identity must be a hybrid identity and cannot be a cloud only identity. This means that
the same identity is also represented in AD DS. https://learn.microsoft.com/en-us/azure/storage/files/storagefiles-identity-ad-ds-assign-permissions?tabs=azureportal
Box 2: AD DS only
upvoted 2 times

Alster77 1 year, 11 months ago
I chose the answers presented. In exam taken 24 July 2023
Box 1: Azure AD - https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions
Box 2 - Azure AD and AD DS - read what's in the Important note which talks about AD DS and Azure AD DS - https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-configure-permissions
upvoted 4 times

massnonn 2 years ago
To assign permissions to an Azure file share and its folders, you can use the Azure Active Directory (Azure AD) identity store. Azure AD provides a centralized identity and access management solution for Azure services, including Azure file shares.
upvoted 1 times

zellck 2 years, 2 months ago
1. Azure AD only
2. AD DS only

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#ad-ds

This is because the share-level permission is configured against the identity represented in Azure AD, whereas the directory/file-level permission is enforced with that in AD DS.

upvoted 9 times

aztitef 2 years, 2 months ago

1. Azure AD only.

2. Azure AD DS only

Share-level permissions on Azure file shares are configured for Azure Active Directory (Azure AD) users, groups, or service principals, while directory and file-level permissions are enforced using Windows access control lists (ACLs).

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

upvoted 5 times

> **upliftinghut** 2 years, 2 months ago
>
> Thanks for the link, but as I read it, the users/groups need to be hybrid, can't be pure Azure AD => Azure AD DS both
>
> upvoted 2 times

> **Tweety1972** 2 years, 2 months ago
>
> Share-level permissions on Azure file shares are configured for Azure Active Directory (Azure AD) users, groups, or service principals, while directory and file-level permissions are enforced using Windows access control lists (ACLs).
>
> upvoted 1 times

majstor86 2 years, 3 months ago

1. AD DS only

2. AD DS only

upvoted 6 times

> **Tweety1972** 2 years, 2 months ago
>
> Share-level permissions on Azure file shares are configured for Azure Active Directory (Azure AD) users, groups, or service principals, while directory and file-level permissions are enforced using Windows access control lists (ACLs).
>
> upvoted 2 times

Question #84 Topic 2

You have an Azure subscription.

You plan to deploy a new Conditional Access policy named CAPolicy1.

You need to use the What if tool to evaluate how CAPolicy1 wall affect users. The solution must minimize the impact of CAPolicy1 on the users.

To what should you set the Enable policy setting for CAPolicy1?

A. Off

B. On

C. Report only

Suggested Answer: *C*

Community vote distribution

C (100%)

OrangeSG Highly Voted 1 year, 5 months ago

Selected Answer: C

By setting the "Enable policy" setting to "Report only" for CAPolicy1, the policy will not be enforced, but it will still generate reports on how it would have affected users if it were enforced. This will allow you to evaluate the impact of the policy on users and make any necessary adjustments before enabling it.

upvoted 7 times

flafernan Most Recent 7 months, 3 weeks ago

Selected Answer: C

In a scenario where you plan to implement a “Conditional Access Policy”, however, if you just want to do a test and apply a policy without affecting users, the option you should use is “What if”, when configuring o conditional access policy. You must check “Report only”, this way it will be possible to simulate the impact of a new conditional access policy before applying it. It is even considered good practice.

upvoted 1 times

Self_Study 10 months, 3 weeks ago

Selected Answer: C

On exam 7/8/23. Answers are correct.

upvoted 3 times

zellck 1 year, 2 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only
Conditional Access is widely used by our customers to stay secure by applying the right access controls in the right circumstances. However one of the challenges with deploying a Conditional Access policy in your organization is determining the impact to end users. It can be difficult to anticipate the number and names of users impacted by common deployment initiatives such as blocking legacy authentication, requiring multifactor authentication for a population of users, or implementing sign-in risk policies.

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment.

upvoted 3 times

majstor86 1 year, 3 months ago

Selected Answer: C

C. Report only

upvoted 3 times

shahnawazkhot 1 year, 5 months ago

Great!

upvoted 1 times

⊟ **Nickname01** 1 year, 5 months ago

correct answer

upvoted 4 times

Question #85 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant that contains 500 users and an administrative unit named AU1.

From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members.

You need to create and upload a file for the bulk add.

What should you include in the file?

A. only the display name of each user

B. only the user principal name (UPN) of each user

C. only the user principal name (UPN) and display name of each user

D. only the user principal name (UPN) and object identifier of each user

E. only the object identifier of each user

Suggested Answer: *C*

Community vote distribution

B (90%) 8%

Ajdlfasudfo0 Highly Voted 2 years, 5 months ago

Selected Answer: B

asking for administrative unit import: https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units-members-add

UPN is the correct answer

upvoted 16 times

wardy1983 Most Recent 1 year, 5 months ago

https://learn.microsoft.com/en-us/entra/identity/users/users-bulk-add

upvoted 1 times

im30batman 1 year, 5 months ago

https://learn.microsoft.com/en-us/entra/identity/users/groups-bulk-import-members#bulk-import-group-members

It says here that you can use Either the UPN or the Object ID

I tested it and both worked.

upvoted 1 times

yonie 1 year, 6 months ago

Selected Answer: B

Users already exists.

Answer is B

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-members-add#add-users-to-an-administrative-unit-in-a-bulk-operation

upvoted 1 times

quangDV 1 year, 6 months ago

Provided answer is correct

https://learn.microsoft.com/en-us/entra/identity/users/users-bulk-add

upvoted 1 times

quangDV 1 year, 6 months ago

Sorry, not fully read the question.

The correct answer is B. As the users to be added to the administrative unit are already present in AAD, therefore only users' SPNs are required.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-members-add

upvoted 2 times

wardy1983 1 year, 7 months ago

Answer: B

Explanation:

When adding users to an administrative unit using the Bulk add members feature, the file should contain only the user principal names (UPNs) of the users. The UPN is the unique identifier for each user in Azure AD and is typically in the format of an email address (e.g. [email protected]). By including only the UPN in the file, you can ensure that the correct users are added to the administrative unit.

upvoted 2 times

whm1919 1 year, 7 months ago

Selected Answer: D

Answer is D/

The correct answer is D. only the user principal name (UPN) and object identifier of each user.

When adding users to an administrative unit in Azure AD by using Bulk add members, you must include the user principal name (UPN) and object identifier of each user in the file. The display name is not required.

Here is an example of the format of the file:

Version=1
Item type=Member
Member object ID,User principal name
[Object identifier],user@example.com
[Object identifier],anotheruser@example.com
You can find the object identifier for each user in the Azure AD admin center. To do this, go to Users > All users. Select the user that you want to find the object identifier for, and then click the Attributes tab. The object identifier will be listed under Object ID.

upvoted 1 times

pentium75 11 months ago

No, only UPN per https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-members-add#add-users-to-an-administrative-unit-in-a-bulk-operation

upvoted 1 times

Feraso 1 year, 8 months ago

Selected Answer: B

Answer is B

Edit the downloaded CSV template with the list of users you want to add.

Add one user principal name (UPN) in each row. Don't remove the first two rows of the template.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-members-add#add-users-to-an-administrative-unit-in-a-bulk-operation

upvoted 1 times

TheProfessor 1 year, 9 months ago

Selected Answer: B

Correct answer is B

upvoted 2 times

Softeng 1 year, 9 months ago

Selected Answer: B

only UPN is needed

answer on documentation: https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units-members-add#:~:text=Add%20one%20user%20principal%20name%20(UPN)%20in%20each%20row.%20Don%27t%20remove%20the%20first%20two%20rows%20of%20t

upvoted 1 times

ITFranz 1 year, 9 months ago

B is the correct answer.

In the Bulk add members pane, download the comma-separated values (CSV) template.

Edit the downloaded CSV template with the list of users you want to add.
Add one user principal name (UPN) in each row. Don't remove the first two rows of the template.
Save your changes and upload the CSV file.
https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units-members-add
upvoted 2 times

alfaAzure 1 year, 10 months ago

Selected Answer: C

C. Only the user principal name (UPN) and display name of each user

When using the Bulk add members feature in Azure Active Directory, you should include a file that contains the user principal name (UPN) and display name of each user you want to add to the administrative unit. This information helps Azure AD identify the users and place them into the appropriate administrative unit (AU1) within your organization's directory.

The user principal name (UPN) is a unique identifier for each user in Azure AD, and the display name provides a human-readable name associated with the user. Including both UPN and display name in the file ensures that Azure AD can accurately match the users and add them to the specified administrative unit.
upvoted 3 times

zellck 2 years, 2 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units-members-add#add-users-to-an-administrative-unit-in-a-bulk-operation
Edit the downloaded CSV template with the list of users you want to add.
- Add one user principal name (UPN) in each row.
upvoted 3 times

r_git 2 years, 3 months ago

Selected Answer: B

B. only the user principal name (UPN) of each user

"In the Bulk add members pane, download the comma-separated values (CSV) template.
Edit the downloaded CSV template with the list of users you want to add.
Add one user principal name (UPN) in each row. Don't remove the first two rows of the template."

https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units-members-add#add-users-to-an-administrative-unit-in-a-bulk-operation
upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: B

B. only the user principal name (UPN) of each user
upvoted 3 times

OrangeSG 2 years, 5 months ago

Selected Answer: B

When adding users to an administrative unit using the Bulk add members feature, the file should contain only the user principal names (UPNs) of the users. The UPN is the unique identifier for each user in Azure AD and is typically in the format of an email address (e.g. user@contoso.com). By including only the UPN in the file, you can ensure that the correct users are added to the administrative unit.
upvoted 4 times

dumpIT 2 years, 5 months ago

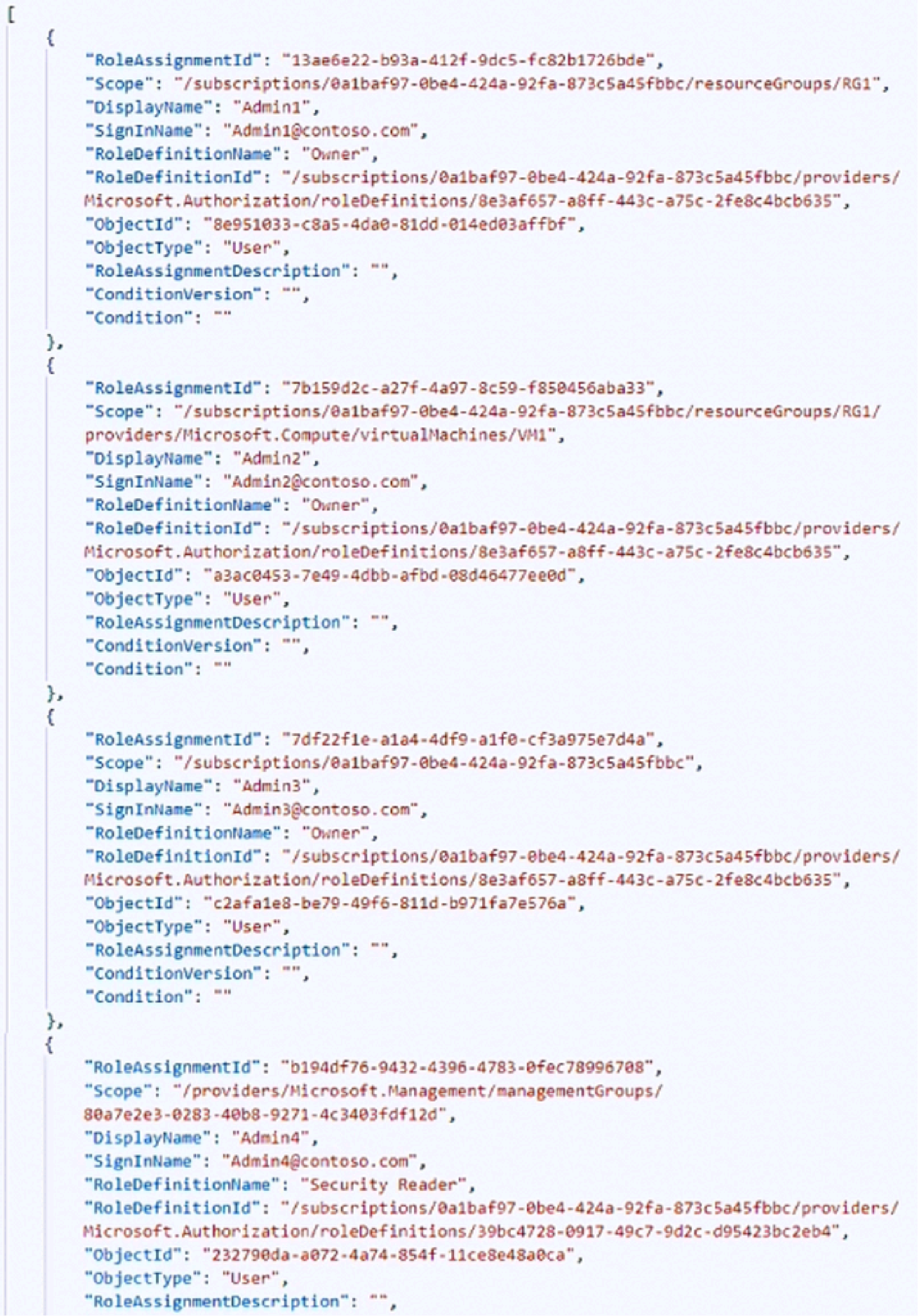
Selected Answer: B

definitely B. also tested in lab
upvoted 4 times

HOTSPOT

-

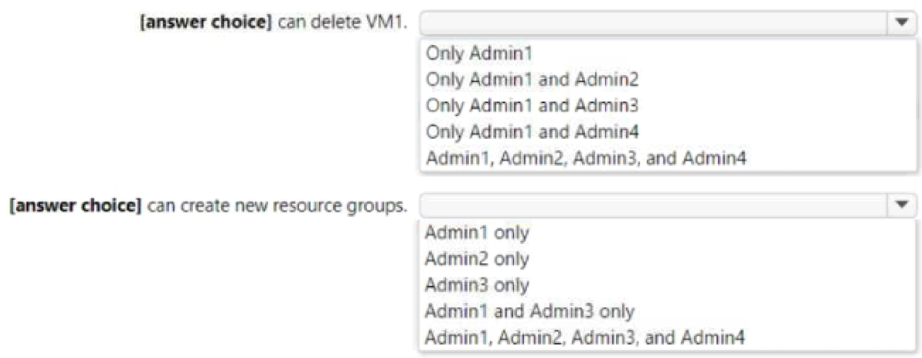
You have the role assignments shown in the following exhibit.



```
[
    {
        "RoleAssignmentId": "13ae6e22-b93a-412f-9dc5-fc82b1726bde",
        "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1",
        "DisplayName": "Admin1",
        "SignInName": "Admin1@contoso.com",
        "RoleDefinitionName": "Owner",
        "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
        Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
        "ObjectId": "8e951033-c8a5-4da0-81dd-014ed03affbf",
        "ObjectType": "User",
        "RoleAssignmentDescription": "",
        "ConditionVersion": "",
        "Condition": ""
    },
    {
        "RoleAssignmentId": "7b159d2c-a27f-4a97-8c59-f850456aba33",
        "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1/
        providers/Microsoft.Compute/virtualMachines/VM1",
        "DisplayName": "Admin2",
        "SignInName": "Admin2@contoso.com",
        "RoleDefinitionName": "Owner",
        "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
        Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
        "ObjectId": "a3ac0453-7e49-4dbb-afbd-08d46477ee0d",
        "ObjectType": "User",
        "RoleAssignmentDescription": "",
        "ConditionVersion": "",
        "Condition": ""
    },
    {
        "RoleAssignmentId": "7df22f1e-a1a4-4df9-a1f0-cf3a975e7d4a",
        "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc",
        "DisplayName": "Admin3",
        "SignInName": "Admin3@contoso.com",
        "RoleDefinitionName": "Owner",
        "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
        Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
        "ObjectId": "c2afa1e8-be79-49f6-811d-b971fa7e576a",
        "ObjectType": "User",
        "RoleAssignmentDescription": "",
        "ConditionVersion": "",
        "Condition": ""
    },
    {
        "RoleAssignmentId": "b194df76-9432-4396-4783-0fec78996708",
        "Scope": "/providers/Microsoft.Management/managementGroups/
        80a7e2e3-0283-40b8-9271-4c3403fdf12d",
        "DisplayName": "Admin4",
        "SignInName": "Admin4@contoso.com",
        "RoleDefinitionName": "Security Reader",
        "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
        Microsoft.Authorization/roleDefinitions/39bc4728-0917-49c7-9d2c-d95423bc2eb4",
        "ObjectId": "232790da-a072-4a74-854f-11ce8e48a0ca",
        "ObjectType": "User",
        "RoleAssignmentDescription": "",
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



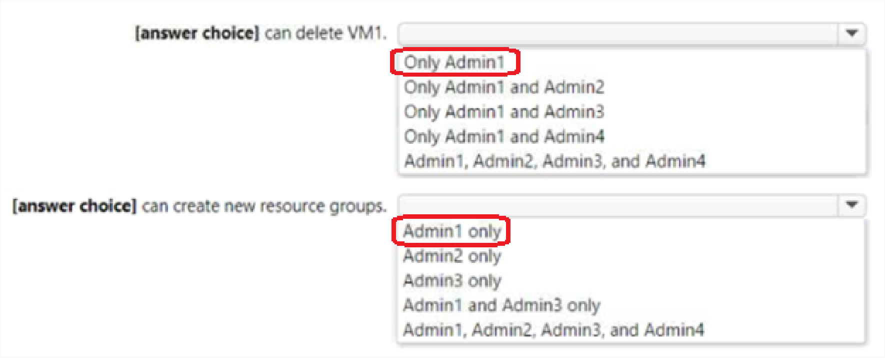
[answer choice] can delete VM1.

- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

- Admin1 only
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Suggested Answer:



[answer choice] can delete VM1.

- [✓ Only Admin1]
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

- [✓ Admin1 only]
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

⊟ **Sekoume** Highly Voted 2 years, 5 months ago

some people pay for this ...

upvoted 59 times

⊟ **8de3321** 7 months ago

Did you get it for free?

upvoted 1 times

⊟ **e31180b** 8 months ago

I did :(

upvoted 2 times

⊟ **AzureJobsTillRetire** Highly Voted 2 years, 5 months ago

Is the question complete? I can only see Admin1 being an owner of RG1 and Admin4 being a security reader. It the question is complete, obviously only Admin1 could possibly delete or create something.

upvoted 29 times

⊟ **Nhadipour** Most Recent 4 months, 3 weeks ago

Can delete VM1: Admin1, Admin3 (Technically admin2 can delete its own VM as well!)

Can create a new resource group: Admin 3 only

Admin1 ("Owner" at RG1 Scope)

Admin2 ("Owner" at VM1 Scope)

Admin3 ("Owner" at Subscription Scope)

Admin4 ("Security Reader" at Management Group Scope)

upvoted 9 times

⊟ **barte** 5 months, 3 weeks ago

can delete VM1: Admin1 (owner of the RG1 which the VM1 resides in) and Admin3 (owner of the entire subscription)

can create new resource groups: Admin3 only (only Admin3 is an owner of the subscription)

upvoted 8 times

⊟ **Exam2us** 7 months, 1 week ago

Admin1 have Owner permission to RG1 so he can delete the VM. Admin3 has the Owner permission to the subscription so he should be able to delete the VM as well.

For the second question who can create RG it should be Admin3.

upvoted 2 times

schpeter_091 8 months ago

I think it is a wrong question. Admin 1 is an owner but the scope is RG1. So he can delete a VM(inside that RG), but he cannot create another RG, since RG cannot be created in another RG. There is no such option that nobody can create an RG.

upvoted 1 times

xRiot007 10 months, 1 week ago

Is this question incomplete? Admin 2 and 3 don't even have roles

upvoted 1 times

91743b3 10 months, 3 weeks ago

A question very similar to this but with 2 additional role assignments and two additional question choices was on exam Aug 06 2024. Make sure you understand the concept.

upvoted 2 times

TheProfessor 1 year, 9 months ago

I think the question is not completed. So the response is just based on the "RoleName"?

upvoted 2 times

zellck 2 years, 2 months ago

1. Only Admin1
2. Admin1 only

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.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-reader
View permissions for Microsoft Defender for Cloud. Can view recommendations, alerts, a security policy, and security states, but cannot make changes.

upvoted 5 times

saturation97 2 years, 2 months ago

Sooo, I guess we go with Admin 1

upvoted 4 times

majstor86 2 years, 3 months ago

not a complete question. Admin 2 and Admin 3 are not mentioned!!!

upvoted 7 times

Question #87 *Topic 2*

You have an Azure subscription that contains a user named User1.

You need to ensure that User1 can create managed identities. The solution must use the principle of least privilege.

What should you do?

A. Create a management group and assign User1 the Hybrid Identity Administrator Azure Active Directory (Azure AD) role.

B. Create a management group and assign User1 the Managed Identity Operator role.

C. Create a resource group and assign User1 to the Managed Identity Contributor role.

D. Create an organizational unit (OU) and assign User1 the User administrator Azure Active Directory (Azure AD) role.

Suggested Answer: *C*

Community vote distribution

C (96%) 4%

Seelearndo Highly Voted 1 year, 11 months ago

Selected Answer: C

A - Wrong - Hybrid Identity Admin cannot create managed identities. Permissions are: Can manage AD to Azure AD cloud provisioning, Azure AD Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless Single sign-on (Seamless SSO), and federation settings.

B - wrong - Managed Identity Operator cannot create managed identities. Permissions are: Read and Assign User Assigned Identity

C - correct: Managed Identity Contributor can Create, Read, Update, and Delete User Assigned Identity.

D - incorrect - can create users, but does not follow the principal of least privilege, as the permission set is comprehensive. User administrator can manage all aspects of users and groups.

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
upvoted 18 times

waqqy Most Recent 5 months ago

Selected Answer: C

C. Create a resource group and assign User1 to the Managed Identity Contributor role.

Explanation:
Managed Identity Contributor Role: This role allows the user to manage managed identities, including creating and deleting them, within the scope of the assigned resource group. It provides the necessary permissions without granting excessive access1.
Principle of Least Privilege: By assigning the Managed Identity Contributor role at the resource group level, you ensure that User1 has the minimum permissions required to perform the task, reducing the risk of unnecessary access to other resources.
upvoted 1 times

alfaAzure 1 year, 4 months ago

Selected Answer: B

B. Create a management group and assign User1 the Managed Identity Operator role.

The Managed Identity Operator role provides the necessary permissions for managing managed identities within Azure, while following the principle of least privilege. This role allows the user to create, update, and delete managed identities without granting broader permissions than necessary.
upvoted 1 times

Austin6488 8 months, 3 weeks ago

it's wrong, Operator role can't create. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
Managed Identity Contributor -- Create, Read, Update, and Delete User Assigned Identity
Managed Identity Operator -- Read and Assign User Assigned Identity

upvoted 1 times

⊟ **Strifelife** 1 year, 5 months ago

What's the resource group for ?

upvoted 3 times

⊟ **zellck** 1 year, 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-manage-user-assigned-managed-identities?pivots=identity-mi-methods-azp#create-a-user-assigned-managed-identity
To create a user-assigned managed identity, your account needs the Managed Identity Contributor role assignment.

upvoted 4 times

⊟ **majstor86** 1 year, 10 months ago

Selected Answer: C

C. Create a resource group and assign User1 to the Managed Identity Contributor role.

upvoted 4 times

Question #88 *Topic 2*

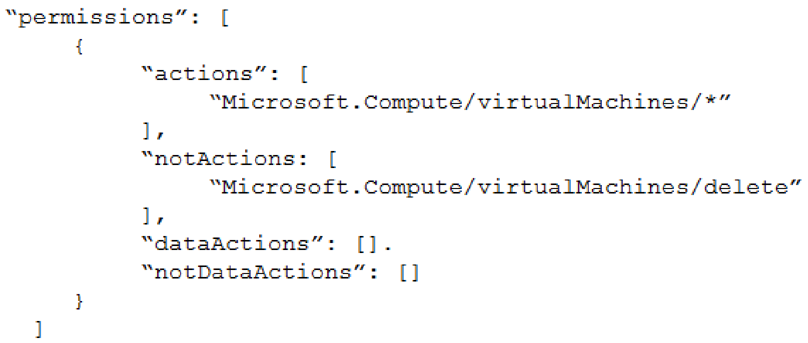
HOTSPOT

-

You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.

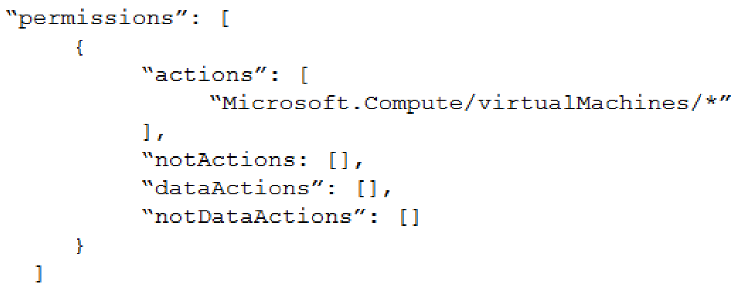
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.



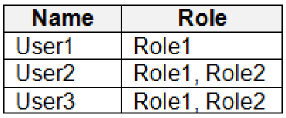
```
"permissions": [
      {
            "actions": [
                  "Microsoft.Compute/virtualMachines/*"
            ],
            "notActions: [
                  "Microsoft.Compute/virtualMachines/delete"
            ],
            "dataActions": [].
            "notDataActions": []
      }
  ]
```

The permissions for Role2 are shown in the following JSON code.



```
"permissions": [
      {
            "actions": [
                  "Microsoft.Compute/virtualMachines/*"
            ],
            "notActions: [],
            "dataActions": [],
            "notDataActions": []
      }
  ]
```

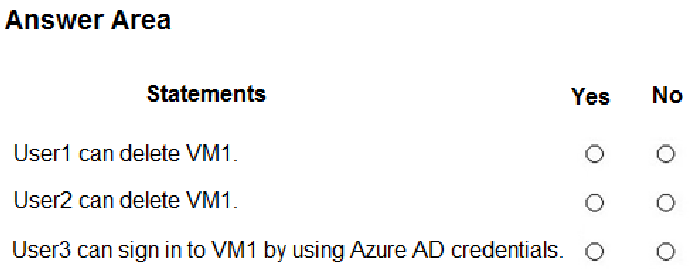
You assign the roles to the users shown in the following table.



Name	Role
User1	Role1
User2	Role1, Role2
User3	Role1, Role2

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

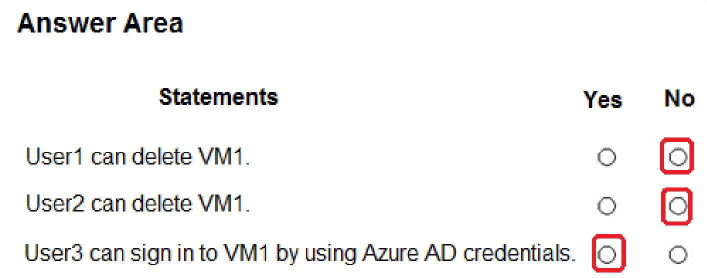
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can delete VM1.	○	○
User2 can delete VM1.	○	○
User3 can sign in to VM1 by using Azure AD credentials.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can delete VM1.	○	[✓ ○]
User2 can delete VM1.	○	[✓ ○]
User3 can sign in to VM1 by using Azure AD credentials.	[✓ ○]	○

AzureJobsTillRetire Highly Voted 2 years, 5 months ago

I thought the answers could be No Yes No

Box1: User1 can delete VM1 - No
User1 only has Role1, and Roles has notActions of VM delete.

Box2: User2 can delete VM - Yes
User2 has both Role1 and Role2 assigned. Role2 gives User2 the ability to delete VM.

Box3: User3 can sign in to VM by using Azure AD credentials - No
To be able to sign in to VM by using Azure AD credentials, User3 needs to have either Virtual Machine Administrator Login or Virtual Machine User Login. Those logins have actions defined in the dataActions section. For example, Microsoft.Compute/virtualMachines/login/action provides Log in to a virtual machine as a regular user. In both Role1 and Role2, the dataActions is not defined.
Refs:
https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-administrator-login

upvoted 59 times

John07 2 weeks ago

```
{
"role": "Virtual Machine Administrator Login",
"description": "Grants a user the ability to log in as administrator to a virtual machine.",
"permissions": {
"compute": {
"actions": [
"Microsoft.Compute/virtualMachines/login/action",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write"
],
"notActions": []
}
},
"assignableScopes": [
"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/{vmName}"
]
}
```

upvoted 1 times

schpeter_091 7 months, 1 week ago

correct answers. Supporting the login thingy:
These are needed to be able to login:
DataActions
Microsoft.Compute/virtualMachines/login/action Log in to a virtual machine as a regular user
Microsoft.Compute/virtualMachines/loginAsAdmin/action Log in to a virtual machine with Windows administrator or Linux root user privileges

upvoted 1 times

BayaliJihad 2 years, 2 months ago

I agree with you

upvoted 1 times

tecnicosoffshoretech 2 years, 2 months ago

Box3 should be yes, he has all the Virtual Machine roles since it has been granted with *
upvoted 4 times

zellck 2 years, 2 months ago
Logging in requires dataActions permissions, not actions permissions.
upvoted 12 times

MunnyStax 1 year, 3 months ago
The Virtual Machine Administrator Login and Virtual Machine User Login roles use dataActions, so they can't be assigned at the management group scope. Currently, you can assign these roles only at the subscription, resource group, or resource scope.
https://learn.microsoft.com/en-us/entra/identity/devices/howto-vm-sign-in-azure-ad-windows
upvoted 1 times

massnonn 2 years ago
DataActions it's only for storage https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#control-and-data-actions
upvoted 3 times

femzy 1 year, 7 months ago
Not true, look at what MS says on the Data Action section of compute provider...Microsoft.Compute/virtualMachines/loginAsAdmin/action Log in to a virtual machine with Windows administrator or Linux root user privileges
upvoted 1 times

bobbywong234 1 year, 5 months ago
Microsoft.Compute/virtualMachines/* should include all privileges for doing so
upvoted 2 times

Ajdlfasudfo0 Highly Voted 👍 2 years, 5 months ago
N-Y-N
https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#notactions
If a user is assigned a role that excludes an action in NotActions, and is assigned a second role that grants access to the same action, the user is allowed to perform that action. NotActions is not a deny rule – it is simply a convenient way to create a set of allowed actions when specific actions need to be excluded.
upvoted 17 times

SSL2 1 year, 7 months ago
Makes sense
upvoted 2 times

ca7859c Most Recent 🕘 1 month ago
NYY

Permission required for login:
Microsoft.Compute/virtualMachines/login/action

User has
Microsoft.Compute/virtualMachines/*
upvoted 1 times

belyo 1 month, 3 weeks ago
following this https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-determines-if-a-user-has-access-to-a-resource
evaluation is for user over a resource
once deny is defined - you cannot overdrive it regardless of how much allow actions are added
no-no-no
upvoted 1 times

pentium75 11 months ago
No - has only Role1 which forbids deletion
Yes - Role2 allows it
No - No data actions
upvoted 1 times

nExoR 11 months, 1 week ago

How Roles are Processed

Aggregation: Azure RBAC aggregates all the Actions and NotActions from the roles assigned to the user.

Most Restrictive Wins: Any action explicitly denied (NotActions) by any role will be denied, regardless of other roles granting that action.

No Order or Priority: There is no specific order in which roles are processed, nor is there a predefined priority among roles. The system evaluates the combined set of permissions and applies the most restrictive policy.

This cumulative and restrictive evaluation ensures that any specific denial of permissions (NotActions) is respected, thereby providing a secure and predictable access control mechanism.

upvoted 1 times

⊟ **Atilgen** 1 year, 1 month ago

You need "dataActions": [
"Microsoft.Compute/virtualMachines/login/action",
"Microsoft.HybridCompute/machines/login/action"
],
to be able to login a vm

upvoted 2 times

⊟ **[Removed]** 1 year, 6 months ago

Microsoft.Compute
Other
Log in to Virtual Machine
This is the data action required to logon to the VM

upvoted 1 times

⊟ **[Removed]** 1 year, 6 months ago

3rd is NO

upvoted 1 times

⊟ **[Removed]** 1 year, 6 months ago

2nd is Yes

User2 and User3 are assigned both Role1 and Role2. Since Role2 does not specify any "notActions", it effectively grants all permissions on virtual machines, including delete. In Azure, if there are conflicting permissions, the most permissive permission takes precedence. Therefore, even though Role1 denies the delete action, Role2 allows it, so User2 and User3 will be able to delete virtual machines.

upvoted 2 times

⊟ **bob_sez** 1 year, 7 months ago

As per this:
https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/control-plane-and-data-plane
Logging into the server is an action on the data plane for which the user 3 does not have permission. So no for User 3 logging into the VM

Overall: No, Yes, NO

upvoted 1 times

⊟ **wardy1983** 1 year, 7 months ago

Box1: User1 can delete VM1 - No
User1 only has Role1, and Roles has notActions of VM delete.
Box2: User2 can delete VM - Yes
User2 has both Role1 and Role2 assigned. Role2 gives User2 the ability to delete VM.
Box3: User3 can sign in to VM by using Azure AD credentials - No
To be able to sign in to VM by using Azure AD credentials, User3 needs to have either Virtual Machine Administrator Login or Virtual Machine User Login. Those logins have actions defined in the dataActions section. For example, Microsoft.Compute/virtualMachines/login/action provides Log in to a virtual machine as a regular user. In both Role1 and Role2, the dataActions is not defined.

upvoted 2 times

⊟ **wardy1983** 1 year, 8 months ago

Box1: User1 can delete VM1 - No
User1 only has Role1, and Roles has notActions of VM delete.
Box2: User2 can delete VM - Yes
User2 has both Role1 and Role2 assigned. Role2 gives User2 the ability to delete VM.
Box3: User3 can sign in to VM by using Azure AD credentials - No
To be able to sign in to VM by using Azure AD credentials, User3 needs to have either Virtual Machine

Administrator Login or Virtual Machine User Login. Those logins have actions defined in the dataActions section. For example, Microsoft.Compute/virtualMachines/login/action provides Log in to a virtual machine as a regular user. In both Role1 and Role2, the dataActions is not defined.

upvoted 1 times

heatfan900 1 year, 10 months ago

Y, Y, N

USER 1 CAN DELETE THE VM AS THEY HAVE THE RIGHT TO DO SO AS PER THE WILDCARD IN THE 'ACTIONS' SECTION. WHEN THERE IS A CONFLICT BETWEEN 'ACTIONS' AND 'NOT ACTIONS' THE PRIOR ALWAYS WINS. THIS IS NOT LIKE ALLOW/DENY WHERE DENY ALWAYS WINS OUT DURING A CONFLICT.

USER 2 CAN DO SO AS WELL AS THE PERMISSIONS CLEARLY STATE.

USER 3 CANNOT AUTHENTICATE TO THE VM WITH AZURE BECAUSE THE ROLES DO NOT HAVE THE PERMISSIONS SET TO DO THIS.

upvoted 2 times

STC007 1 year, 8 months ago

Hi, User1 cannot delete the VM, "The NotActions permission specifies the control plane actions that are subtracted or excluded from the allowed Actions that have a wildcard (*)."

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#notactions

Use the NotActions permission if the set of actions that you want to allow is more easily defined by subtracting from Actions that have a wildcard (*).

Actions - NotActions = Effective control plane permissions

upvoted 3 times

Self_Study 1 year, 10 months ago

On exam 7/8/23. NYN for me.

upvoted 3 times

Ario 1 year, 12 months ago

No YEs NO

upvoted 1 times

zellck 2 years, 2 months ago

NYN is the answer.

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#notactions
If a user is assigned a role that excludes an action in NotActions, and is assigned a second role that grants access to the same action, the user is allowed to perform that action. NotActions is not a deny rule – it is simply a convenient way to create a set of allowed actions when specific actions need to be excluded.

upvoted 7 times

zellck 2 years, 2 months ago

https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm
Now that you've created the VM, you need to configure an 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 who have this role assigned can log in to an Azure virtual machine with administrator privileges.
- Virtual Machine User Login: Users who have this role assigned can log in to an Azure virtual machine with regular user privileges.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-administrator-login
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-user-login

Logging in requires dataActions permissions, not actions permissions.

upvoted 4 times

Alexbz 2 years, 2 months ago

I tried to replicate this scenario in my lab and I got No for all three options. However maybe I was missing something and I'm wrong. I created 2 custom roles with the same permissions and assigned them to the users, none of them even could see the VM. Then I assigned them Reader role and

tried again but I was not able to either delete or login to the VM with either of these three users.
upvoted 3 times

Diaperface 2 years, 2 months ago
I think N-N-Y. "Deny assignments block users from performing specific Azure resource actions even if a role assignment grants them access." - https://learn.microsoft.com/en-us/azure/role-based-access-control/deny-assignments
upvoted 4 times

tecnicosoffshoretech 2 years, 2 months ago
This is not correct, since it is a ¨Not actions¨ not a deny rule

NotActions and deny assignments are not the same and serve different purposes. NotActions are a convenient way to subtract specific actions from a wildcard (*) action.

¨Deny assignments block users from performing specific actions even if a role assignment grants them access¨

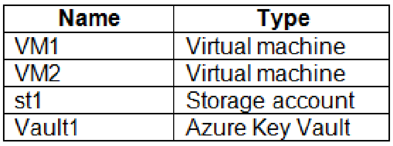
https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions#differences-between-notactions-and-deny-assignments
upvoted 1 times

Question #89 *Topic 2*

DRAG DROP

-

You have an Azure subscription that contains the resources shown in the following table.



Name	Type
VM1	Virtual machine
VM2	Virtual machine
st1	Storage account
Vault1	Azure Key Vault

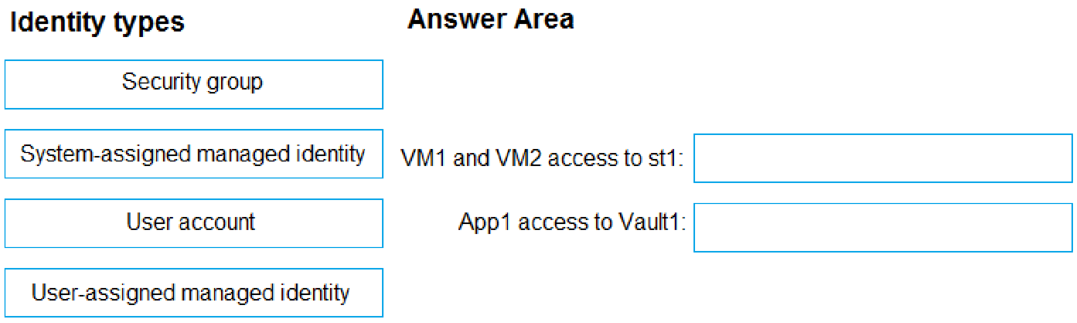
You plan to perform the following actions:

- Deploy a new app named App1 that will require access to Vault1.
- Configure a shared identity for VM1 and VM2 to access st1.

You need to configure identities for each requirement. The solution must minimize administrative effort.

Which type of identity should you configure for each requirement? To answer, drag the appropriate identity types to the correct requirements. Each identity type 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.



Identity types

Security group

System-assigned managed identity

User account

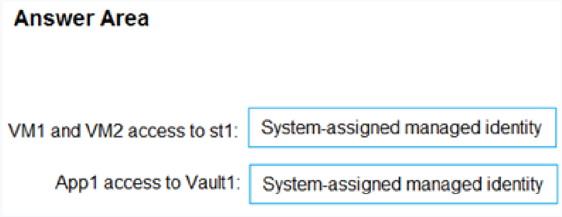
User-assigned managed identity

Answer Area

VM1 and VM2 access to st1:

App1 access to Vault1:

Suggested Answer:



Answer Area

VM1 and VM2 access to st1: System-assigned managed identity

App1 access to Vault1: System-assigned managed identity

AzureJobsTillRetire Highly Voted 2 years, 5 months ago

Box1: VM1 and VM2 access to st1 - User-assigned managed identity

Requirement: Configure a shared identity for VM1 and VM2 to access st1

We have to create a User-assigned managed identity to be shared with VM1 and VM2

Box2: App1 access to Vault1 - System-assigned managed identity

upvoted 66 times

Exam2us 7 months, 1 week ago

Key work is least amount of administrative burden. If we create user assigned managed identity it's too much of a hassle. So system assigned managed identity is the ideal approach.

upvoted 1 times

LHU 1 week, 4 days ago

Or is it? With a user-assigned we only need to assign the role *once*.

upvoted 1 times

[Removed] 1 year, 10 months ago

user assigned managed identity is 1:multiple

system assigned managed identity is: 1:1

upvoted 9 times

fonte Highly Voted 2 years, 5 months ago

Hi all,

Passed today (13JAN2023) my exam with 918. 50 questions (45 + 5 of a case study).

Around 95% of the questions are here.

I've compiled the questions and my answers in a ppt, feel free to check it out and hope it helps.

https://www.dropbox.com/s/ay00xp2fnloq1ex/AZ%20500%20-%20Exam%20Topics.pptx?dl=0

The password for the file is az500prep and you need to download the file first since dropbox doesn't allow opening protected files.

Thanks to all the people that comment on questions, I wouldn't have passed without them :)

upvoted 9 times

BayaliJihad 2 years, 2 months ago

Can you share it with us please? it says it's deleted

upvoted 4 times

d365ppp 2 years, 3 months ago

your file does not exist

upvoted 5 times

Nhadipour Most Recent 4 months, 3 weeks ago

VM1 and VM2 access to st1: User-assigned managed identity

App1 access to Vault1: System-assigned managed identity

upvoted 2 times

Drummer 1 year ago

System-assigned managed identity: This identity is created and tied to the lifecycle of a specific Azure resource, such as a VM. It is automatically deleted when the resource is deleted. It simplifies the management since it's created and maintained automatically by Azure.

User-assigned managed identity: This identity is created independently of the resources that use it. It can be assigned to multiple Azure resources, making it a good choice for applications or services that need to share the same identity.

VM1 and VM2 to access st1: System-assigned managed identity

App1 access to Vault1: User-assigned managed identity

upvoted 2 times

xRiot007 11 months, 1 week ago

VM1 and VM2 need a shared identity, so they will use a user assigned MI.

App1 is alone, so it can use a system assigned MI.

upvoted 2 times

Mouwk 1 year, 5 months ago

Choosing system or user-assigned managed identities:

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identity-best-practice-recommendations

upvoted 2 times

wardy1983 1 year, 7 months ago

Box1: VM1 and VM2 access to st1 - User-assigned managed identity

Requirement: Configure a shared identity for VM1 and VM2 to access st1

We have to create a User-assigned managed identity to be shared with VM1 and VM2

Box2: App1 access to Vault1 - System-assigned managed identity

upvoted 1 times

heatfan900 1 year, 10 months ago

for VM1 and 2 the USER-ASSIGNED MI is needed so that it can be shared between the two as per the requirement.

for the App the SYSTEM-ASSIGNED MI will suffice as only that one app requires access to the Key Vault, therefore, the S-A MI works ok for this example.

upvoted 2 times

Ario 1 year, 12 months ago

we can use both managed identity ofc , but if you just consider the question carefully state :The solution must minimize administrative effort ! no doubt system-assigned has less effort

upvoted 1 times

_fvt 1 year, 10 months ago

"Configure a shared identity for VM1 and VM2 to access st1" if you really consider the question.

So

1. User-assigned managed identity
2. System-assigned managed identity

upvoted 1 times

_fvt 1 year, 10 months ago

You cannot share a System-assigned managed identity

upvoted 1 times

Bryan09 2 years, 1 month ago

For a VM that needs access to a storage account, you can use a system-assigned managed identity or a user-assigned managed identity.

A system-assigned managed identity is a managed identity that is automatically created by Azure for an Azure resource during resource creation. When you enable a system-assigned managed identity on a VM, Azure creates an identity for the VM in the Azure AD tenant that's trusted by the subscription of the VM. You can then use this identity to authenticate to Azure services like storage accounts.

A user-assigned managed identity is a standalone Azure resource that you create and assign to a VM. You can then use this identity to authenticate to Azure services like storage accounts. The main advantage of a user-assigned managed identity is that it can be reused across multiple VMs or other Azure resources.

upvoted 2 times

zellck 2 years, 2 months ago

1. System-assigned managed identity
2. User-assigned managed identity

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#managed-identity-types

There are two types of managed identities:

- System-assigned. Some Azure resources, such as virtual machines allow you to enable a managed identity directly on the resource.
- User-assigned. You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more Azure Resources.

upvoted 2 times

zellck 2 years, 2 months ago

Sorry, typo. Should be:

1. User-assigned managed identity
2. System-assigned managed identity

upvoted 9 times

obaali1990 2 years, 2 months ago

The correct answers should be:

Box 1: User-assigned managed Identity

Box 2: System-assigned Managed identity

upvoted 2 times

ConanBarb 2 years, 3 months ago

Box 1: User-assigned MI (as it will be reused for two VMs and thus minimize admin effort)

Box 2: User account (note that nothing says App1 is an Azure service (Web App, Function, Logic App, VM, container etc), it could be any app on-prem or other hosting, and therefor it would need an App Registration and a user account with Delegated or Application access)

There are a few other questions that refer to "a deployed app" where the equivalent reasoning is applied leading to App Registration etc)

upvoted 2 times

majstor86 2 years, 3 months ago

VM1 and VM2 access to st1 - User-assigned managed identity

App1 access to Vault1 - System-assigned managed identity

upvoted 4 times

Nick66 2 years, 5 months ago

Configure a shared identity for VM1 and VM2 to access st1: should be a User-assigned managed identity

upvoted 5 times

Question #90 *Topic 2*

You have an Azure AD tenant. The tenant contains users that are assigned Azure AD Premium P2 licenses.

You have a partner company that has a domain named fabrikam.com. The fabrikam.com domain contains a user named User1. User1 has an email address of user1@fabrikam.com

You need to provide User1 with access to the resources in the tenant. The solution must meet the following requirements:

• User1 must be able to sign in by using the user1@fabrikam.com credentials.
• You must be able to grant User1 access to the resources in the tenant.
• Administrative effort must be minimized.

What should you do?

A. Create a user account for User1.

B. To the tenant, add fabrikam.com as a custom domain.

C. Create an invite for User1.

D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

Suggested Answer: *C*

Community vote distribution

C (100%)

OrangeSG Highly Voted 2 years, 5 months ago

Selected Answer: C

You should create an invite for User1 to join your Azure AD tenant as a guest user. This will allow him to sign in with his existing credentials (user1@fabrikam.com), and you can then grant him access to the resources in the tenant. This option also minimizes administrative effort as it is a simple process to invite a guest user.

upvoted 11 times

8de3321 Most Recent 7 months ago

Selected Answer: B

I believe I saw this question somewhere else and the answer was to create a custom domain. I am not sure myself. Can someone so sure the answer is C, please explain why option B would not be the answer?.

upvoted 1 times

Ivan80 1 year, 5 months ago

In exam 1/28/24

upvoted 2 times

ESAJRR 1 year, 11 months ago

Selected Answer: C

C. Create an invite for User1.

upvoted 1 times

zellck 2 years, 2 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-overview#b2b-collaboration
With B2B collaboration, you can invite anyone to sign in to your Azure AD organization using their own credentials so they can access the apps and resources you want to share with them. Use B2B collaboration when you need to let external users access your Office 365 apps, software-as-a-service (SaaS) apps, and line-of-business applications, especially when the partner doesn't use Azure AD or it's impractical for administrators to set up a mutual connection through B2B direct connect. There are no credentials associated with B2B collaboration users. Instead, they authenticate with their home organization or identity provider, and then your organization checks the guest user's eligibility for B2B collaboration.

upvoted 4 times

[Removed] 2 years, 3 months ago

Looks like b2b collaboration: https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-overview

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: C

C. Create an invite for User1

upvoted 1 times

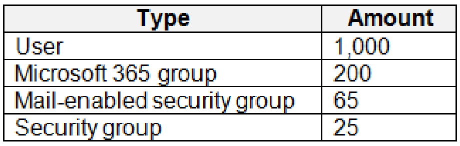
Ajdlfasudfo0 2 years, 5 months ago

correct, you invite the external user to your tenant.

upvoted 2 times

Question #91 Topic 2

You have an Azure AD tenant that contains the identities shown in the following table.



Type	Amount
User	1,000
Microsoft 365 group	200
Mail-enabled security group	65
Security group	25

You plan to implement Azure AD Identity Protection.

What is the maximum number of user risk policies you can configure?

A. 1

B. 90

C. 200

D. 265

E. 1000

Suggested Answer: *D*

Community vote distribution

A (82%) C (18%)

Seelearndo Highly Voted 2 years, 5 months ago

Selected Answer: A

You can only configure one user risk policy per tenant.

https://janbakker.tech/microsoft-secure-score-series-11-turn-on-user-risk-policy/#:~:text=You%20can%20only%20configure%20one%20user%20risk%20policy%20per%20tenant.

upvoted 27 times

ITSavy Highly Voted 2 years, 4 months ago

Selected Answer: C

correct answer is C - 200

The maximum number of user risk policies you can configure in Azure AD Identity Protection depends on your Azure AD Premium license plan. According to Microsoft documentation, the number of user risk policies that can be configured varies between different Azure AD Premium license plans.

For the Azure AD Premium P1 license plan, you can configure up to 90 user risk policies.
For the Azure AD Premium P2 license plan, you can configure up to 200 user risk policies.

It's not specified in the Microsoft documentation if there's a plan that allows for 256 user risk policies.

upvoted 8 times

chikorita 2 years, 4 months ago

AD licensce plan is not specified

upvoted 2 times

ConanBarb 2 years, 3 months ago

Sure, Identity Protection is in P2 only

upvoted 1 times

khamrumunnu Most Recent 1 month, 1 week ago

Selected Answer: A

Answer : A

You can only configure a single User Risk Policy per tenant.

upvoted 1 times

Nhadipour 4 months, 3 weeks ago

Selected Answer: A

Azure AD Identity Protection allows only ONE (1) user risk policy per tenant

upvoted 1 times

ITFranz 5 months, 4 weeks ago

Selected Answer: C

Maybe the question is trying to state the Minimum user risk policy.
there is no specific mention of a minimum number of user risk policies that can be configured in a tenant. However, we can infer that the minimum number is 1, as Azure AD Identity Protection allows administrators to configure user risk policies to protect against identity-based risks. Also, There is no specific limit mentioned for the number of user risk policies you can configure in Azure AD Identity Protection. However, user risk policies are implemented as Conditional Access policies in Azure AD, and there is a limit of 195 Conditional Access policies per tenant

upvoted 1 times

8de3321 7 months ago

Selected Answer: A

I am pretty sure I read about this on the learn.microsoft page. I simply don't remember what the number was exactly. I am trying to find the page and the link but failing.

upvoted 1 times

Hot_156 6 months, 1 week ago

Copilot says it is 90

upvoted 1 times

Atilgen 1 year, 1 month ago

You can only create 1 user risk policy, it goes for the entire tenant.

upvoted 2 times

Apptech 1 year, 3 months ago

User risk policy is set up in Azure AD --> user risk policy under section "protect". You only can set up 1 policy. Check by yourself. MS recommends migrating user risk policy to conditional access for more conditions and controls. Question asks for User risk policy and not for Conditional access policy. Answer definetely is 1

upvoted 3 times

Obama_boy 1 year, 6 months ago

Selected Answer: A

in exam 08/12/23

upvoted 1 times

Jinkx 1 year, 6 months ago

Selected Answer: A

In the given scenario:

The total number of licensed users (User type) is 1,000.
Given the minimum of 500 licensed users for policy calculation, you can calculate the maximum number of user risk policies using the following formula:

Maximum User Risk Policies
=
(
Total Licensed Users
10
,
000
)
×
100
Maximum User Risk Policies=(
10,000
Total Licensed Users

)×100

Maximum User Risk Policies
=
(
1
,
000
10
,
000
)
×
100
=
10
Maximum User Risk Policies=(
10,000
1,000

)×100=10

Therefore, the maximum number of user risk policies you can configure is 10.

So, the correct answer is:

A. 1
upvoted 2 times

⊟ **Slawekyo** 1 year, 1 month ago
Are you on drugs?
upvoted 9 times

⊟ **8de3321** 7 months ago
I can't believe I am writing the same exam as him. Who knows this bro could end up being my colleague.
upvoted 4 times

⊟ **wardy1983** 1 year, 7 months ago
Answer: A
Explanation:
You can only configure one user risk policy per tenant.
https://janbakker.tech/microsoft-secure-score-series-11-turn-on-user-riskpolicy/#:~:
text=You%20can%20only%20configure%20one%20user%20risk%20policy%20per%20tenant.
upvoted 2 times

⊟ **Pixan** 1 year, 7 months ago
Hi Everyone!!
Join ET and get actual and valid study material: https://examstopics.quora.com/ and pass your exam in first attempt. Study Smart Not Hard
upvoted 1 times

⊟ **TheProfessor** 1 year, 7 months ago
Correct answer is - A maximum of 195 policies can be created in a single Microsoft Entra organization (tenant).

https://learn.microsoft.com/en-us/entra/identity/users/directory-service-limits-restrictions
upvoted 1 times

⊟ **bob_sez** 1 year, 7 months ago
They are not talking about conditional access policy but Identity Protection
upvoted 1 times

⊟ **ServerBrain** 1 year, 11 months ago
Selected Answer: A

Logic says one policy for all users...

Imagine creating 90 or more policies, ridiculous..

upvoted 1 times

Happyme77 2 years, 1 month ago

Selected Anser : A. single user can create a maximum of 200 directories not 200 risk policies. Answer is 1.

upvoted 1 times

Alexbz 2 years, 2 months ago

Selected Answer: A

While Identity Protection also provides two risk policies with limited conditions, we highly recommend setting up risk-based policies in Conditional Access.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#migrate-risk-policies-from-identity-protection-to-conditional-access

upvoted 1 times

zellck 2 years, 2 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa#overview-of-azure-ad-identity-protection

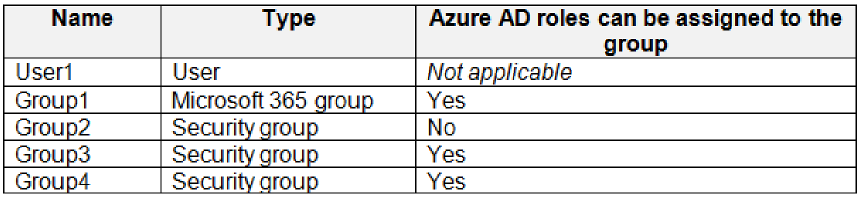
The following three policies are available in Azure AD Identity Protection to protect users and respond to suspicious activity. You can choose to turn the policy enforcement on or off, select users or groups for the policy to apply to, and decide if you want to block access at sign-in or prompt for additional action.

- User risk policy
- Sign in risk policy
- MFA registration policy

upvoted 4 times

Question #92 Topic 2

You have an Azure subscription that contains a resource group named RG1 and the identities shown in the following table.



Name	Type	Azure AD roles can be assigned to the group
User1	User	*Not applicable*
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1.

Which identities can you add to Group4 as members?

A. User1 only

B. User1 and Group3 only

C. User1, Group1, and Group3 only

D. User1, Group2, and Group3 only

E. User1, Group1, Group2, and Group3

Suggested Answer: *B*

Community vote distribution

A (73%) 13% 13%

⊟ **OrangeSG** Highly Voted 2 years, 5 months ago

Selected Answer: A

This exam question test about role-assignable group feature in Azure Active Directory.
Refer to Microsoft document on role-assignable group: “Group nesting is not supported. A group can't be added as a member of a role-assignable group.”

Reference
Create a role-assignable group in Azure Active Directory
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible

Use Azure AD groups to manage role assignments
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept
upvoted 24 times

⊟ **basak** 1 year, 10 months ago

if 2 security groups - for example, group parent has assigned role app developer and group child has no role assigned.
in this case you can't add child as a member of parent. since child has no role assigned you can add group parent inside group child.
upvoted 2 times

⊟ **km_2022** Highly Voted 2 years, 3 months ago

Selected Answer: A

Answer Is A.

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/azure/active-directory/roles/groups-concept
upvoted 11 times

⊟ **mmmyo** 1 month, 2 weeks ago

For the security group type, you can add an existing group to another group (also known as nested groups). https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups#add-a-group-to-another-group
upvoted 1 times

mmmyo Most Recent 1 month, 3 weeks ago

Selected Answer: D

User1 ✅ (Users can be members of any security group)

Group2 (Security Group - Cannot be assigned Azure AD roles) ✅ (Even though Group2 cannot be assigned roles itself, it can still be a member of another group.)

Group3 (Security Group - Can be assigned Azure AD roles) ✅ (Security groups that can be assigned roles can also be added to other groups.)

❌ Group1 (Microsoft 365 Group - Can be assigned Azure AD roles)

Microsoft 365 groups cannot be members of security groups in Azure AD.

upvoted 2 times

ITFranz 5 months, 4 weeks ago

Selected Answer: A

It seems that things have changed.

group nesting is supported for security groups in Azure, but with some limitations:

1. Security groups can be nested within other security groups.
2. Nesting is not supported for all scenarios. For example, it's not supported for application access.
3. You can create dynamic groups that include members of other security groups using the 'memberOf' attribute.
4. There are restrictions on nesting:

• You can't add security groups to Microsoft 365 groups.

• You can't add Microsoft 365 groups to security groups or other Microsoft 365 groups.

• You can't add distribution groups in nesting scenarios.

• You can't add security groups as members of mail-enabled security groups

upvoted 2 times

Hot_156 3 months, 3 weeks ago

IMPORTANT!!!! It is about Azure Roles and not Azure AD Roles!

I did LAB, and I can add all the security groups but the M365.

The answer should be "D"

upvoted 2 times

Hot_156 3 months, 2 weeks ago

I was WRONG! It is just user1

upvoted 1 times

schpeter_091 7 months, 1 week ago

user 1 only - made a quick test in lab with the following outcome:

user1- can be added

group1 - it says, MS 365 groups are not allowed

group2 - does not even appear in the list when i wanted to add into group4

group3 - can be selected to add, but it gives the message: group nesting not supported

upvoted 1 times

Jimmy500 1 year ago

First, we can not add Microsoft365 group into Security group, we can skip Group1. Nesting is not supported for Role Assignable groups it means if group is role assignable, we cannot add any group there, so we need to skip other groups as well. We can only keep User1.

upvoted 2 times

bxlin 1 year, 1 month ago

Only User1 and Group2 can be added to Group4.

Note: Nesting is currently not supported for groups that can be assigned to a role. Hence not Group 1 and 3.

upvoted 3 times

JaridB 1 year ago

that is correct but unfortunately that is not an option.

Role-assignable groups cannot be nested within other role-assignable groups. This means you cannot add a role-assignable Microsoft 365 group to another role-assignable group.

Suppose you have two role-assignable groups: Group A and Group B. Group A cannot be added as a member of Group B if both are role-assignable.

upvoted 2 times

Nava702 1 year, 3 months ago

Selected Answer: A

A. User 1 only.

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

upvoted 2 times

Jarid 1 year, 3 months ago

The question asks which identities can be added to Group4 as members. The table shows the following information about the relevant groups:

Group1: Microsoft 365 group - Azure AD roles can be assigned to the group. This means Group1 itself can be assigned roles, but users cannot be directly added to it.

Group2: Security group - No - Azure AD roles cannot be assigned to this group, and users cannot be directly added to it.

Group3: Security group - Yes - Azure AD roles can be assigned to this group, and users can be added as members.

Group4: Security group - Yes - Azure AD roles can be assigned to this group, and users can be added as members.

Since Group1 and Group2 cannot have users added directly as members, they are not valid options. User1 and Group3 can be added to Group4 because they are both security groups that allow adding members.

upvoted 1 times

Mnguyen0503 1 year, 5 months ago

Selected Answer: A

Tested in lab. When trying to add a Security group with Azure AD roles assigned, I got this error: Failed to add group member. Nesting is currently not supported for groups that can be assigned to a role.

Those that claimed to have tested in lab, you might want test twice before posting ...

upvoted 2 times

NICKTON81 1 year, 5 months ago

B is okay;

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-assign-role?tabs=ms-powershell

upvoted 1 times

[Removed] 1 year, 6 months ago

Contributor is an RBAC role if it was Azure AD role then nested group are not allowed

upvoted 1 times

[Removed] 1 year, 6 months ago

User1,Group2,Group3 only M365 cannot be nested

upvoted 1 times

[Removed] 1 year, 6 months ago

Tested in the Lab

upvoted 1 times

Obama_boy 1 year, 6 months ago

Selected Answer: D

The correct answer is:

D. User1, Group2, and Group3 only.

Reasoning:

User1 is an individual user and can be added to security groups without restrictions.

Group2 is a security group, and security groups can be nested within other security groups in Azure AD.

Group3 is also a security group and can be nested as well.

Group1 is a Microsoft 365 group which cannot be nested within other security groups, hence it cannot be added to Group4.

Azure AD roles assigned to the group are irrelevant in the context of which members can be added to Group4. The key factor is whether the type of identity (user or group) can be nested within another group.

upvoted 4 times

flafernan 1 year, 6 months ago

Selected Answer: E

The question was: "What identities can you add to Group4 as members?" At no point is there any talk of assigning inherited functions between groups. Therefore, the answer is the letter:

E. User1, Group1, Group2 and Group3.

upvoted 1 times

⊟ **wardy1983** 1 year, 7 months ago

Answer: A

Explanation:

This exam question test about role-assignable group feature in Azure Active Directory.

Refer to Microsoft document on role-assignable group: “Group nesting is not supported. A group can't be added as a member of a role-assignable group.”

Reference

Create a role-assignable group in Azure Active Directory

https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible

Use Azure AD groups to manage role assignments

https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept

upvoted 1 times

⊟ **wardy1983** 1 year, 8 months ago

This exam question test about role-assignable group feature in Azure Active Directory.

Refer to Microsoft document on role-assignable group: “Group nesting is not supported. A group can't be added as a member of a role-assignable group.”

upvoted 2 times

Question #93 *Topic 2*

HOTSPOT

-

You have an Azure subscription that contains a storage account named contoso2023.

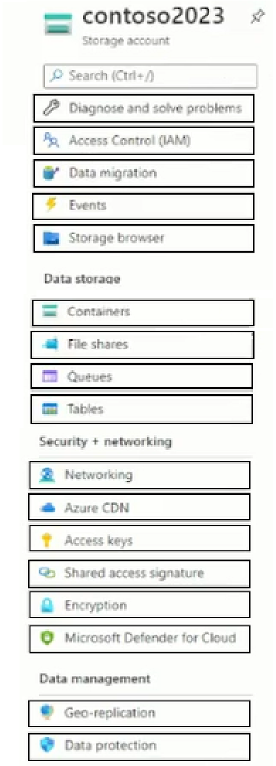
You need to perform the following tasks:

• Verify that identity-based authentication over SMB is enabled.
• Only grant users access to contoso2023 in the year 2023.

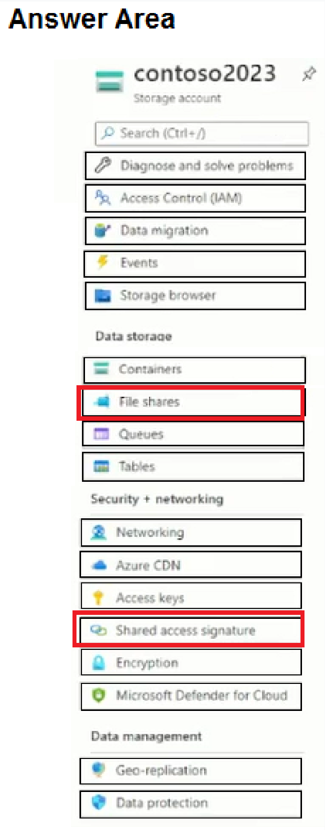
Which two settings should you use? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



Answer Area

contoso2023
Storage account

Search (Ctrl+/)

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Azure CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Geo-replication

Data protection

AzureJobsTillRetire Highly Voted 2 years, 5 months ago

The given answers are correct.

1. File Shares

Requirement: Verify that identity-based authentication over SMB is enabled

Go there to configure Identity-based authentication (Active Directory) for Azure file shares.

Ref: https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview

2. Share access signature

Requirement: Only grant users access to contoso2023 in the year 2023

upvoted 15 times

majstor86 Highly Voted 2 years, 3 months ago

1. File Shares

2. Share access signature

upvoted 9 times

pentium75 Most Recent 11 months ago

Question is weird but stil:

"SMB" is related to File Shares so File Shares.

"Only access in the year 2023" is only doable with SAS so this

upvoted 1 times

Andy_S 1 year, 7 months ago

Something wrong is in this question. File Share (SMB) does not support SAS authentication. Instead it is clearly written we can map FS using Storage Account Key or by Kerberos (ADDS and/OR AAD DS)

upvoted 1 times

heatfan900 1 year, 10 months ago

FILE SHARES WHICH FACILITATE SMB CONNECTIVITY.

SAS WHICH ALLOWS FOR SPECIFICITY WHEN IT COMES TO ACCESSIBILITY OF THE STORAGE ACCOUNT.

upvoted 3 times

zellck 2 years, 2 months ago

1. File shares

2. Shared access signature (SAS)

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview
This article explains how Azure file shares can use domain services, either on-premises or in Azure, to support identity-based access to Azure file shares over SMB. Enabling identity-based access for your Azure file shares allows you to replace existing file servers with Azure file shares without replacing your existing directory service, maintaining seamless user access to shares.

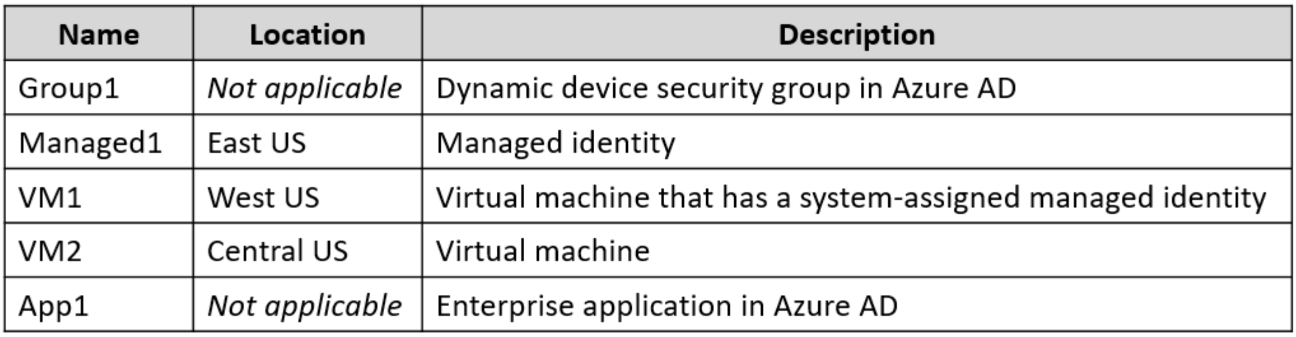
https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview
A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:
- What resources the client may access.
- What permissions they have to those resources.
- How long the SAS is valid.
upvoted 6 times

ZakySama 2 years, 2 months ago
Answers are correct
upvoted 2 times

ligu 2 years, 4 months ago
Answer is correct
upvoted 2 times

Question #94 Topic 2

You have an Azure subscription that is linked to an Azure AD tenant and contains the resources shown in the following table.



Name	Location	Description
Group1	*Not applicable*	Dynamic device security group in Azure AD
Managed1	East US	Managed identity
VM1	West US	Virtual machine that has a system-assigned managed identity
VM2	Central US	Virtual machine
App1	*Not applicable*	Enterprise application in Azure AD

Which resources can be assigned the Contributor role for VM1?

A. Managed1 and App1 only

B. Group1 and Managed1 only

C. Group1, Managed1, and VM2 only

D. Group1, Managed1, VM1, and App1 only

Suggested Answer: *A*

Community vote distribution

A (72%) D (28%)

973b658 Highly Voted 2 years, 1 month ago

D.
https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps
"You can assign a role to a user, group, service principal, or managed identity. "

App1 has service principal.
https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

upvoted 15 times

basak 1 year, 10 months ago

Tested. D is correct.

upvoted 3 times

liorh 2 years ago

looks correct to me

upvoted 1 times

Franc_Coetzee 2 years ago

The keyword for the Group is "Dynamic", once you make any group a dynamic group, the option to assign roles to it becomes grayed out.

upvoted 12 times

pentium75 11 months ago

"Role-assignable groups" are about Azure AD roles, not Azure RBAC roles.

upvoted 1 times

bxlin 1 year, 1 month ago

that is not true. you can assign role to a dynamic group

upvoted 1 times

OrangeSG Highly Voted 1 year, 8 months ago

Selected Answer: A

The Contributor role can be assigned to any Azure resource, including users, groups, service principals, and managed identities.

• Group1 is a dynamic device security group in Azure AD. Dynamic groups are not role-assignable, so Group1 cannot be assigned the Contributor role for VM1.

• Managed1 is a managed identity. Managed identities can be assigned the Contributor role for VM1.

• VM1 is a virtual machine. Virtual machines can be assigned the Contributor role for themselves.

• App1 is an enterprise application in Azure AD. Enterprise applications can be assigned the Contributor role for VM1.

Therefore, the only resources that can be assigned the Contributor role for VM1 are Managed1, VM1, and App1.

upvoted 10 times

cuongdo1793 Most Recent 1 month ago

Selected Answer: A

✕ Why D. Group1, Managed1, VM1, and App1 only is incorrect:

Group1 is a dynamic device group, which can't be used as a principal in RBAC role assignment.

VM1 is a resource, not a principal you assign roles to — it's the target of the role assignment. A. Managed1 and App1 only is still the correct choice.

upvoted 1 times

JBAnalyst 6 months, 3 weeks ago

Selected Answer: A

You can't assign RBAC to a "dynamic" group type which is what group 1 is

All answers that have group 1 is automatically wrong

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept

upvoted 2 times

8de3321 7 months ago

Selected Answer: D

I wish this website gave answers instead of making people fight over the options and confuse people trying to write the exam. I paid for this service and this is what I am presented with. What is this exam, if people cannot find the proper answer on the Microsoft website even with access and then expects people to do it under time pressure with very minimal access? This is insane. If this was the exam I would choose option D or something because I don't think Microsoft would make the question too easy to find with the method of elimination.

upvoted 3 times

fenth7 7 months ago

Selected Answer: D

d is correct

upvoted 2 times

pentium75 11 months ago

Selected Answer: D

This is about an Azure RBAC role, not an Entra ID role. Thus everything, except for VM2 which doesn't have a managed identity, can get it assigned.

upvoted 2 times

ACSC 1 year, 3 months ago

Selected Answer: D

Tested for user, group, VM and App. All of them can be assigned Contributor role for VM.

upvoted 2 times

cris_exam 1 year, 5 months ago

This question is weird, because it should have a choice for: Managed ID, App1 and VM.

Dynamic Entra Sec Groups cannot have roles assigned, all the other can have.

The closet answer to truth is A.

upvoted 1 times

[Removed] 1 year, 6 months ago

Difference between Azure AD roles and Azure RBAC is as follows:

RBAC can have a User, group, or service principal, Managed identity (group nesting is allowed and the group can dynamic as well

Azure AD roles only users and groups (group nesting is not allowed as soon as you enable entra roles can be enabled the membership type greys out to assign and group nesting is not allowed.

Here contributor is a RBAC role not azure ad role

upvoted 1 times

WilianCArias 1 year, 6 months ago

D.

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps

"You can assign a role to a user, group, service principal, or managed identity. "

upvoted 2 times

⊟ 👤 **ManiMessner** 1 year, 7 months ago

Selected Answer: D

Tested, D is correct

upvoted 4 times

⊟ 👤 **rosef** 1 year, 7 months ago

Selected Answer: A

Tested. When creating a group, if you choose dynamic user "Microsoft Entra roles can be assigned to the group" option turns to NO automatically. So when you eliminate group1, answer is A.

upvoted 3 times

⊟ 👤 **xRiot007** 11 months, 2 weeks ago

Microsoft Entra roles and RBAC roles are 2 different things.

upvoted 2 times

⊟ 👤 **wardy1983** 1 year, 7 months ago

Answer: D

Explanation:

Confirmed in my lab. I think VM1 in D should change to VM2 though.

upvoted 1 times

⊟ 👤 **ErikPJordan** 1 year, 9 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

⊟ 👤 **InnoMaf** 1 year, 9 months ago

Correct answer is A

role-assignable groups is limited to AD Azure roles

https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#restrictions-for-role-assignable-groups

upvoted 2 times

⊟ 👤 **pentium75** 11 months ago

"Role-assignable groups" are about Entra roles, not Azure roles.

upvoted 1 times

⊟ 👤 **vcloudpmp** 1 year, 10 months ago

https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept

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

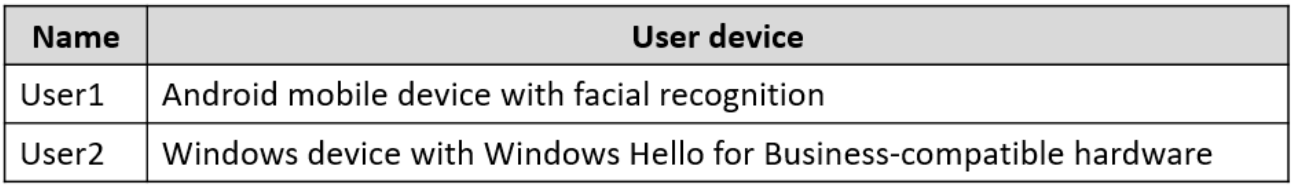
upvoted 2 times

Question #95 Topic 2

DRAG DROP

-

You have an Azure AD tenant that contains the users shown in the following table.

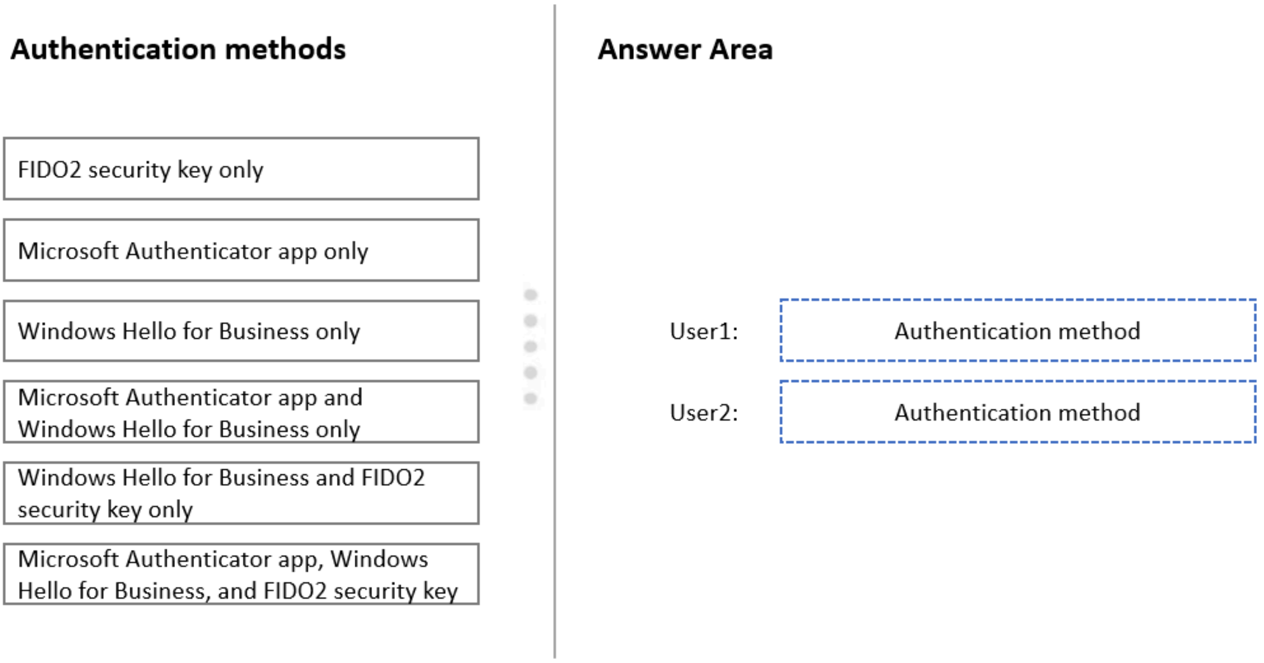


Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Authentication methods

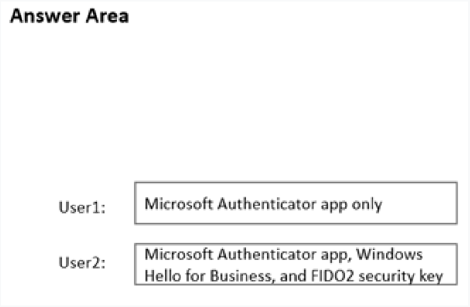
- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1: Authentication method

User2: Authentication method

Suggested Answer:



Answer Area

User1: Microsoft Authenticator app only

User2: Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

ITTesters Highly Voted 1 year, 12 months ago

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#choose-a-passwordless-method

Assigned Windows 10 device: Windows Hello for Business and/or FIDO2 security key

Mobile or non-windows device: Passwordless sign-in with the Authenticator app

upvoted 14 times

⊟ **yonie** 1 year, 6 months ago

Exactly.

Why are we adding Windows: MS authenticator to User 2?

upvoted 2 times

⊟ **petrus** Highly Voted 2 years ago

Correct

Android: MS authenticator

Windows: MS authenticator, Hello for Business, FIDO2 key

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

upvoted 11 times

⊟ **ca7859c** Most Recent 1 month ago

Answer is correct

upvoted 1 times

⊟ **91743b3** 10 months, 3 weeks ago

On exam Aug 06 2024

upvoted 2 times

⊟ **pentium75** 11 months ago

Answers seem correct.

On Android, FIDO2 key and Hello are not supported, leave only Authenticator.

On Windows, user can use Hello (the device does support that), OR he can use FIDO2 key, OR he can use Authenticator (on his phone).

upvoted 3 times

⊟ **Koekjesdoos_111** 9 months, 2 weeks ago

Who says user 2 has a phone ?

upvoted 3 times

⊟ **brooklyn510** 1 year, 5 months ago

On exam 1/2/24

upvoted 3 times

⊟ **[Removed]** 1 year, 6 months ago

Persona Scenario Environment Passwordless technology

Admin Secure access to a device for management tasks Assigned Windows 10 device Windows Hello for Business and/or FIDO2 security key

Admin Management tasks on non-Windows devices Mobile or non-windows device Passwordless sign-in with the Authenticator app

Information worker Productivity work Assigned Windows 10 device Windows Hello for Business and/or FIDO2 security key

Information worker Productivity work Mobile or non-windows device Passwordless sign-in with the Authenticator app

Frontline worker Kiosks in a factory, plant, retail, or data entry Shared Windows 10 devices FIDO2 Security keys

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

Using this table User1 is MS Autheticator

User 2 Windows Hello for Business and/or FIDO2 security key

upvoted 2 times

⊟ **zied01** 1 year, 7 months ago

With web sign in windows (new feature) you can sign in with ms authenticator app

The question are updated with new features, exp

A question for verified id

So i think the answers are correct

upvoted 1 times

⊟ **just_nuno** 1 year, 9 months ago

Answer is not correct. To have MS authenticator, Hello for Business, FIDO2 key a Windows device is obviously not enough. Also need to have a Fido Key and a mobile.

upvoted 2 times

⊟ **Self_Study** 1 year, 10 months ago

On exam 7/8/23. Answers are correct. The devices were twisted.

upvoted 4 times

⊟ **ITTesters** 1 year, 12 months ago

Why is the MS Authenticator app listed for User2?
He does not have a mobile device, only a Windows device with HFB.
upvoted 4 times

⊟ **_fvt** 1 year, 11 months ago
I'm not sure too, but in facts you can use MS Authenticator (from an Android/iOS device) to passwordless logon on your windows device. It's like it's not specified that the user have a Fido key or not, but if he has one, he can use it. Same for the mobile device I guess.
upvoted 4 times

⊟ **Pupu86** 2 years ago
MS authenticator is for IOS/Android devices

MS Hello only works with laptops/desktops with compatible hardware for Hello Business so simply means only new devices allow the use of Hello Business and its not backward-compatible

FIDO2 Key is only when user doesn't IOS/Android phones/devices, laptops, desktops
upvoted 1 times

⊟ **liorh** 2 years, 1 month ago
what is the correct answer?
upvoted 1 times

⊟ **billo79152718** 2 years, 1 month ago
Correct
upvoted 4 times

Question #96 *Topic 2*

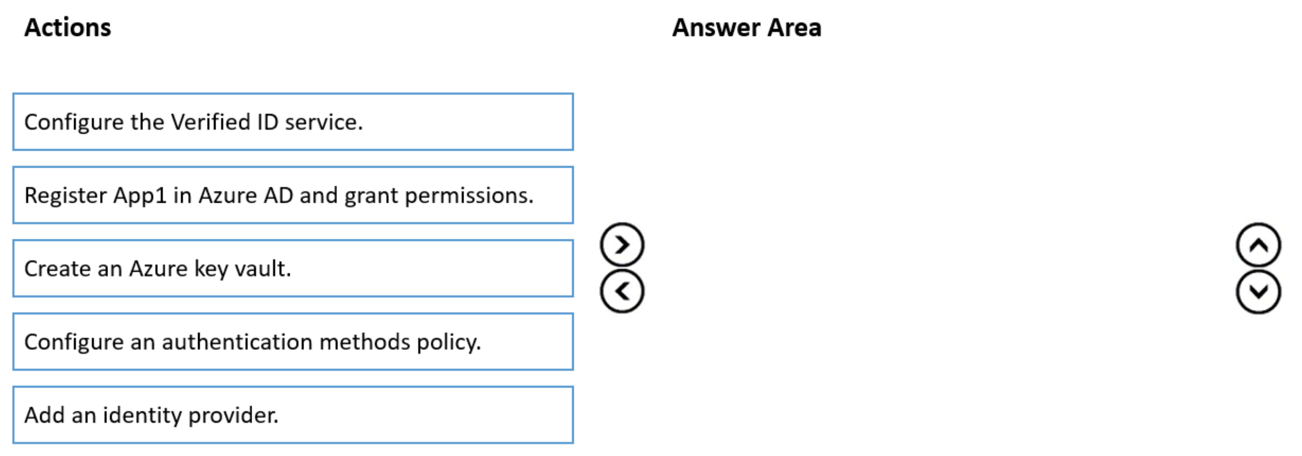
DRAG DROP

-

You have an Azure AD tenant and an application named App1.

You need to ensure that App1 can use Microsoft Entra Verified ID to verify credentials.

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

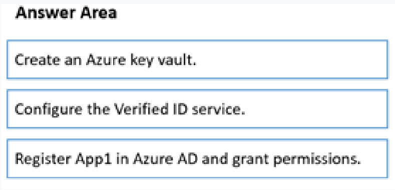


Actions

- Configure the Verified ID service.
- Register App1 in Azure AD and grant permissions.
- Create an Azure key vault.
- Configure an authentication methods policy.
- Add an identity provider.

Answer Area

Suggested Answer:



Answer Area

- Create an Azure key vault.
- Configure the Verified ID service.
- Register App1 in Azure AD and grant permissions.

billo79152718 Highly Voted 2 years, 1 month ago

Given answers is correct.

https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

upvoted 15 times

Pupu86 Highly Voted 2 years ago

Answer is correct

https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

upvoted 7 times

91743b3 Most Recent 10 months, 3 weeks ago

There was a new questions similar to this but with different answer choices on exam Aug 06 2024. It asked what are the three steps to configure Microsoft Entra Verified ID in your org.

upvoted 6 times

cris_exam 1 year, 5 months ago

Correct, given answer.

Create an Azure Key Vault instance.
Configure the Verified ID service using the manual setup.
Register an application in Microsoft Entra ID.

https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant

upvoted 2 times

Question #97 *Topic 2*

DRAG DROP

-

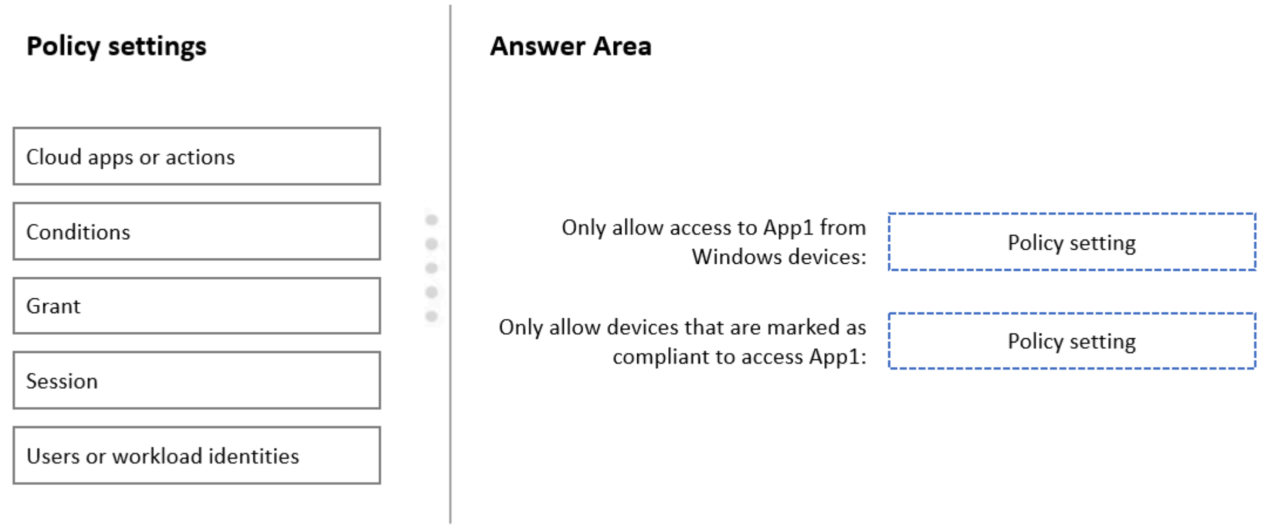
You have an Azure subscription that contains an Azure web app named App1.

You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:

• Only allow access to App1 from Windows devices.
• Only allow devices that are marked as compliant to access App1.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting 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.



Policy settings

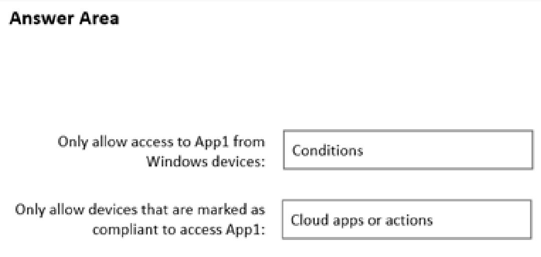
- Cloud apps or actions
- Conditions
- Grant
- Session
- Users or workload identities

Answer Area

Only allow access to App1 from Windows devices: Policy setting

Only allow devices that are marked as compliant to access App1: Policy setting

Suggested Answer:



Answer Area

Only allow access to App1 from Windows devices: Conditions

Only allow devices that are marked as compliant to access App1: Cloud apps or actions

⊟ **liorh** Highly Voted 👍 2 years, 1 month ago

1:conditions

2:grant

tested in lab for 10000%

upvoted 42 times

⊟ **basak** 1 year, 10 months ago

correct

upvoted 1 times

⊟ **Self_Study** Highly Voted 👍 1 year, 10 months ago

On exam 7/8/23. Went with Conditions and Grant.

upvoted 10 times

⊟ **pentium75** Most Recent ⏲ 11 months ago

Conditions

Grant

upvoted 2 times

brooklyn510 1 year, 5 months ago

On exam 1/2/24

upvoted 4 times

Obama_boy 1 year, 6 months ago

For the scenario described, the correct Conditional Access policy settings would be:

Only allow access to App1 from Windows devices:

Policy Setting: Conditions -> Device platforms -> select Windows

Only allow devices that are marked as compliant to access App1:

Policy Setting: Grant -> Grant access -> Require device to be marked as compliant

These settings will ensure that only devices running Windows and marked as compliant can access the application, aligning with the described requirements.

upvoted 8 times

xRiot007 10 months, 1 week ago

Microsoft English is sometimes so broken. Should have called both Conditions because to require a device to be compliant is clearly a condition that needs to be satisfied.

upvoted 2 times

anjanc 6 months ago

Yes you're right

upvoted 1 times

wardy1983 1 year, 8 months ago

Conditions,

Grant,

Only allow access to App1 from Windows devices: Conditions Only allow devices that are marked as compliant

to access App1: Grant

upvoted 2 times

bsakabato 1 year, 10 months ago

2: Conditions is more suitable to allow access based on device compliance, versus grant that control authorization after access

Conditons can use the filter for device parameter with attribute device.isCompliant -eq "True"

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices

upvoted 2 times

ESAJRR 1 year, 10 months ago

1:conditions

2:grant

upvoted 1 times

heatfan900 1 year, 10 months ago

CONDITIONS = only allowing access to the app based on the condition your device runs Windows

GRANT = Only granting access to the App, after logging into the device, by ensuring the device is compliant with the policy

upvoted 1 times

yanaginagi 1 year, 10 months ago

1: conditions

2: grant

tested!

upvoted 3 times

973b658 2 years, 1 month ago

OK

1

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-platforms

2

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant

upvoted 2 times

⊟ **973b658** 2 years, 1 month ago

not

1:conditions

2:grant

upvoted 1 times

⊟ **nazimb** 2 years, 1 month ago

1-Condition

2-Grant

upvoted 3 times

⊟ **billo79152718** 2 years, 1 month ago

Tested in lab.

Only allow access to App1 from Windows devices: Conditions

Only allow devices that are marked as compliant to access App1: Gran

upvoted 4 times

⊟ **billo79152718** 2 years, 1 month ago

Mistyped NOT Gran, but Grant *

upvoted 3 times

Question #98 *Topic 2*

You have an Azure subscription that contains a web app named App1.

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1.

You need to add Google as an identity provider in Azure AD.

Which two pieces of information should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a client ID

B. a tenant name

C. the endpoint URL of an application

D. a tenant ID

E. a client secret

Suggested Answer: *AE*

Community vote distribution

AE (94%) 6%

brooklyn510 Highly Voted 11 months, 4 weeks ago

On exam 1/2/24

upvoted 5 times

Rjaesh Most Recent 7 months, 1 week ago

Azure portal - Choose tenant (if multiple tenant) --> external identity --> Set up identity providers --> Google --> Client Id and Client secret

upvoted 2 times

ndv4461 10 months, 3 weeks ago

Client ID: This is a unique identifier provided by Google when you register your application with the Google identity provider.

Client Secret: This is a secret key provided by Google when you register your application with the Google identity provider.

upvoted 4 times

Ivan80 11 months ago

In exam 1/28/24

upvoted 3 times

yonie 1 year ago

Selected Answer: AE

Enter the client ID and client secret you obtained earlier

https://learn.microsoft.com/en-us/entra/external-id/google-federation#step-2-configure-google-federation-in-microsoft-entra-external-id

upvoted 3 times

[Removed] 1 year ago

Configure Google as an identity provider

Sign in to the Azure portal as the global administrator of your Azure AD B2C tenant.

If you have access to multiple tenants, select the Settings icon in the top menu to switch to your Azure AD B2C tenant from the Directories + subscriptions menu.

Choose All services in the top-left corner of the Azure portal, search for and select Azure AD B2C.

Select Identity providers, then select Google.

Enter a Name. For example, Google.

For the Client ID, enter the Client ID of the Google application that you created earlier.

For the Client secret, enter the Client Secret that you recorded.

Select Save.

https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-google?pivots=b2c-user-flow

upvoted 3 times

OrangeSG 1 year, 2 months ago

Selected Answer: AE

To add Google as an identity provider in Azure AD, you should configure the following pieces of information:

A. a client ID: This is obtained from the Google Developers Console when you create a new project.

E. a client secret: This is also obtained from the Google Developers Console when you create a new project.

These two pieces of information are necessary to enable sign-in for users with a Google account1. The client ID and client secret are used by Azure AD to communicate with Google's authentication system.

Please note that while tenant name and tenant ID are important pieces of information in Azure AD, they are not specifically required to add Google as an identity provider1. The endpoint URL of an application is also not required for this specific task.

upvoted 3 times

Ario 1 year, 5 months ago

Selected Answer: AE

Client ID: This is a unique identifier provided by Google when you register your application with the Google identity provider.

Client Secret: This is a secret key provided by Google when you register your application with the Google identity provider.

Redirect URI: This is the URL that Azure AD will use to redirect users back to your application after authentication. since there is no redirect option here

upvoted 3 times

ghostme 1 year, 7 months ago

Selected Answer: AE

Configure Google as an identity provider :

https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-google?pivots=b2c-user-flow

or the Client ID, enter the Client ID of the Google application that you created earlier.

For the Client secret, enter the Client Secret that you recorded.

upvoted 3 times

Mannkoff 1 year, 7 months ago

Selected Answer: AE

Right Answer

upvoted 3 times

blueking 1 year, 7 months ago

AE

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/google-federation

upvoted 3 times

billo79152718 1 year, 7 months ago

Sorry first given answers is correct. ET please delete my 2 previous comments. :-(

A and E is correct.

upvoted 1 times

billo79152718 1 year, 7 months ago

Selected Answer: BD

Is correct

upvoted 1 times

billo79152718 1 year, 7 months ago

Selected Answer: AE

Given answers is correct.

upvoted 1 times

billo79152718 1 year, 7 months ago

Seems to be:

B. A tenant name

D. A tenant id

Sorry for my previous.

See link:

https://cloud.google.com/architecture/identity/federating-gcp-with-azure-ad-configuring-provisioning-and-single-sign-on

upvoted 1 times

Question #99 *Topic 2*

You have an Azure subscription that contains a user named User1.

You need to ensure that User1 can perform the following tasks:

- Create groups.
- Create access reviews for role-assignable groups.
- Assign Azure AD roles to groups.

The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Groups administrator

B. Authentication administrator

C. Identity Governance Administrator

D. Privileged role administrator

Suggested Answer: *D*

Community vote distribution

D (88%) 13%

golitech 4 months, 4 weeks ago

Selected Answer: A

B,C,D cannot create groups

upvoted 1 times

MohCert 10 months, 4 weeks ago

Selected Answer: D

Answer is D

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#privileged-role-administrator

None of the other three roles has the privileges to perform ALL mentioned tasks

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#identity-governance-administrator

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#authentication-administrator

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#groups-administrator

upvoted 3 times

cris_exam 11 months, 1 week ago

Selected Answer: D

tested and Privileged Role Admin was able to perform all required tasks.

upvoted 1 times

ndv4461 1 year ago

I think D is the correct answer.

upvoted 1 times

Obama_boy 1 year ago

Selected Answer: C

C. Identity Governance Administrator

The Identity Governance Administrator role in Azure AD is designed for managing identity governance features, including access reviews, entitlement management, and privileged identity management. This role allows a user to create and manage access reviews, which are used to govern group memberships and role assignments, including Azure AD roles for role-assignable groups.

Assigning User1 the Identity Governance Administrator role would allow them to perform the tasks mentioned (creating groups, creating access reviews for role-assignable groups, and assigning Azure AD roles to groups) while adhering to the principle of least privilege, as this role is specifically focused on governance features and does not grant broader administrative rights that are not necessary for the tasks.

upvoted 1 times

yonie 1 year ago

Doesnt seem to have permission to create groups or assign roles. It is focused only on access reviews.

upvoted 1 times

wardy1983 1 year, 1 month ago

Answer: D

Explanation:

D : Users with this role can manage role assignments in Azure Active Directory, as well as within Azure AD Privileged Identity Management. They can create and manage groups that can be assigned to Azure AD roles. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.Under Action you'll find :microsoft.directory/accessReviews/definitions.groupsAssignableToRoles/create >>Create access reviews for membership in groups that are assignable to Azure AD roles

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-roleadministrator

upvoted 1 times

alfaAzure 1 year, 4 months ago

Selected Answer: D

D is correct.

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

upvoted 3 times

ESAJRR 1 year, 4 months ago

Selected Answer: D

D. Privileged role administrator

upvoted 1 times

alfaAzure 1 year, 4 months ago

Correct D.

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

upvoted 1 times

Ario 1 year, 5 months ago

Selected Answer: C

D also is correct but considering the principle of least privilege and the given requirements, option C, "Identity Governance Administrator," remains the best choice for User1.

upvoted 1 times

Alexbz 1 year, 6 months ago

Selected Answer: D

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

Under Action you'll find :

microsoft.directory/accessReviews/definitions.groupsAssignableToRoles/create >> Create access reviews for membership in groups that are assignable to Azure AD roles

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

upvoted 3 times

billo79152718 1 year, 7 months ago

D is correct. According to Microsoft Documentation.

https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-connected-machine-agent?tabs=WindowsScript

upvoted 1 times

Malikusmanrasheed 1 year, 6 months ago

That link is off no relevance

upvoted 1 times

⊟ **Naszari** 1 year, 7 months ago

Selected Answer: D

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

upvoted 4 times

Question #100 *Topic 2*

SIMULATION

-

You need to ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group. The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

Suggested Answer:

RBAC role: 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.

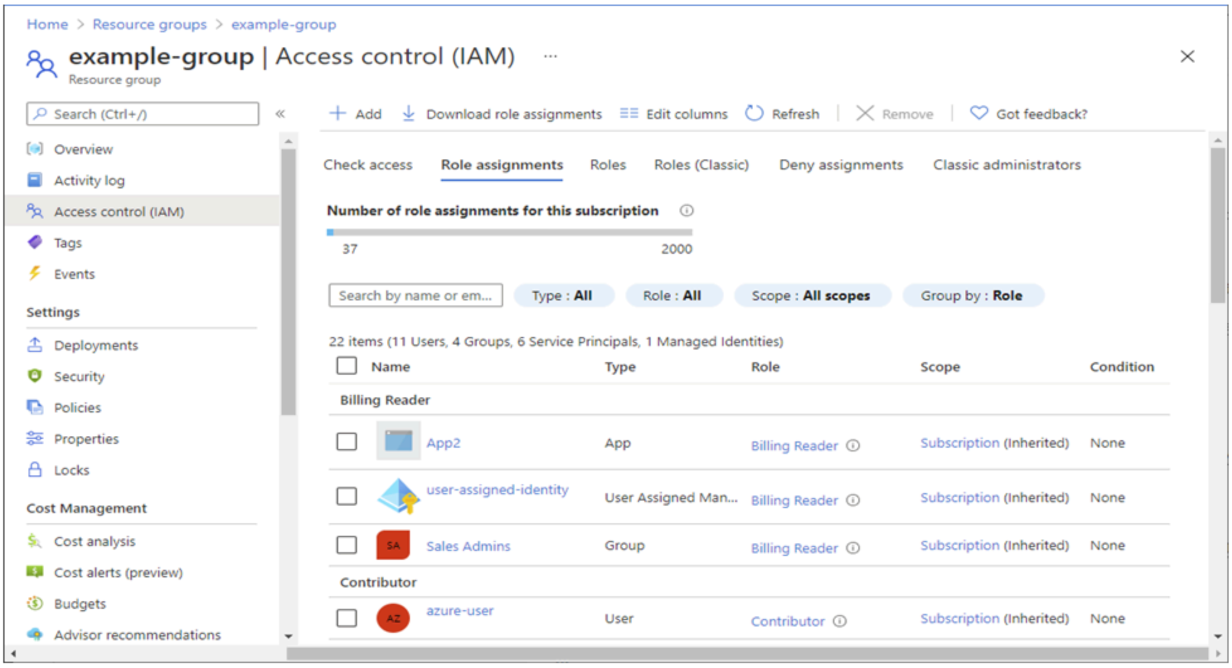
Grant a user access to Azure resources using the Azure portal
Azure role-based access control (Azure RBAC) is the way that you manage access to Azure resources.
Here you will grant a user access to create and manage virtual machines in a resource group.

Grant access
In Azure RBAC, to grant access, you assign an Azure role.

Step 1: In the list of Resource groups, open the RG1lod28681041 resource group.

Step 2: In the navigation menu, click Access control (IAM).

Step 3: Click the Role assignments tab to see the current list of role assignments.



Number of role assignments for this subscription

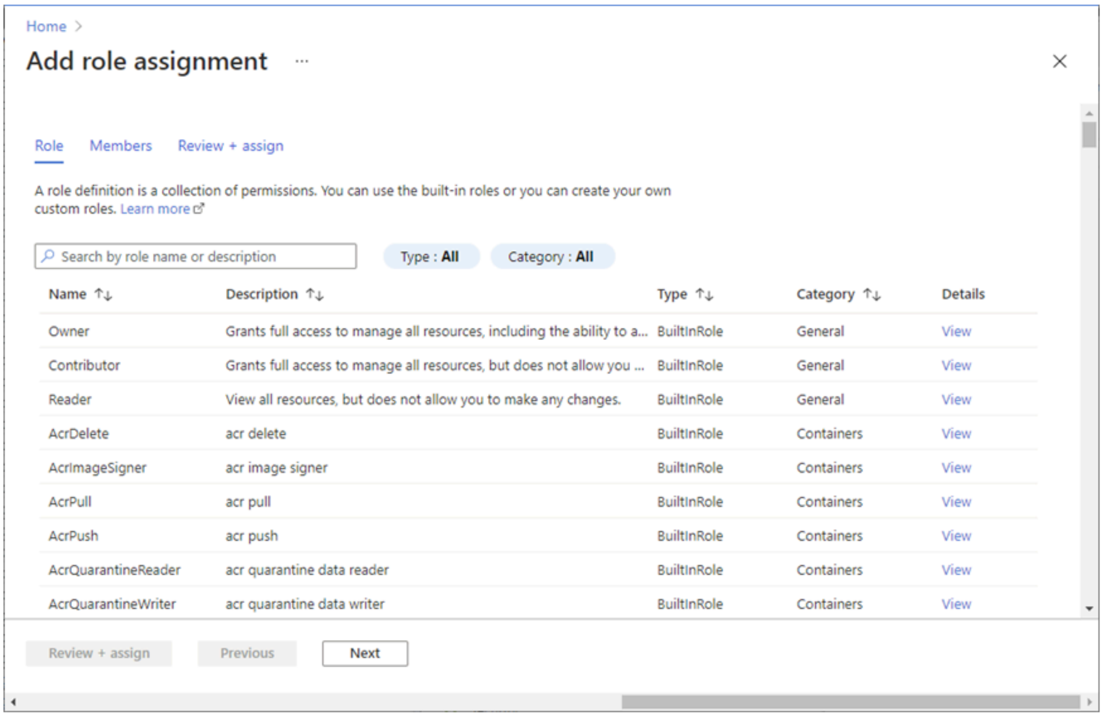
37 2000

22 items (11 Users, 4 Groups, 6 Service Principals, 1 Managed Identities)

Name	Type	Role	Scope	Condition
Billing Reader				
App2	App	Billing Reader	Subscription (Inherited)	None
user-assigned-identity	User Assigned Man...	Billing Reader	Subscription (Inherited)	None
Sales Admins	Group	Billing Reader	Subscription (Inherited)	None
Contributor				
azure-user	User	Contributor	Subscription (Inherited)	None

Step 4: Click Add > Add role assignment.

Step 5: On the Role tab, select the Virtual Machine Contributor role.



A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

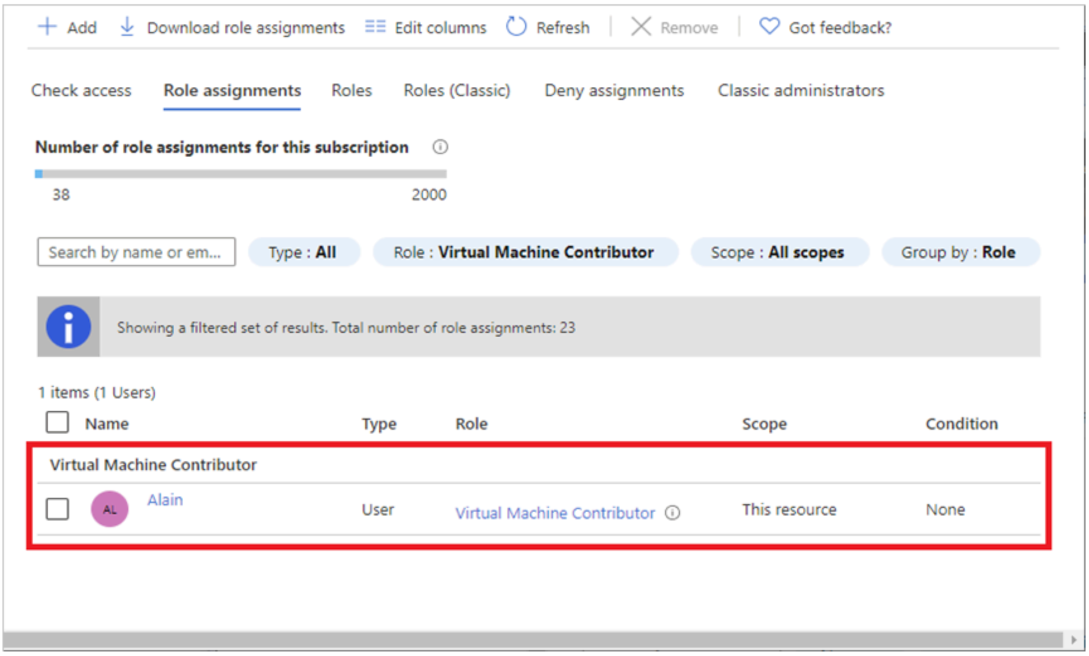
Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to a...	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you ...	BuiltInRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
AcrDelete	acr delete	BuiltInRole	Containers	View
AcrImageSigner	acr image signer	BuiltInRole	Containers	View
AcrPull	acr pull	BuiltInRole	Containers	View
AcrPush	acr push	BuiltInRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View

Step 6: On the Members tab, select yourself or another user.

Step 7: On the Review + assign tab, review the role assignment settings.

Step 8: Click Review + assign to assign the role.

After a few moments, the user is assigned the Virtual Machine Contributor role at the RG1lod28681041 resource group scope.



Number of role assignments for this subscription ⓘ

38 2000

Search by name or em... | Type : **All** | Role : **Virtual Machine Contributor** | Scope : **All scopes** | Group by : **Role**

Showing a filtered set of results. Total number of role assignments: 23

1 items (1 Users)

☐ Name	Type	Role	Scope	Condition
Virtual Machine Contributor				
☐ AL Alain	User	Virtual Machine Contributor ⓘ	This resource	None

Reference:
https://learn.microsoft.com/en-us/azure/role-based-access-control/quickstart-assign-role-user-portal
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#classic-virtual-machine-contributor

⊟ **91743b3** 10 months, 3 weeks ago

On exam Aug 06 2024

upvoted 2 times

⊟ **autobandventieldopje** 1 year, 6 months ago

VM contributor is correct

upvoted 2 times

⊟ **liorh** 2 years, 1 month ago

what is the correct answer?

upvoted 2 times

⊟ **Crazysaffer** 2 years ago

Virtual Machine Contributor role

upvoted 2 times

Question #101 *Topic 2*

SIMULATION

-

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

To complete this task, sign in to the Azure portal.

Suggested Answer:

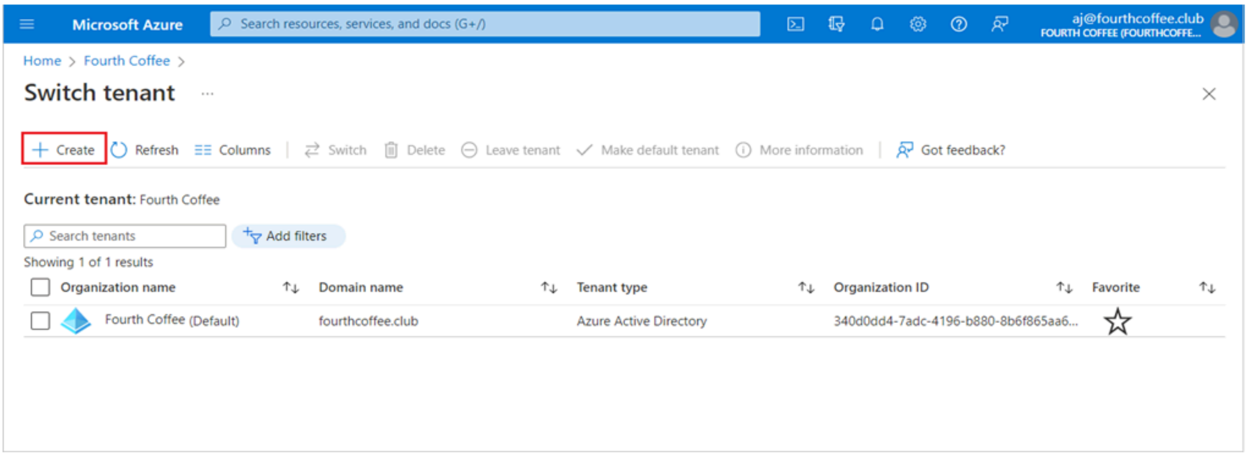
Create Azure AD directory
To create a new tenant

Azure Active Directory - Overview page - Create a tenant
Step 1: Sign in to your organization's Azure portal.

Step 2: From the Azure portal menu, select Azure Active Directory.

Step 3: On the overview page, select Manage tenants

Step 4: Select Create.



Current tenant: Fourth Coffee

Showing 1 of 1 results

□ Organization name	Domain name	Tenant type	Organization ID	Favorite
□ Fourth Coffee (Default)	fourthcoffee.club	Azure Active Directory	340d0dd4-7adc-4196-b880-8b6f865aa6...	☆

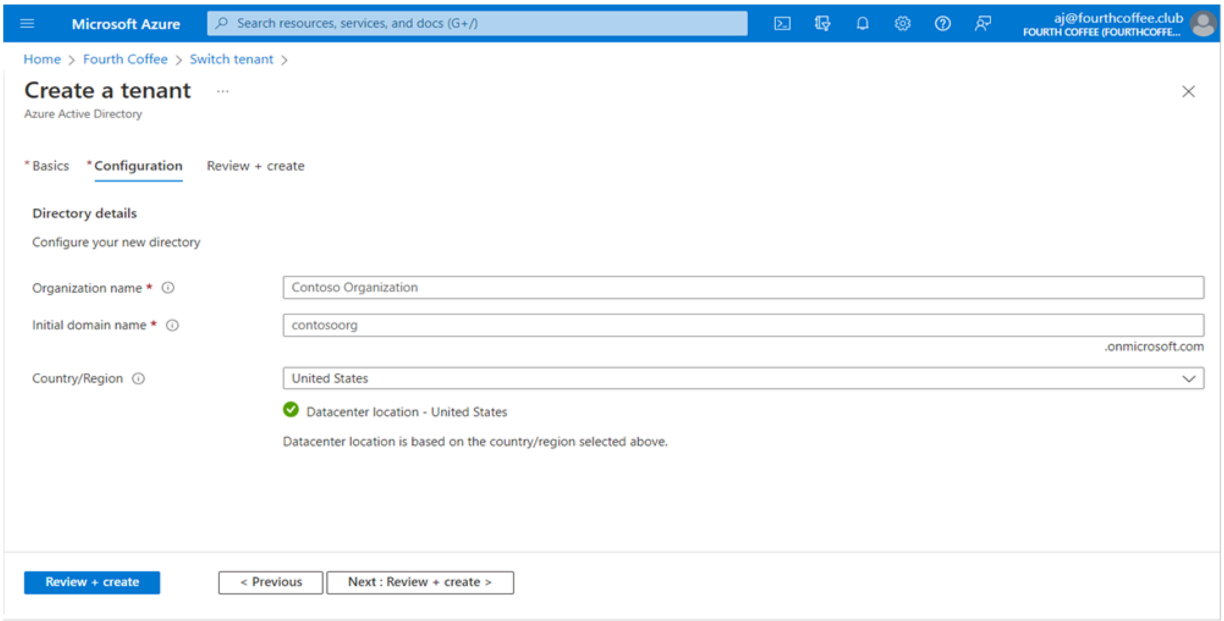
Step 5: On the Basics tab, select the type of tenant you want to create, either Azure Active Directory or Azure Active Directory (B2C).

Step 6: Select Next: Configuration to move on to the Configuration tab.

Step 7: On the Configuration tab, enter the following information:
Type your desired Organization name (for example Contoso Organization) into the Organization name box.

Type your desired Initial domain name (We use 28681041) into the Initial domain name box.

Select your desired Country/Region or leave the United States option in the Country or region box.



Directory details

Configure your new directory

Organization name * : Contoso Organization

Initial domain name * : contosoorg .onmicrosoft.com

Country/Region : United States

✓ Datacenter location - United States

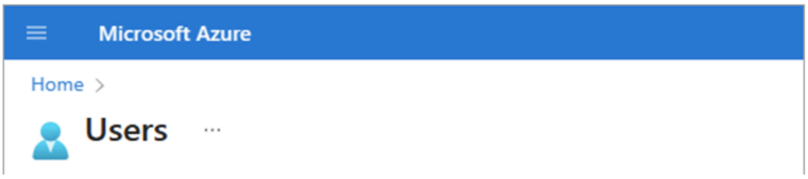
Datacenter location is based on the country/region selected above.

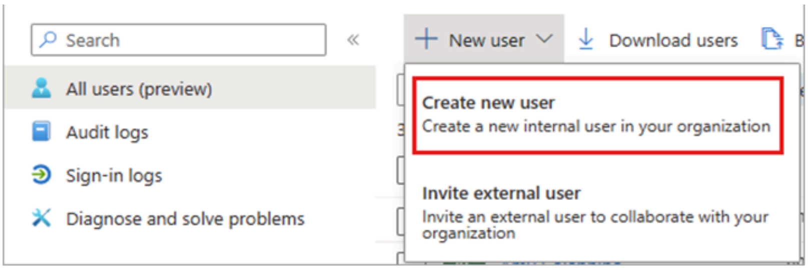
Step 8: Select Next: Review + Create. Review the information you entered and if the information is correct, select create.

Step 9: Your new tenant is created with the domain 28681041.onmicrosoft.com.

Add new users or delete existing users from your Azure Active Directory (Azure AD) tenant.
Add a new user
You can create a new user for your organization or invite an external user from the same starting point.

1. Sign in to the Azure portal in the User Administrator role.
2. Navigate to Azure Active Directory > Users.
3. Select either Create new user or Invite external user from the menu. You can change this setting on the next screen.




Search
All users (preview)
Audit logs
Sign-in logs
Diagnose and solve problems
New user
Download users
Create new user
Create a new internal user in your organization
Invite external user
Invite an external user to collaborate with your organization

4. On the New User page, provide the new user's information:

Identity: user1@28681041.onmicrosoft.com
Details omitted

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

6. Select Create.

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

Reference:
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

autobandventieldopje 7 months ago

Explanation seems correct

upvoted 4 times

Question #102 Topic 2

HOTSPOT

-

You have an Azure subscription that contains a user named Admin1 and an Azure key vault named Vault1.

You plan to implement Microsoft Entra Verified ID.

You need to create an access policy to ensure that Admin1 has permissions to Vault1 that support the implementation of the Verified ID service. The solution must use the principle of least privilege.

Which three key permissions should you select? To answer, select the appropriate permissions in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Key permissions

Key Management Operations

□ Select all

□ Get

□ List

□ Update

□ Create

□ Import

□ Delete

□ Recover

□ Backup

□ Restore

Cryptographic Operations

□ Select all

□ Decrypt

□ Encrypt

□ Unwrap Key

□ Wrap Key

□ Verify

□ Sign

Privileged Key Operations

□ Select all

□ Purge

□ Release

Rotation Policy Operations

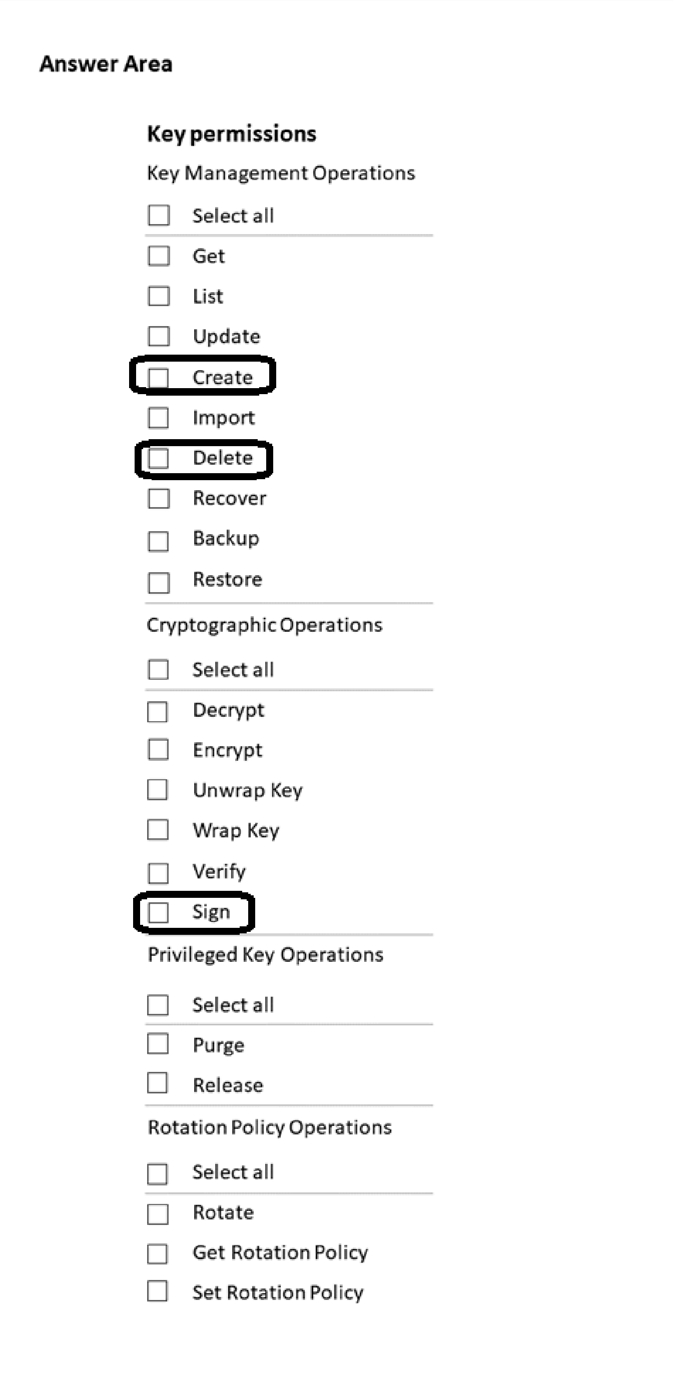
□ Select all

□ Rotate

□ Get Rotation Policy

□ Set Rotation Policy

Suggested Answer:



Answer Area

Key permissions

Key Management Operations

- □ Select all
- □ Get
- □ List
- □ Update
- □ [✓ Create]
- □ Import
- □ [✓ Delete]
- □ Recover
- □ Backup
- □ Restore

Cryptographic Operations

- □ Select all
- □ Decrypt
- □ Encrypt
- □ Unwrap Key
- □ Wrap Key
- □ Verify
- □ [✓ Sign]

Privileged Key Operations

- □ Select all
- □ Purge
- □ Release

Rotation Policy Operations

- □ Select all
- □ Rotate
- □ Get Rotation Policy
- □ Set Rotation Policy

billo79152718 Highly Voted 2 years, 1 month ago

Given answers is correct.

https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

upvoted 12 times

workhard Most Recent 11 months, 1 week ago

By default, the account that creates a vault is the only one with access (vault creators have by default permissions to create and delete keys). The Verified ID service needs access to the key vault. You must authenticate your key vault, allowing the account used during configuration to create and delete keys. The account used during configuration also requires permissions to sign so that it can create the domain binding for Verified ID.
So, if the Admin1 account is not the one that created Vault1, it will need to get the following key permissions: create, delete and sign.
https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant

upvoted 4 times

Christof 1 year, 7 months ago

Create, Delete, Sign. "Follow these steps to create a key vault using the Azure portal. Note:
By default, the account that creates a vault is the only one with access. The Verified ID service needs access to the key vault. You must configure your key vault with access policies allowing the account used during configuration to CREATE and DELETE keys. The account used during configuration also requires permissions to SIGN so that it can create the domain binding for Verified ID. If you use the same account while testing, modify the default policy to grant the account sign permission, in addition to the default permissions granted to vault creators.

upvoted 4 times

Christof 1 year, 7 months ago

Reference for above: https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant

upvoted 1 times

ErikPJordan 1 year, 9 months ago

https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

- Go to Set access policies for the Verified ID Admin user, you can see screenshot where Get, Create, Delete, Sign is selected

upvoted 1 times

ErikPJordan 1 year, 9 months ago

Confusing ....For Key permissions, verify that the following permissions are selected: Get, Create, Delete, and Sign. By default, Create and Delete are already enabled. Sign should be the only key permission you need to update.

upvoted 2 times

fireb 1 year, 10 months ago

In all, you need these 4 permissions enabled: Get, Create, Delete, and Sign.
However, by default, Create and Delete are enabled.
Therefore, Sign and Get should be the only key permissions you need to update.

https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

upvoted 2 times

03038b8 1 year, 11 months ago

Considering the principle of least privilege, the definite answers for the three key permissions to support the implementation of Azure Verified ID are:

Sign: This permission allows the user (Admin1) to use the keys in Vault1 for signing operations, which is necessary for verifying the authenticity of the Verified ID.

Verify: This permission enables the user (Admin1) to use the keys in Vault1 for verification operations, which is essential for validating the Verified ID.

Get: This permission allows the user (Admin1) to retrieve the keys from Vault1. It may be required for certain operations during the implementation of Azure Verified ID, such as retrieving the public key for verification purposes.

By selecting these three key permissions (Sign, Verify, and Get) for Admin1 in the access policy of Vault1, you ensure that Admin1 has the necessary permissions to support the implementation of Azure Verified ID, while following the principle of least privilege.

I apologize for any confusion caused earlier, and I appreciate your patience.

upvoted 1 times

03038b8 1 year, 11 months ago

My bad, it's Create, Delete, sign. The first answer was chatgpt answer but after verification it appears to be Create, Delete, Sign

upvoted 1 times

timHAG 1 year, 9 months ago

I am with this answer, its to help the idverify, creat and delete are enabled by default, you will need sign get and verify in addition

upvoted 1 times

Kb80 1 year, 11 months ago

One quirk I also encountered when configuring this in the lab is that when I went to register the decentrialized ID the key vault operation failed with an error that you need to add "List" also. Then it would proceed.

upvoted 2 times

[Removed] 1 year, 12 months ago

Which three key permissions get create delete

upvoted 1 times

Ario 1 year, 12 months ago

should pick also GET
https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

upvoted 2 times

femzy 1 year, 7 months ago

For intial setup, you will want to go with Create, Delete and Sign as 3 key permissions.First 2 are enabled by default.

upvoted 1 times

⊟ **973b658** 2 years, 1 month ago

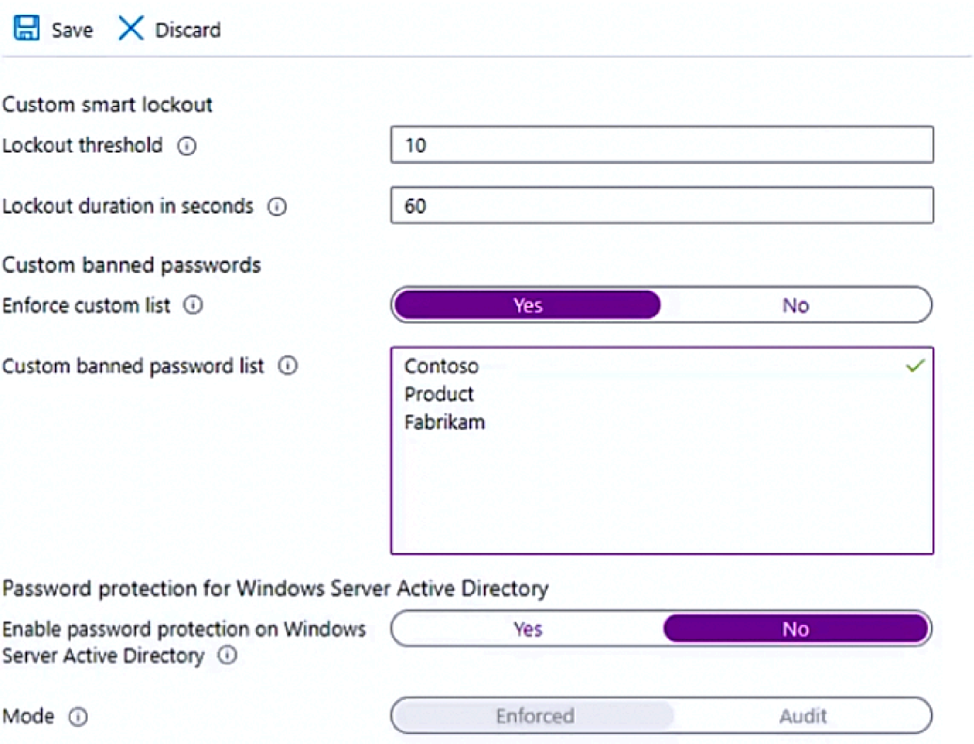
create,delete,sign

upvoted 2 times

Question #103 *Topic 2*

You have an Azure AD tenant that contains three users named User1, User2, and User3.

You configure Azure AD Password Protection as shown in the following exhibit.



Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ [✓ Yes] No

Custom banned password list ⓘ
Contoso
Product
Fabrikam

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes [✓ No]

Mode ⓘ Enforced Audit

The users perform the following tasks:

- User1 attempts to reset her password to C0nt0s0.
- User2 attempts to reset her password to F@brikamHQ.
- User3 attempts to reset her password to Pr0duct123.

Which password reset attempts fail?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User 3 only

E. User1, User2, and User3

Suggested Answer: *E*

Community vote distribution

E (100%)

⊟ Alexbz Highly Voted 👍 2 years ago

Selected Answer: E

Confirmed in my lab, you'll get " Unfortunately, you can't use that password because it contains words or characters that have been blocked by your administrator. Please try again with a different password." when you select either of those password.

upvoted 13 times

⊟ d3N Highly Voted 👍 1 year, 10 months ago

Audit or not it doesn't matter in this scenario.

The question is about Azure AD users where Password Protection is enabled.

PP is composed by 2 lists: Microsoft and Custom Banned Password list.
Evaluating proccess will be:
C0nt0s0. - contoso will get 1 point as it is in Custom Banned Password list + 1 point for "." = 2 points
F@brikamHQ. - fabrikam will get 1 point as it is in Custom Banned Password list + 2 points for HQ + 1 point for "." = 4 points. You need 5 for password to be accepted.
Product123. - product will get 1 point as it is in Custom Banned Password list + 1 point for each character in 123 + 1 point for "." = 5 points.
So I will say that the password for User3 might be accepted but as we don't have the option for "User1 and User2 only", I suppose that "123" is a combination included in Microsoft Banned Password list and if it so - this fact sucks as nobody knows what it contains, you have to test it because you won't find it in any documentation.

upvoted 5 times

Pamban Most Recent 1 year, 2 months ago

Selected Answer: E

It is Normalization guys.. Answer is E

Link
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad#how-are-passwords-evaluated

upvoted 1 times

Apptech 1 year, 3 months ago

The custom banned password list considers common character substitution, such as "o" and "0", or "a" and "@". For that reason all three are banned.
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection#what-are-banned-password-lists

upvoted 2 times

flafernan 1 year, 7 months ago

Selected Answer: E

This is because Azure AD Password Protection is designed to check passwords for patterns including sequences of prohibited characters, even when some letters are stripped for numbers or special characters. It performs a thorough check of passwords against a list of banned words and common patterns to improve password security.

In this case, the passwords "C0nt0s0", "F@brikamHQ", and "Pr0duct123" contain variations of prohibited words in the custom list, such as "Contoso", "Fabrikam", and "Product", and are therefore considered insecure by Azure AD password protection. The tool is sensitive to substitutions of letters for numbers, special characters and other variations, as these practices still result in predictable and insecure passwords.

upvoted 3 times

Self_Study 1 year, 10 months ago

Selected Answer: E

On exam 7/8/23. Answers are correct as audit mode only.

upvoted 4 times

Self_Study 1 year, 10 months ago

Oh, in my test it was audit mode only. Read carefully what you get.

upvoted 2 times

ESAJRR 1 year, 11 months ago

Selected Answer: E

E. User1, User2, and User3

upvoted 1 times

Mahavijay 1 year, 11 months ago

I think all attempts will pass thr successfully as the setting enable password protection on Windows AD is set to NO but in answers there is no such option. Something is wrong here
Can some one please verify?

upvoted 3 times

hellboycze 1 year, 11 months ago

Windows Server AD is related to onpremise ADDS and not Azure AD. Users1-3 are from Azure AD.

upvoted 2 times

Mahavijay 1 year, 11 months ago

Set the option for Enable password protection on Windows Server Active Directory to Yes.

When this setting is set to No, all deployed Azure AD Password Protection DC agents go into a quiescent mode where all passwords are accepted as-is. No validation activities are performed, and audit events aren't generated.

upvoted 3 times

⊟ **Ario** 1 year, 12 months ago

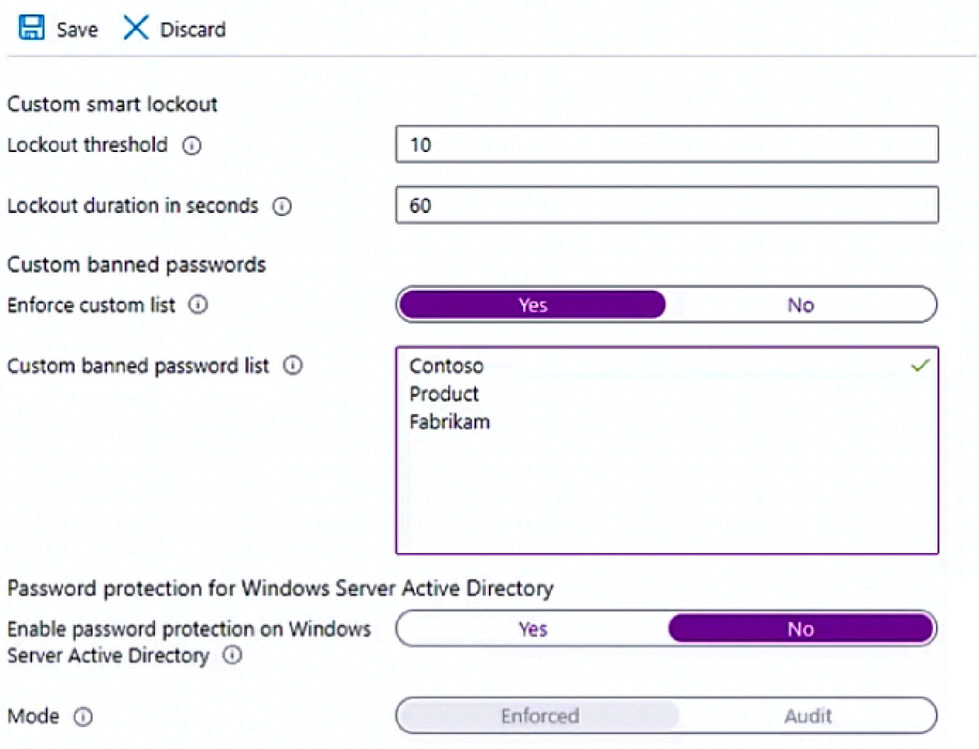
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations

upvoted 1 times

Question #103 Topic 2

You have a Microsoft Entra tenant that contains three users named User1, User2, and User3.

You configure Microsoft Entra Password Protection as shown in the following exhibit.



Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ [✓ Yes] No

Custom banned password list ⓘ ✓

Contoso
Product
Fabrikam

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes [✓ No]

Mode ⓘ Enforced Audit

The users perform the following tasks:

- User1 attempts to reset her password to C0nt0s0.
- User2 attempts to reset her password to F@brikamHQ.
- User3 attempts to reset her password to Pr0duct123.

Which password reset attempts fail?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User 3 only

E. User1, User2, and User3

Suggested Answer: *E*

Community vote distribution

E (100%)

⊟ **LHU** 1 week, 4 days ago

Selected Answer: E

The reason this question is so simple is because it's a boolean problem; either all of them fail for the same reason, or none of them fail. But the answers already say "well, at least one of them fails", which makes it real easy.

upvoted 1 times

⊟ **AlPers** 8 months, 1 week ago

After normalization, the password is evaluated as follows:

Each banned password that's found in a user's password is given one point.

Each remaining character that isn't part of a banned password is given one point.

A password must be at least five (5) points to be accepted.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad#how-are-passwords-evaluated

upvoted 2 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **robluis1987** 8 months, 3 weeks ago

I love such easy questions

upvoted 1 times

⊟ **obaemf** 9 months, 1 week ago

Selected Answer: E

All attempts matches banned words and their banned variations

upvoted 1 times

⊟ **NeoTactics** 9 months, 3 weeks ago

Selected Answer: E

All attempts will fail, because words (and also permutations) are enforced in the custom list.

upvoted 1 times

Question #104 *Topic 2*

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

A user named User1 is eligible for the Billing administrator role.

You need to ensure that the role can only be used for a maximum of two hours.

What should you do?

A. Create a new access review.

B. Edit the role assignment settings.

C. Update the end date of the user assignment.

D. Edit the role activation settings.

Suggested Answer: *B*

Community vote distribution

D (88%) 13%

⊟ **xcapell** Highly Voted 2 years ago

D. Role activation settings

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

upvoted 16 times

⊟ **Anarchira** 2 years ago

Correct

upvoted 1 times

⊟ **Pillartech** Most Recent 11 months, 2 weeks ago

Selected Answer: D

D is the answer

upvoted 1 times

⊟ **Ivan80** 1 year, 5 months ago

In exam 1/28/24

upvoted 3 times

⊟ **bob_sez** 1 year, 7 months ago

So stupid these questions.
You have to indeed actually edit the Role>Assignment>Settings.
But once there the duration changes are under Activation>Settings
I have no idea which one MS wants selected here.

upvoted 1 times

⊟ **pentium75** 11 months ago

It's not reality but rather the wording in the official documentation that matters ;) Thus D.

upvoted 1 times

⊟ **Nava702** 1 year, 3 months ago

So often such questions have more than one answer. Look out for those. If you select only one you will lose points.

upvoted 1 times

⊟ **flafernan** 1 year, 7 months ago

Selected Answer: D

Considering the original judgment presented in the question, letter D (Edit function activation settings) would be the most pertinent choice, since the other options would not directly apply to the function's time limitation.

However, it is important to note that the actual configuration of time limitations for privileged roles must be performed through Azure AD Privileged

Identity Management (PIM) policies to ensure secure use and required compliance of privileged roles. Therefore, although D may be the most detailed option based on the logic of the question, the specific configuration of the time limitation must be performed in PIM.

upvoted 4 times

OrangeSG 1 year, 8 months ago

Selected Answer: D

To ensure that the Billing administrator role can only be used for a maximum of two hours, you need to edit the role activation settings. To do this, follow these steps:

1. Sign in to the Azure portal.
2. Go to Azure Active Directory > Privileged Identity Management.
3. Click Roles > Role settings.
4. Select the Billing administrator role.
5. Under Activation maximum duration, set the maximum duration to 2 hours.
6. Click Save.

Once you have edited the role activation settings, User1 will be able to activate the Billing administrator role for a maximum of two hours at a time. After two hours, the role assignment will automatically expire.

Reference
Configure Microsoft Entra role settings in Privileged Identity Management
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

upvoted 4 times

ErikPJordan 1 year, 9 months ago

Selected Answer: D

Double DD

upvoted 4 times

heatfan900 1 year, 10 months ago

THE ACTIVATION TAB WITHIN THE PIM ROLE SETTINGS.

ASSIGNMENT SPECIFIES WHEN THE ROLE ITSELF EXPIRES AND WHO IS ASSIGNED TO IT.

upvoted 1 times

ESAJRR 1 year, 11 months ago

Selected Answer: B

B. Edit the role assignment settings.

upvoted 1 times

Ario 1 year, 12 months ago

Selected Answer: D

D. Edit the role activation settings.

upvoted 1 times

sigvast 1 year, 12 months ago

Selected Answer: D

The user is eligible for the role, this means that he will request the role (it's an activation process). Assignment is when an admin manually assign a role to someone.

upvoted 2 times

03038b8 2 years ago

Tested.
you can Edit either from Role->Choose the role (Billing Administrator in this case)->Role Settings->Edit and then under Activation you setup Activation maximum duration

or if you want

Azure AD Privileged Identity Management -> Azure AD Roles -> Roles Under Manage you choose Assignments (if the role has already been assigned at least once) you click Settings-> Edit and then under Activation you setup Activation maximum duration
if the role has not been assigned to someone under Manage you click Settings, you choose the role and then Edit under Activation you setup Activation maximum duration

upvoted 1 times

AjayD123 2 years ago

Selected Answer: D

Role Activation settings

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings#role-settings

upvoted 3 times

⊟ **Hara** 2 years ago

Selected Answer: D

D. - Similar as xcapell

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settingshttps://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

upvoted 2 times

⊟ **Alexbz** 2 years ago

Selected Answer: B

Answer is correct!

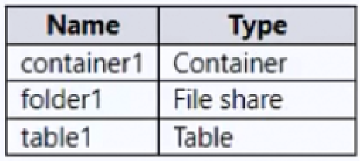
upvoted 2 times

Question #105 *Topic 2*

HOTSPOT

-

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

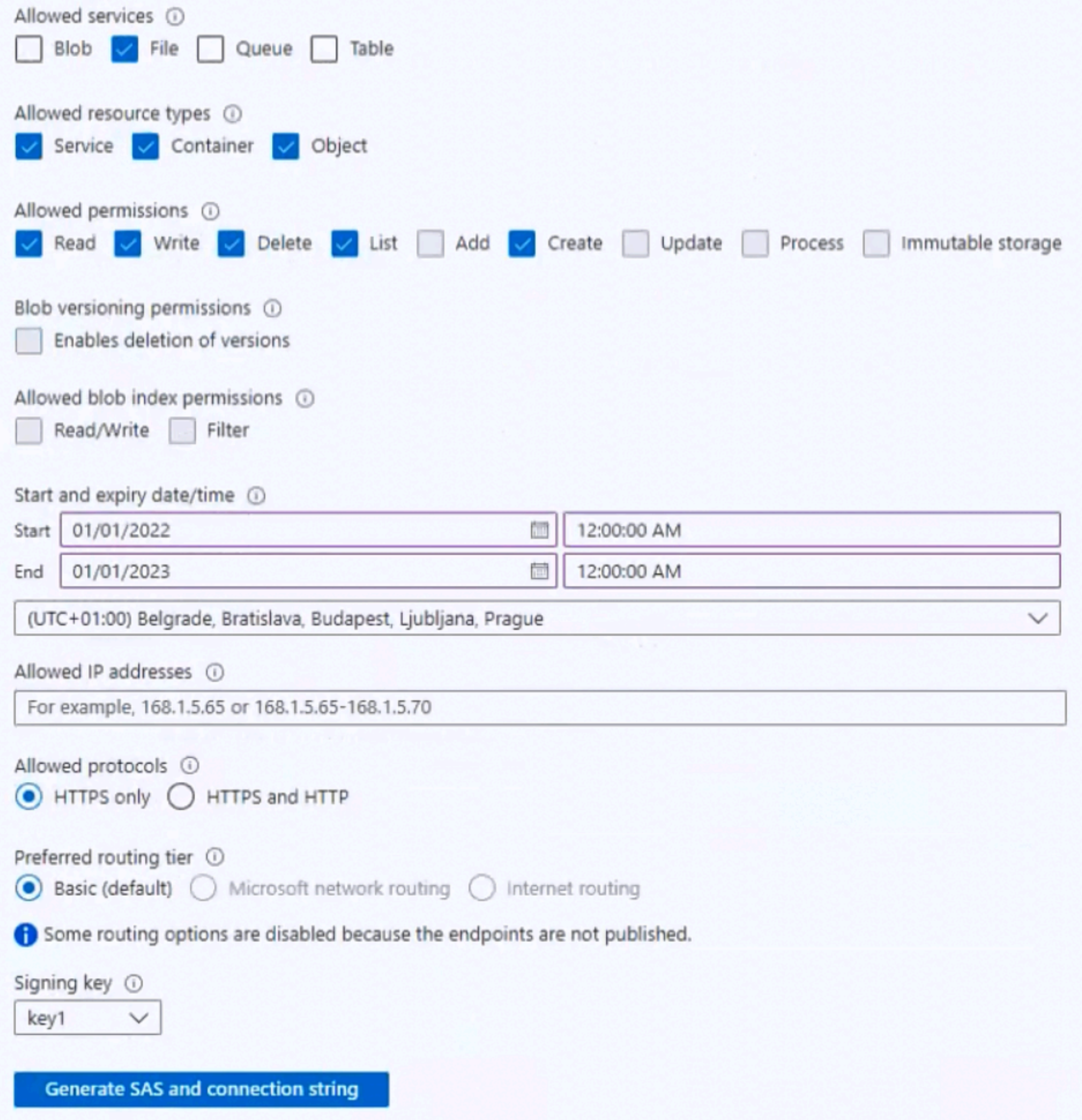


Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

• Storage Blob Data Reader
• Storage Table Data Contributor
• Storage File Data SMB Share Reader

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.



Allowed services ⓘ

□ Blob ☑ File □ Queue □ Table

Allowed resource types ⓘ

☑ Service ☑ Container ☑ Object

Allowed permissions ⓘ

☑ Read ☑ Write ☑ Delete ☑ List □ Add ☑ Create □ Update □ Process □ Immutable storage

Blob versioning permissions ⓘ

□ Enables deletion of versions

Allowed blob index permissions ⓘ

□ Read/Write □ Filter

Start and expiry date/time ⓘ

Start 01/01/2022 12:00:00 AM

End 01/01/2023 12:00:00 AM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses ⓘ

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

● HTTPS only ○ HTTPS and HTTP

Preferred routing tier ⓘ

● Basic (default) ○ Microsoft network routing ○ Internet routing

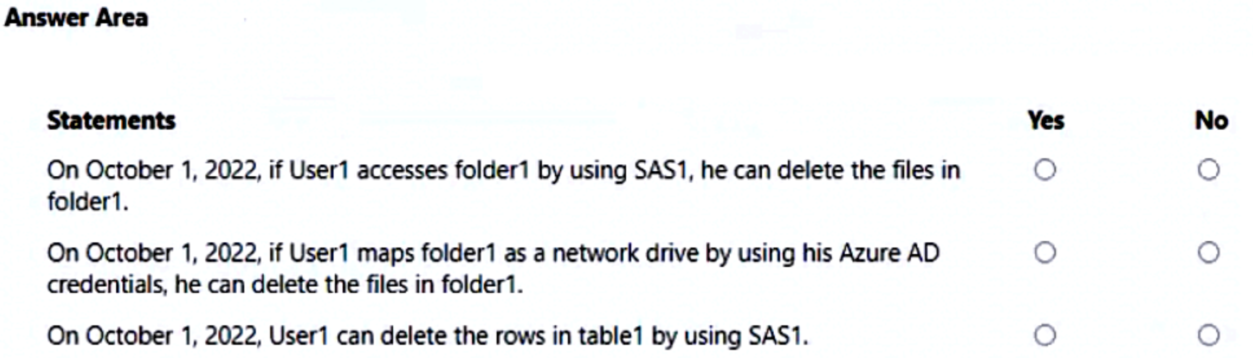
ⓘ Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

key1

Generate SAS and connection string

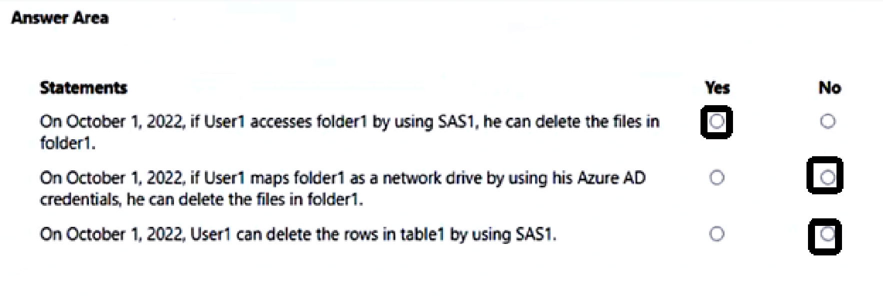
For each of the following statements, select Yes if the statement is true. Otherwise, select No.



Answer Area

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	○	○
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure AD credentials, he can delete the files in folder1.	○	○
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	[✓ ○]	○
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure AD credentials, he can delete the files in folder1.	○	[✓ ○]
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	○	[✓ ○]

sigvast Highly Voted 1 year, 5 months ago

RBAC roles only apply when connecting with AD credentials :

1. Y beacause SAS gives him File Delete permission
2. N because he has only SMB File Reader, he can't delete
3. N because SAS only gives File permission, not Table

upvoted 31 times

BigShot0 Highly Voted 1 year, 3 months ago

Y - The SAS permissions apply

N - The RBAC permissions apply and only has Reader

N - SAS only has File permission - not Table permission

upvoted 10 times

heatfan900 Most Recent 1 year, 4 months ago

Y, N, N

SAS TOKENS ARE A SET OF SECURITY SPECIFICIATIONS AND PERMISSIONS WRAPPED INTO A TOKEN. THE SETTINGS AT THE VERY TOP DO NOT AFFECT THEM.

User1 has access to delete the files in the FILE SHARE folder1 via the SAS TOKEN.

User1 does not have access to do this, based on the very first permissions outlined separate from the token, I will not be allowed to delete.

User1 cannot delete the rows in table1 of the TABLE SERVICE via the SAS TOKEN because the token does not include any permissions to work with the Storage Type Service.

upvoted 5 times

MoMoMoMo1 1 year, 4 months ago

1. Yes: User has Delete Permissions from SAS key.
2. No: RBAC does not apply to SMB NTFS shares, RBAC will be for connection and then NTFS for File permissions.

Azure Files supports identity-based authentication over SMB through the following methods.

a. On-premises AD DS authentication:

b. Azure AD DS authentication:

c. Azure AD Kerberos for hybrid identities:

e. AD Kerberos authentication for Linux clients:

3. No: SAS only has File share selected.

upvoted 2 times

Self_Study 1 year, 4 months ago

On exam 7/8/23. Questions were different.

upvoted 3 times

Ario 1 year, 5 months ago

Answer will be No,No,No

upvoted 3 times

massnonn 1 year, 6 months ago

Wrong user1 has table data contributor for me N N Y

upvoted 1 times

John_P_Doe 1 year ago

It's stated "delete rows in table1 using SAS1": SAS1 doesn't provide access to table1, so answer is No for #3

upvoted 1 times

⊟ **massnonn** 1 year, 6 months ago

Sorry is N N N

upvoted 2 times

⊟ **Hara** 1 year, 6 months ago

Agree with answer - Y N N

upvoted 3 times

Question #106 *Topic 2*

You have an Azure subscription that contains a user named User1 and a storage account that hosts a blob container named blob1.

You need to grant User1 access to blob1. The solution must ensure that the access expires after six days.

What should you use?

A. a shared access signature (SAS)

B. role-based access control (RBAC)

C. a shared access policy

D. a managed identity

Suggested Answer: *A*

Community vote distribution

A (100%)

OrangeSG 8 months, 3 weeks ago

Selected Answer: A

A shared access signature (SAS) is a URI that grants access to Azure Storage resources without requiring a storage account key. SAS tokens can be used to grant access to specific resources, such as a blob container, for a specific period of time.

To grant User1 access to blob1 with an expiration of six days, you can create a SAS token with the following parameters:
- Permissions: r, w, or d, depending on the level of access that you want to grant.
- Start time: The current time.
- Expiry time: Six days from now.

Once you have created the SAS token, you can provide it to User1. User1 can then use the SAS token to access blob1 until the expiry time.

upvoted 2 times

ESAJRR 9 months ago

Selected Answer: A

A. a shared access signature (SAS)

upvoted 1 times

Hara 1 year ago

Selected Answer: A

answer is correct - SAS can specific expired date

upvoted 3 times

Anarchira 1 year ago

Selected Answer: A

Correct, I got a lot of questions like this in az-104.

upvoted 1 times

Question #107 Topic 2

You have an Azure subscription linked to an Azure AD tenant named contoso.com. Contoso.com contains a user named User1 and an Azure web app named App1.

You plan to enable User1 to perform the following tasks:

- Configure contoso.com to use Microsoft Entra Verified ID.
- Register App1 in contoso.com.

You need to identify which roles to assign to User1. The solution must use the principle of least privilege.

Which two roles should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Authentication Policy Administrator

B. Authentication Administrator

C. Cloud App Security Administrator

D. Application Administrator

E. User Administrator

Suggested Answer: *AD*

Community vote distribution

AD (92%) 8%

xcapell Highly Voted 2 years ago

AD.

https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

Ensure that you have the global administrator or the authentication policy administrator permission for the directory you want to configure. If you're not the global administrator, you need the application administrator permission to complete the app registration including granting admin consent.

upvoted 12 times

8de3321 Most Recent 7 months ago

Selected Answer: CD

The answer is Cloud App Administrator and Application Administrator. This exact same question is available in the practice assessment on the leran.Microsoft website and they also show you the answer alongside the reason for the answer. Please check and confirm. Thank you!

upvoted 1 times

Hot_156 4 months ago

Share the link.

Are you saying you can configure Microsoft Verify ID with Cloud app security admin?

upvoted 1 times

Jimmy500 1 year ago

Prerequisites

You need an Azure tenant with an active subscription. If you don't have an Azure subscription, create one for free.

Ensure that you have the Global Administrator or the authentication policy administrator permission for the directory you want to configure. If you're not the Global Administrator, you need the application administrator permission to complete the app registration including granting admin consent.

Ensure that you have the contributor role for the Azure subscription or the resource group where you are deploying Azure Key Vault.

Ensure that you provide access permissions for Key Vault. For more information, see Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control.

https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant

AD

upvoted 2 times

Pamban 1 year, 2 months ago

Selected Answer: AD

Answers: AD

Link: https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant

upvoted 2 times

crutester 1 year, 4 months ago

Selected Answer: AD

AD.
https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant
Ensure that you have the global administrator or the authentication policy administrator permission for the directory you want to configure. If you're not the global administrator, you need the application administrator permission to complete the app registration including granting admin consent.

upvoted 1 times

OrangeSG 1 year, 8 months ago

Selected Answer: AD

To enable User1 to perform the tasks, you should assign the following roles:

- Authentication Policy Administrator: This role is required to configure the tenant for Microsoft Entra Verified ID. The user needs to have the global administrator or the authentication policy administrator permission for the directory they want to configure.

- Application Administrator: This role is required to register an application in Microsoft Entra ID. If User1 is not the global administrator, they need the application administrator permission to complete the app registration including granting admin consent.

Reference
Configure your tenant for Microsoft Entra Verified ID
https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

upvoted 3 times

TheProfessor 1 year, 9 months ago

Selected Answer: AD

Correct Answer: A, D

upvoted 1 times

BigShot0 1 year, 9 months ago

Selected Answer: AD

A - Authentication Policy Administrator - Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and verifiable credentials.
D - Application Administrator - Can create and manage all aspects of app registrations and enterprise apps.

NOT B - Authentication Administrator - Can access to view, set and reset authentication method information for any non-admin user.

You are setting policy for the Org, not managing users.

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

upvoted 2 times

heatfan900 1 year, 10 months ago

Prerequisites

You need an Azure tenant with an active subscription. If you don't have an Azure subscription, create one for free.

Ensure that you have the global administrator or the authentication policy administrator permission for the directory you want to configure. If you're not the global administrator, you need the application administrator permission to complete the app registration including granting admin consent.

• Configure contoso.com to use Microsoft Entra Verified ID. >>authentication policy administrator
• Register App1 in contoso.com >>application administrator

upvoted 1 times

alfaAzure 1 year, 10 months ago

Selected Answer: AD

AD is correct.

https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

upvoted 1 times

⊟ **_fvt** 1 year, 10 months ago

Selected Answer: AD

Given answer is correct

upvoted 1 times

⊟ **Self_Study** 1 year, 10 months ago

Selected Answer: BD

The correct answer is B and D. Authentication Administrator and Application Administrator.

upvoted 1 times

⊟ **pentium75** 11 months ago

Authentication Administrator has too much privilege

upvoted 1 times

Question #108 *Topic 2*

You have an Azure AD tenant.

You plan to implement an authentication solution to meet the following requirements:

• Require number matching.
• Display the geographical location when signing in.

Which authentication method should you include in the solution?

A. Microsoft Authenticator

B. FIDO2 security key

C. SMS

D. Temporary Access Pass

Suggested Answer: *A*

Community vote distribution

A (100%)

xcapell Highly Voted 1 year ago

A. Microsoft Authenticator
https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context

upvoted 7 times

OrangeSG Most Recent 8 months, 3 weeks ago

Selected Answer: A

Microsoft Authenticator is the only authentication method that meets both requirements:
- It supports number matching, which means that users must enter a number displayed in the Microsoft Authenticator app to approve sign-in attempts.
- It can display the geographical location of the sign-in attempt (based on IP address during sign-in), which can be useful for detecting suspicious activity.

upvoted 4 times

TheProfessor 9 months, 1 week ago

Selected Answer: A

A. Microsoft Authenticator

upvoted 2 times

ESAJRR 10 months ago

Selected Answer: A

A. Microsoft Authenticator

upvoted 2 times

Hara 1 year ago

Selected Answer: A

A. MS Authenticator - experienced

upvoted 3 times

Question #109 *Topic 2*

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You plan to implement single sign-on (SSO) for Azure AD resources.

You need to configure an Intranet Zone setting for all users by using a Group Policy Object (GPO).

Which setting should you configure?

A. Logon options

B. Allow updates to status bar via script

C. Allow active scripting

D. Access data sources across domains

Suggested Answer: *B*

Community vote distribution

B (92%) 8%

ElaineChia Highly Voted 11 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sso-quick-start

Refer to this link above. the answer is B as stated in the supported Microsoft site. Did a research to find the actual answer. thanks you. hope it help to the exam taker.

upvoted 13 times

cris_exam 11 months, 1 week ago

B is correct.
Here's a closer link to the answer.

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sso-quick-start#roll-out-the-feature

"You also must enable an intranet zone policy setting called Allow updates to status bar via script through Group Policy."

upvoted 5 times

randy0077 Most Recent 2 months, 2 weeks ago

Selected Answer: B

B is correct ans: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sso-quick-start#:~:text=called%20Allow%20updates-,to%20status%20bar%20via%20script,-through%20Group%20Policy

upvoted 1 times

moadabdou 4 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sso-quick-start

upvoted 1 times

golitech 4 months, 4 weeks ago

Selected Answer: A

✖ B. Allow updates to status bar via script – This is unrelated to authentication or SSO.
✖ C. Allow active scripting – This controls script execution in browsers but is not required for SSO.
✖ D. Access data sources across domains – This controls how cross-domain resources are accessed, which is not related to seamless sign-in.

upvoted 1 times

waqqy 5 months ago

Selected Answer: B

To configure single sign-on (SSO) for Azure AD resources using a Group Policy Object (GPO), you should configure the "Allow updates to status bar via script" setting in the Intranet Zone

upvoted 1 times

⊟ **crutester** 10 months, 2 weeks ago

Selected Answer: B

B is correct. Verified from this link https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sso-quick-start#roll-out-the-feature

upvoted 3 times

⊟ **xlex** 11 months, 3 weeks ago

Selected Answer: A

Logon options: This setting in the Group Policy Object is used to manage how users are authenticated in the Intranet zone. By configuring this setting, you can enable automatic logon with current username and password. This is a key requirement for seamless SSO as it allows users to access Azure AD resources without repeatedly entering their credentials when they are on the corporate network.
The other options are less relevant to SSO configuration.

upvoted 2 times

⊟ **Yatikumar** 11 months, 3 weeks ago

C. Allow active scripting

Allowing active scripting is a common setting for the Intranet Zone to ensure that scripts can run seamlessly within the local network. This is important for various web-based applications and services, especially when implementing single sign-on (SSO) for Azure AD resources.

upvoted 1 times

⊟ **Vokuhila** 11 months, 3 weeks ago

Answer is C. Allow active scripting

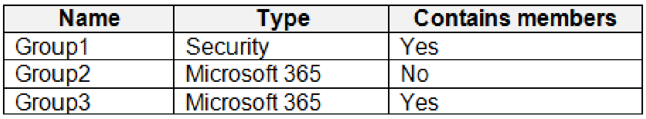
upvoted 1 times

Question #110 *Topic 2*

HOTSPOT

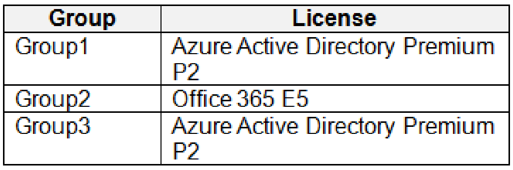
-

You have an Azure AD tenant that contains the groups shown in the following table.



Name	Type	Contains members
Group1	Security	Yes
Group2	Microsoft 365	No
Group3	Microsoft 365	Yes

You assign licenses to the groups as shown in the following table.

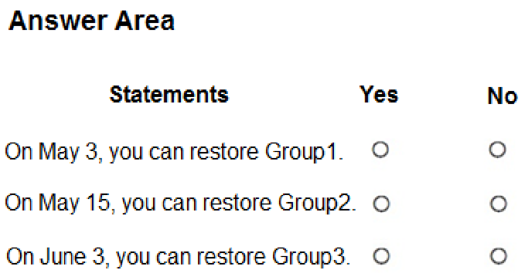


Group	License
Group1	Azure Active Directory Premium P2
Group2	Office 365 E5
Group3	Azure Active Directory Premium P2

On May1, you delete Group1, Group2, and Group3.

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

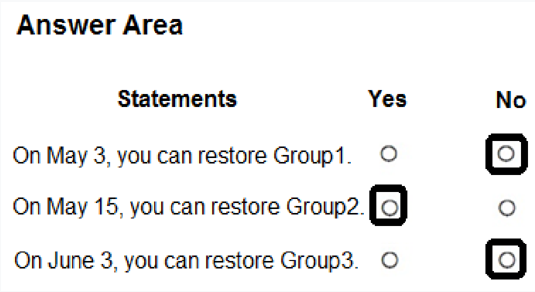
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	○	○
On May 15, you can restore Group2.	○	○
On June 3, you can restore Group3.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	○	[✓ ○]
On May 15, you can restore Group2.	[✓ ○]	○
On June 3, you can restore Group3.	○	[✓ ○]

Vokuhila Highly Voted 1 year, 5 months ago

Answer seems correct

Group 1 cannot be restored - Security groups cannot be restored
Group 2 can be restored because its's an O365 group
Group 3 cannot be restored because 30 days have passed

Please correct me if i'm wrong

upvoted 16 times

flmailla 1 year, 5 months ago

I agree

upvoted 1 times

cris_exam 1 year, 5 months ago

correct

upvoted 2 times

ITFranz Most Recent 1 year, 1 month ago

According to this link.

https://learn.microsoft.com/en-us/entra/identity/users/groups-restore-deleted

When you delete a Microsoft 365 group in Microsoft Entra ID, the deleted group is retained but not visible for 30 days from the deletion date. This behavior is so that the group and its contents can be restored if needed.

May3 and Jun3 is 30 days period. How is this really interpreted for Group3 to be NO ?

The 30 days mark is exactly 30 days.

upvoted 1 times

pentium75 11 months ago

Because groups were deleted May 1, not May 3. May 1 to June 3 is more than 30 days.

upvoted 2 times

Tognan 1 year, 3 months ago

Azure AD security group can be restored with the users , but not the role

So i don't understand the question ; it's only restored the group or group + role ?

upvoted 1 times

Jimmy500 1 year ago

Hi Tognan, If you resster group it will lost all roles that it had previously. Roles are not restorable

upvoted 1 times

Jimmy500 1 year ago

Sorry for typo, restore *

upvoted 1 times

Pamban 1 year, 2 months ago

@Tognan, can you provide the referance for your statement? I can see in MS learn that we can't restore Entra id groups. only 365 groups.

Link: https://learn.microsoft.com/en-us/entra/identity/users/groups-restore-deleted

When you delete a Microsoft 365 group in Microsoft Entra ID, the deleted group is retained but not visible for 30 days from the deletion date. This behavior is so that the group and its contents can be restored if needed. This functionality is restricted exclusively to Microsoft 365 groups in Microsoft Entra ID. It isn't available for security groups and distribution groups. The 30-day group restoration period isn't customizable.

upvoted 1 times

Question #111 *Topic 2*

You have an Azure AD tenant.

You need to ensure that users cannot create passwords containing a variation of the word contoso.

What should you configure?

A. Microsoft Entra Verified ID

B. Microsoft Entra Identity Governance

C. Azure AD Privileged Identity Management (PIM)

D. Azure AD Password Protection

E. Azure AD Identity Protection

Suggested Answer: *D*

Community vote distribution

D (100%)

LHU 1 week, 4 days ago

Selected Answer: D

This is one of those questions that even if you don't know anything about Azure you'd probably guess right.

upvoted 1 times

8de3321 7 months ago

Selected Answer: D

Correct answer is Password Protection and you can configure the list of custom banned passwords

upvoted 1 times

chiquito 1 year, 2 months ago

Selected Answer D:

D is correct : Microsoft Entra Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

Reference:
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad

upvoted 1 times

crutester 1 year, 4 months ago

Selected Answer: D

D is correct.
Password protection for Azure Active Directory (Azure AD) detects and blocks known weak passwords and their variants, and other common terms specific to your organization. It also includes custom banned password lists and self-service password reset capabilities.

upvoted 1 times

Vokuhila 1 year, 5 months ago

Selected Answer: D

D is correct

Azure AD Password Protection enables you to:

Define custom password policies.
Prevent the use of common words or patterns.
Protect against various types of common attacks on passwords.

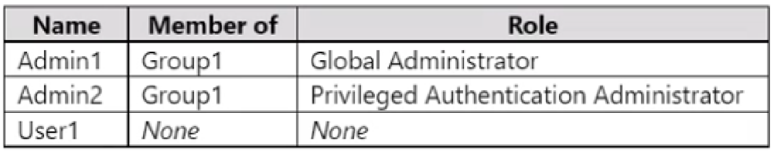
upvoted 4 times

Question #112 Topic 2

HOTSPOT

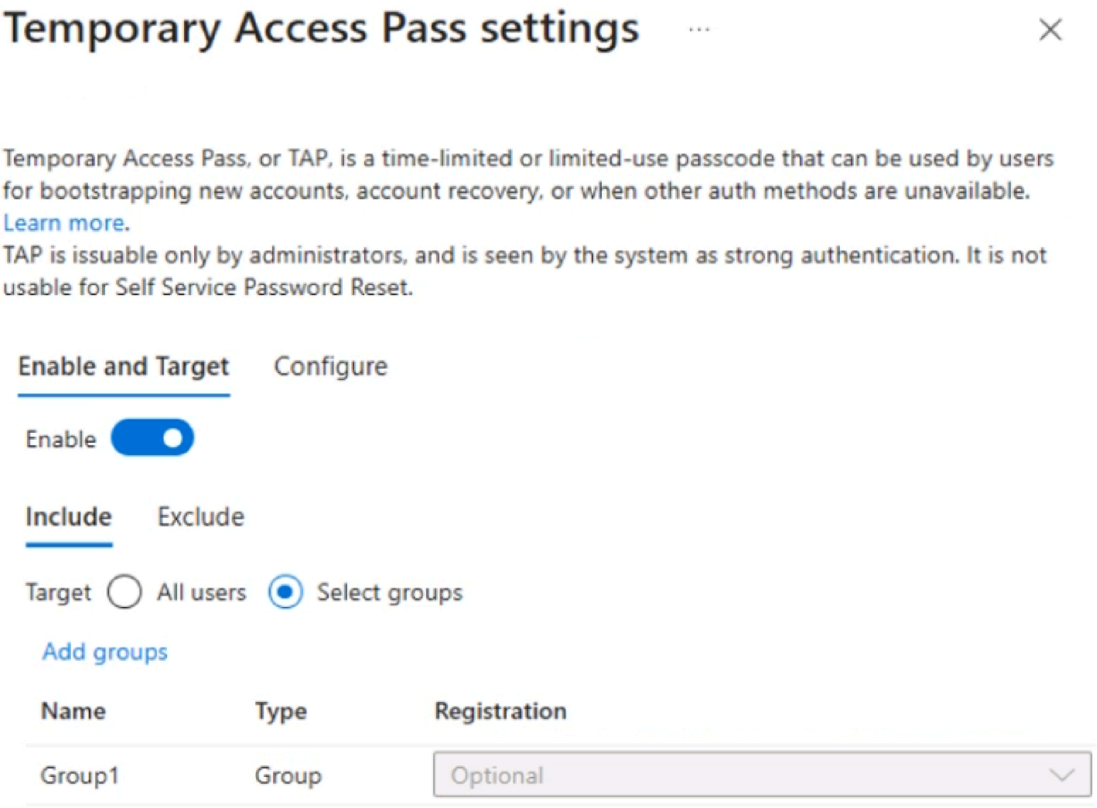
-

You have a Microsoft Entra tenant that contains the users shown in the following table.



Name	Member of	Role
Admin1	Group1	Global Administrator
Admin2	Group1	Privileged Authentication Administrator
User1	*None*	*None*

You configure the Temporary Access Pass settings as shown in the following exhibit.



Temporary Access Pass settings

Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when other auth methods are unavailable. Learn more.
TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service Password Reset.

Enable: On

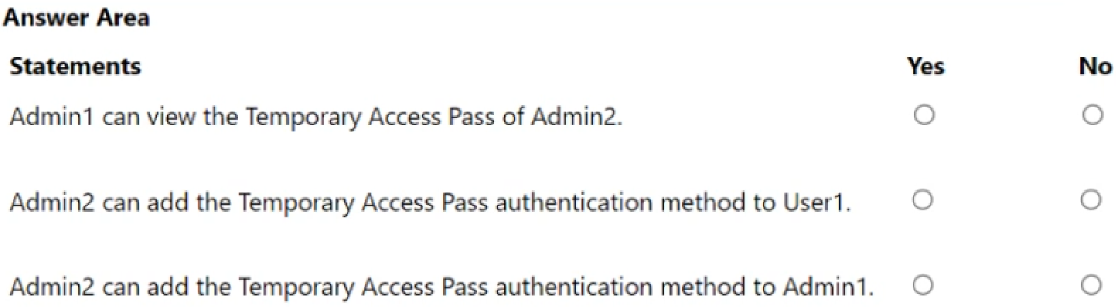
Target ○ All users ● Select groups

Name	Type	Registration
Group1	Group	Optional

You add the Temporary Access Pass authentication method to Admin2.

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

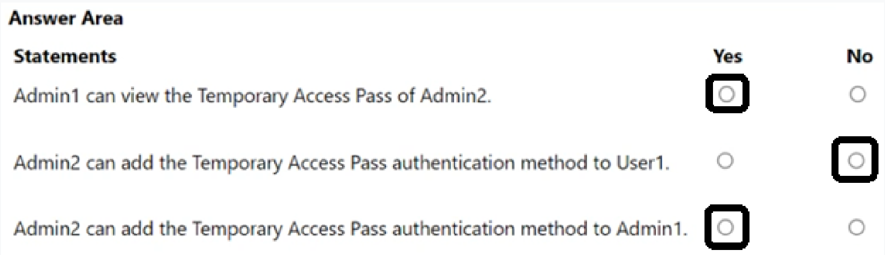
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	○	○
Admin2 can add the Temporary Access Pass authentication method to User1.	○	○
Admin2 can add the Temporary Access Pass authentication method to Admin1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	[✓ ○]	○
Admin2 can add the Temporary Access Pass authentication method to User1.	○	[✓ ○]
Admin2 can add the Temporary Access Pass authentication method to Admin1.	[✓ ○]	○

chiquito Highly Voted 1 year, 2 months ago

Think the answer is correct. User1 is not a member of Group1

Create a Temporary Access Pass

After you enable a TAP policy, you can create TAPs for users in Microsoft Entra ID. These following roles can perform various actions related to a TAP.

• Global Administrators can create, delete, and view a TAP for any user (except themselves).

• Privileged Authentication Administrators can create, delete, and view a TAP for admins and members (except themselves).

• Authentication Administrators can create, delete, and view a TAP for members (except themselves).

• Global Readers can view TAP details for the user (without reading the code itself).

Reference:

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-temporary-access-pass

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-temporary-access-pass

upvoted 5 times

Hot_156 Most Recent 3 months, 4 weeks ago

N - Once you generate the TAP, you cannot see it again! Not even if you are GA.

Y - Priviledge Authentication Admin can add the user1 to the TAP and then generate a TAP.

Y- Priviledge Authentication Admin can generate a TAP for any user

upvoted 1 times

Hot_156 3 months, 3 weeks ago

Be aware that I LAB! this

N - Still no. Once the code is generated, you cannot see it again. It is like a secret code from an app.

N - If the user is not a member of the group, it will fail when trying to generate a TAP.

Y - Same as before

upvoted 3 times

pentium75 11 months ago

YES - Global Admin can view TAP of any user except himself

NO - User1 is not included in the policy, and Privileged Authentication Administrator cannot modify the policy

YES - Privileged Role Administrator can modify authentication methods for administrator

upvoted 3 times

sauliusm 5 months, 3 weeks ago

YYY

The question does not ask if user1 can use the TAP, but if Admin can create it, which he can.

'Although you can create a TAP for any user, only users included in the policy can sign-in with it

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-temporary-access-pass#enable-the-temporary-access-pass-policy

upvoted 2 times

Jimmy500 1 year ago

Privileged Authentication Administrators can create, delete, and view a TAP for admins and members (except themselves).So YYY

upvoted 1 times

Pamban 1 year, 1 month ago

I think Answer is YYY

2nd option: Privileged Authentication Administrators can create, delete, and view a TAP for admins and members (except themselves). which means Privileged Authentication Administrator can add TAP for user1

Link: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-temporary-access-pass

upvoted 3 times

⊟ **pentium75** 11 months ago

No, User1 is not in the group that the TAP policy is assigned to. Privileged Authentication Administrator cannot modify the TAP policy to include User1, and he can also not add User1 to the group.

upvoted 1 times

⊟ **elster** 1 year, 2 months ago

Correct:

Y

N

Y

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-temporary-access-pass

upvoted 3 times

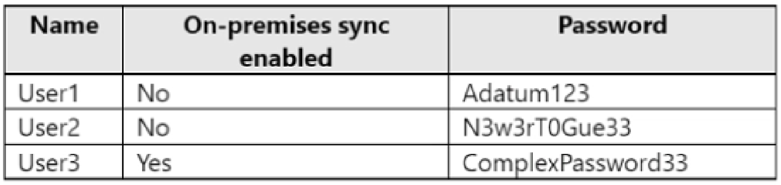
Question #113 *Topic 2*

HOTSPOT

-

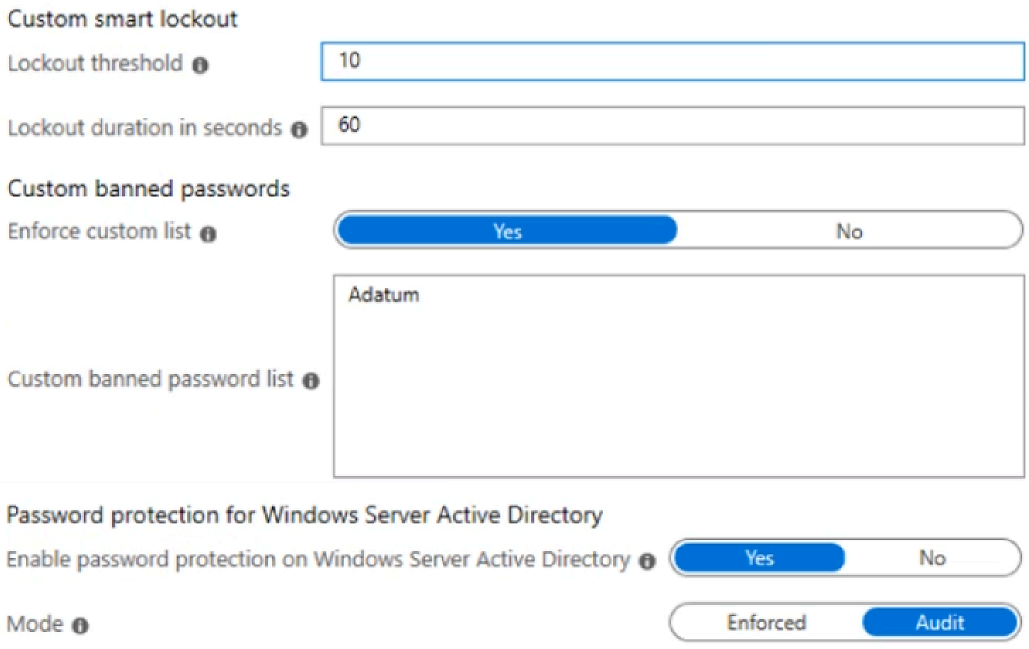
Your network contains an on-premises Active Directory domain named adatum.com that syncs to a Microsoft Entra tenant.

The Microsoft Entra tenant contains the users shown in the following table.



Name	On-premises sync enabled	Password
User1	No	Adatum123
User2	No	N3w3rT0Gue33
User3	Yes	ComplexPassword33

You configure the Microsoft Entra Password Protection settings for adatum.com as shown in the following exhibit.



Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: Yes

Custom banned password list: Adatum

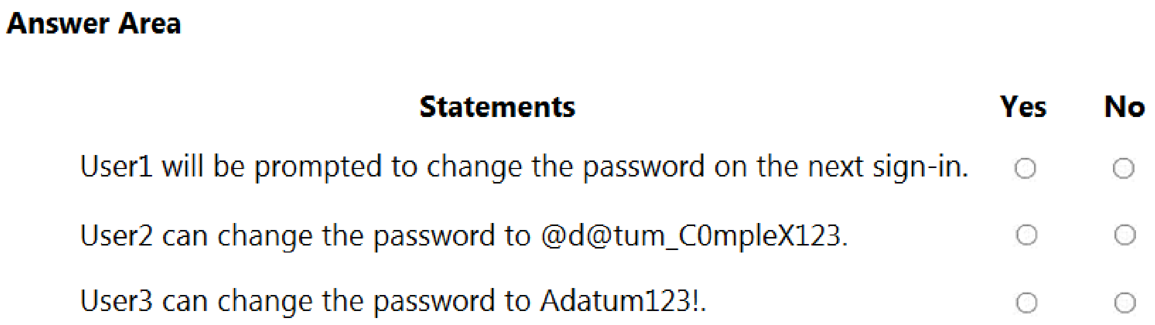
Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes

Mode: Audit

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

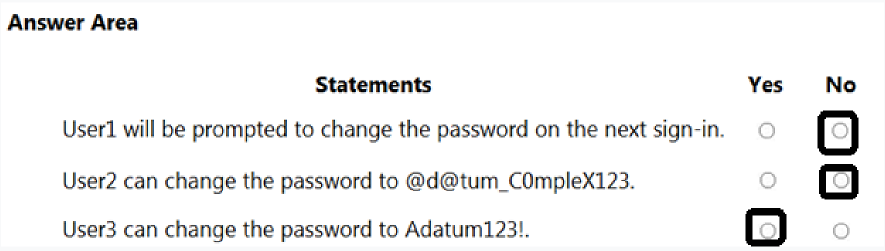
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	○
User2 can change the password to @d@tum_C0mpleX123.	○	○
User3 can change the password to Adatum123!.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	[✓ ○]
User2 can change the password to @d@tum_C0mpleX123.	○	[✓ ○]
User3 can change the password to Adatum123!.	[✓ ○]	○

chiquito Highly Voted 1 year, 2 months ago

Going with NYY

This is not a new question.

Please see Question #62Topic 2 for discussion

Reference:

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad#score-calculation

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-operations#enable-on-premises-password-protection

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

upvoted 10 times

sauliusm 5 months, 3 weeks ago

user 2 can not change the pass, as after normalization it is matching adatum

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad#step-1-normalization

upvoted 1 times

sauliusm 5 months, 3 weeks ago

apologies, it is yes for user2, because of high score due to complexity

upvoted 1 times

pentium75 11 months ago

Audit mode applies to on-premises AD, User2 is native Entra user

upvoted 1 times

elster Highly Voted 1 year, 2 months ago

NYY bc of audit mode.

upvoted 8 times

pentium75 11 months ago

Audit mode applies to on-premises AD, User2 is native Entra user

upvoted 1 times

Hot_156 Most Recent 4 months, 2 weeks ago

First of all - AUDIT AND ENFORCE MODE

This just applies to ON-PREM. Password protection is always on for cloud identities.

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-operations#enable-on-premises-password-protection

Second of all - Azure AD Password Protection's Modern Approach

Azure AD Password Protection doesn't rely on a points system. Instead uses,

-Banned Password Lists

-Smart Detection Algorithms

-Policy Enforcement

Summarizing, Complexity Points Don't Override Banned Terms.

Third of all,

N –Policy applies when the password is changed

N – The new password matches the banner (Complexity doesn't override Banned Terms)

Y – Audit mode is enabled which affects just ON-PREM

upvoted 3 times

chema77 9 months, 3 weeks ago

I would go for NYY:

User1 will be prompted to change the password in the next sign in
Password Protection Enforcement: Only applies during password changes, not during sign-ins.
Answer: No

User2 can change the password to @d@tum_C0mpleX123
Fuzzy Matching: No match.
Substring Matching: No direct match.
Score Calculation: High score due to complexity. adatum [1] + _ [2] + complex [3] + 1 [4] + 2 [5] + 3 [6]
Answer: Yes

User3 can change the password to Adatum123!
Fuzzy Matching: Exact match with “Adatum.”
Substring Matching: Contains “Adatum.”
Score Calculation: Low score due to banned word. However, since Audit mode applies, the change will be logged but not blocked.
Answer: Yes
upvoted 3 times

chema77 9 months, 3 weeks ago
For #2, assumed that tenant name is not Adatum and the user's name is not Adatum.
upvoted 1 times

pentium75 11 months ago
User1 - No (password protection is applied at password change)
User2 - No (he is native Entra user, audit mode applies only to on-premises AD)
User3 - Yes (he is on-premises user that uses audit mode, and the password is not in the list)
upvoted 3 times

Apptech 1 year, 1 month ago
NNY is correct. Here is why: 1. Existing passwords cannpot be checked . 2. The custom banned password list considers common character substitution, such as "o" and "0", or "a" and "@". --> Conclussion @d@tum_Complex123 contains a banned word 3. Audit mode is only for OnPremAD
upvoted 4 times

Sparkletoss 1 year ago
I think user2 is yes because the mode is not enforced and set to audit. if it is enforced, then the custom will ban character substitution. That is how I see it
upvoted 2 times

pentium75 11 months ago
Audit mode applies to on-premises AD, User2 is native Entra user
upvoted 2 times

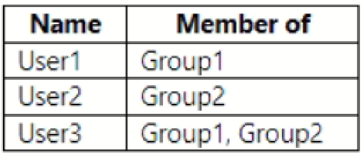
Alagong 1 year, 2 months ago
gonna with NNY
upvoted 4 times

Question #114 *Topic 2*

HOTSPOT

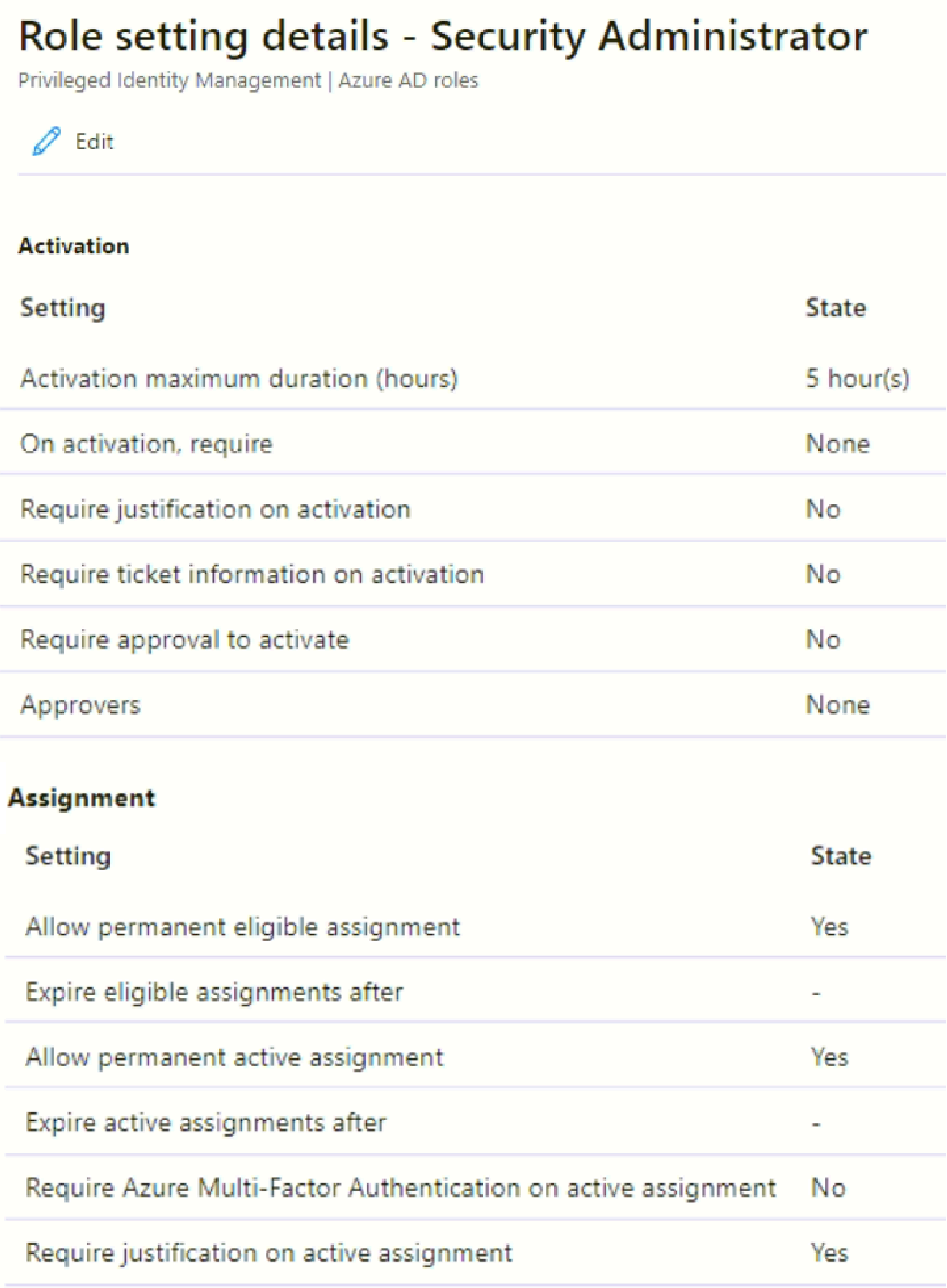
-

You have a Microsoft Entra tenant that contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Microsoft Entra Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.



Role setting details - Security Administrator

Privileged Identity Management | Azure AD roles

Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
On activation, require	None
Require justification on activation	No
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

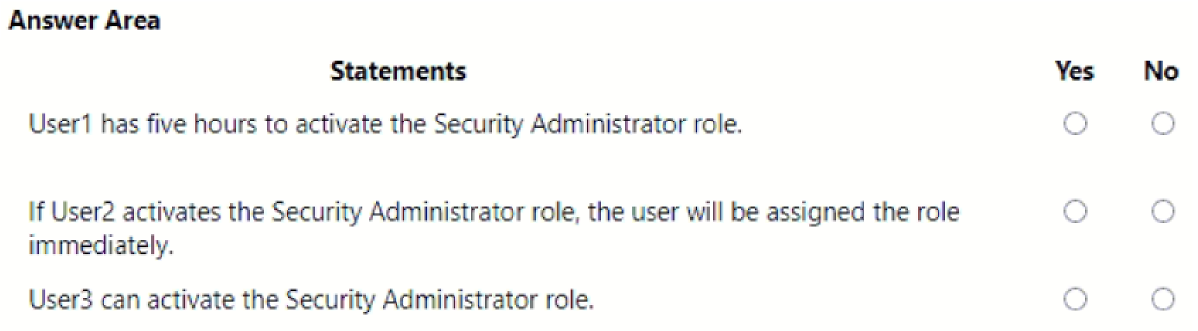
Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

From PIM, you assign the Security Administrator role to the following groups:

- Group1: Active assignment type, permanently assigned
- Group2: Eligible assignment type, permanently eligible

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

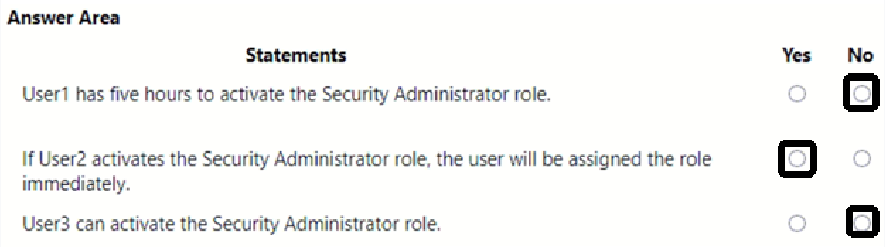
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 has five hours to activate the Security Administrator role.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 has five hours to activate the Security Administrator role.	○	[✓ ○]
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	[✓ ○]	○
User3 can activate the Security Administrator role.	○	[✓ ○]

chiquito Highly Voted 1 year, 2 months ago

Think NYN is ok based on this:

No - User1 is a member of Group1: that has Active assignment type, permanently assigned. Active assignments don't require the member to perform any activations to use the role. Members or owners assigned as active have the privileges assigned to the role at all times.

Yes – No approval is required. There is no waiting.

No – User3 is a member of Group1 and Group 2. Active assignments don't require the member to perform any activations to use the role.

Reference:
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/groups-assign-member-owner

upvoted 12 times

91743b3 Highly Voted 10 months, 3 weeks ago

On exam Aug 06 2024

upvoted 6 times

Question #115 *Topic 2*

DRAG DROP

-

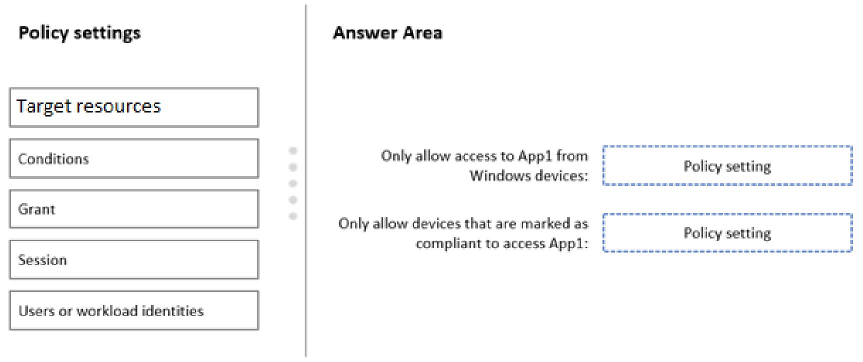
You have an Azure subscription that contains an Azure web app named App1.

You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:

• Only allow access to App1 from Windows devices.
• Only allow devices that are marked as compliant to access App1.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting 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.



Policy settings

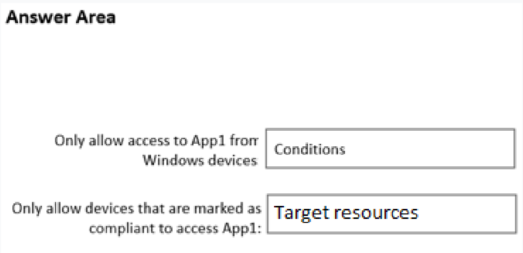
- Target resources
- Conditions
- Grant
- Session
- Users or workload identities

Answer Area

Only allow access to App1 from Windows devices: Policy setting

Only allow devices that are marked as compliant to access App1: Policy setting

Suggested Answer:



Answer Area

Only allow access to App1 from Windows devices: Conditions

Only allow devices that are marked as compliant to access App1: Target resources

chiquito Highly Voted 1 year, 2 months ago

Think the correct answers should be :

Box 1: Conditions

Next, configure Conditions. Select the signals you want to use as conditions for this policy. Options include:

• User risk
• Sign-in risk
• Device platforms
• Locations
• Client apps
• Filter for devices

Box2: Grant

Grant access: The users specified in this policy are granted access, but you can require any of the following further actions:

o Require multi-factor authentication
o Require authentication strength
o Require device to be marked as compliant - This option is required for the policy to use device compliance status.
o Require Microsoft Entra hybrid joined device
o Require approved client app
o Require app protection policy
o Require password change

Reference:

Reference:

https://learn.microsoft.com/en-us/mem/intune/protect/create-conditional-access-intune

upvoted 20 times

⊟ **8de3321** 7 months ago

So cringe when the website gives you wrong answer, especially after you pay for the service.

upvoted 2 times

⊟ **Jimmy500** 1 year ago

You are correct!

upvoted 3 times

⊟ **pentium75** Highly Voted 11 months ago

Conditions

Grant

upvoted 6 times

⊟ **Pamban** Most Recent 1 year, 1 month ago

another repeat question!

upvoted 3 times

⊟ **e2b11ca** 1 year, 2 months ago

Confirmed in lab. Correct answer is Box1: Conditions (User & Sign-in Risk, device platforms, locations, etc) & Box2: Grant (Block or Grant access for MFA, Compliant, hybrid joined devices, etc)

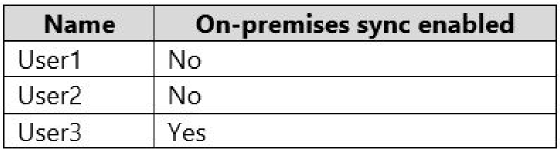
upvoted 4 times

Question #116 Topic 2

HOTSPOT

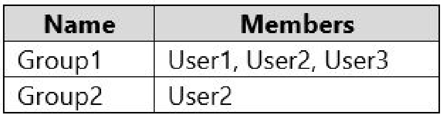
-

Your network contains an on-premises Active Directory domain that syncs to a Microsoft Entra tenant. The tenant contains the users shown in the following table.



Name	On-premises sync enabled
User1	No
User2	No
User3	Yes

The tenant contains the groups shown in the following table.



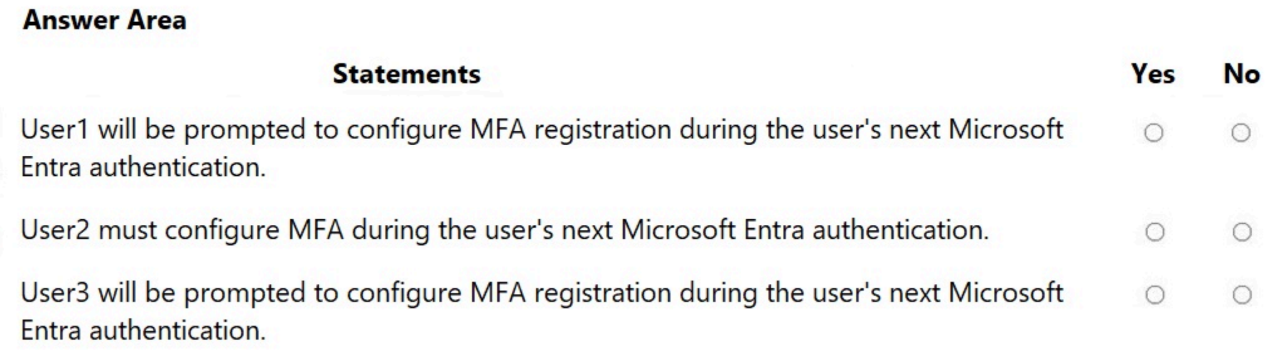
Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

• Assignments:
o Include: Group1
o Exclude: Group2
• Controls: Require Azure MFA registration
• Enforce Policy: On

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

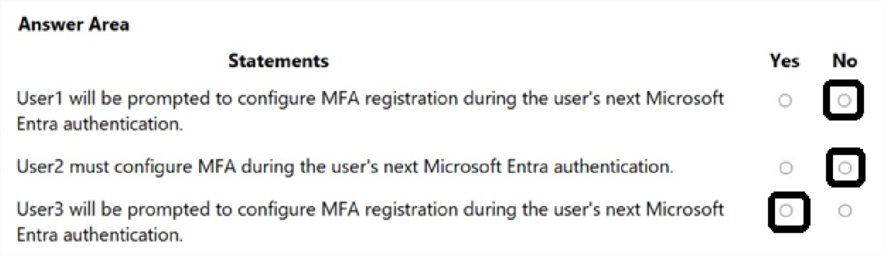
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	○	○
User2 must configure MFA during the user's next Microsoft Entra authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	○	[✓ ○]
User2 must configure MFA during the user's next Microsoft Entra authentication.	○	[✓ ○]
User3 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	[✓ ○]	○

⊟ **Jimmy500** Highly Voted 1 year ago

I think answer should be Yes,No,Yes. Here On-premisses sync does not make any sense as MFA applies user in the Azure if users already synced to Azure we are free to enforce mfa to them (question says users are already in Entra Id) So feel free to Mfa

upvoted 14 times

⊟ **belyo** Most Recent 1 month, 3 weeks ago funny how it states users arent synced, but at the same time ask on next Entra authentication...

how can you not exist in entra and in the same time being auth against it

upvoted 1 times

alzdashti 1 month, 4 weeks ago

No, No, Yes

The answer is correct. User 1 and User 2 are not synced, so they cannot even log in to Entra.

upvoted 2 times

schpeter_091 7 months, 1 week ago

a bit off topic, but still relevant for the future:

From 2025 January:

""We're removing the option to skip multifactor authentication (MFA) registration for 14 days when security defaults are enabled. This means all users will be required to register for MFA on their first login after security defaults are turned on," said Microsoft's Nitika Gupta.

upvoted 4 times

8de3321 7 months ago

Wow, something new to learn all the time huh? By the way, when are you planning to take the exam? I already did one but failed.

upvoted 2 times

pentium75 11 months ago

User1: Yes (policy applies)

User2: No (excluded from policy)

User3: Yes (policy applies, that is synced from on-premises AD is irrelevant)

upvoted 4 times

8de3321 7 months ago

This website is cringe, getting the answers wrong and I cannot believe I paid for this service.

upvoted 2 times

SimarS 1 year ago

Why User1 will not be prompted to configure MFA registration and User3 have to register for MFA?

The only difference I can see - For User1 On-premises sync is not enabled but for User3 it is enabled.

upvoted 1 times

8de3321 7 months ago

All user excepted User 2 will be prompted to set up MFA. This website got the answers wrong. The answer is Y-N-Y.

upvoted 1 times

Apptech 1 year, 1 month ago

I go for YNN. User1: see Pambans explanation. User2: group exclusion overrides 3. synched user will also get registration promt. He is not forced toi register for 14 days, but the promt will appear

upvoted 1 times

Apptech 1 year, 1 month ago

sorry for mistyping: in conclusion to my explanations YNY

upvoted 5 times

Pamban 1 year, 2 months ago

I think box 1 should be YES

explanation: When an administrator enables the Identity Protection policy requiring Microsoft Entra multifactor authentication registration, it ensures that users can use Microsoft Entra multifactor authentication to self-remediate in the future. Configuring this policy gives your users a 14-day period where they can choose to register and at the end are forced to register.

https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-user-experience#multifactor-authentication-registration

upvoted 3 times

Apptech 1 year, 2 months ago

Even if User2 would be a synched account he wouldn't need to register for MFA because group exclusion overrides in this case

upvoted 2 times

danielklein09 1 year, 2 months ago

Agree, only User 3 is synced sonhe will need MFA

upvoted 1 times

Question #117 *Topic 2*

You have a Microsoft Entra tenant named contoso.com.

You plan to collaborate with a partner organization that has a Microsoft Entra tenant named fabrikam.com.

Fabrikam.com uses the following identity providers:

- Google Cloud Platform (GCP)
- Microsoft accounts
- Microsoft Entra ID

You need to configure the Cross-tenant access settings for B2B collaboration.

Which identity providers support cross-tenant access?

A. Microsoft Entra ID only

B. GCP and Microsoft Entra ID only

C. Microsoft accounts and Microsoft Entra ID only

D. GCP, Microsoft accounts, and Microsoft Entra ID

Suggested Answer: *C*

Community vote distribution

D (57%) A (43%)

Pamban Highly Voted 1 year, 2 months ago

Selected Answer: D

I would go for D

Link: https://learn.microsoft.com/en-us/entra/external-id/identity-providers

upvoted 5 times

Saluk_DE Most Recent 1 month ago

Selected Answer: A

The word cross-"tenant" alone indicates that it is a MS Entra ID only thing!

upvoted 1 times

ca7859c 1 month ago

Selected Answer: A

A

Cross Tenant access is only for External Entra ID tenants.

Refer to this video at minute 8:35 (the screen says the same thing)

https://www.youtube.com/watch?v=3Pi_-pHIT_4

upvoted 1 times

Hot_156 4 months, 2 weeks ago

Selected Answer: A

The three of them can be granted access through B2B !!!!BUT!!!! not for cross-tenant access settings!

upvoted 3 times

roky008 4 months, 2 weeks ago

Selected Answer: A

Cross-tenant access settings for B2B collaboration in Microsoft Entra ID allow secure and managed collaboration between different Microsoft Entra tenants.

However, only Microsoft Entra ID supports cross-tenant access settings. Other identity providers, such as Google Cloud Platform (GCP) and Microsoft accounts (personal accounts like Outlook.com or Hotmail.com), do not support cross-tenant access settings in Microsoft Entra ID.

upvoted 1 times

ITFranz 4 months, 3 weeks ago

Selected Answer: A

To support the Answer:

fabrikam.com uses multiple identity providers (GCP, Microsoft accounts, and Microsoft Entra ID), only their Microsoft Entra ID identities will be able to leverage the cross-tenant access settings for B2B collaboration with your contoso.com tenant.

Google Cloud Platform (GCP) and Microsoft accounts are not directly supported for cross-tenant access in this context.

For cross-tenant access settings in B2B collaboration between your Microsoft Entra tenant (contoso.com) and the partner organization's tenant (fabrikam.com), only Microsoft Entra ID is supported as the identity provider.

Cross-tenant access settings are specifically designed for collaboration between Microsoft Entra organizations. They allow you to configure inbound and outbound access policies, trust multifactor authentication (MFA), and device claims from other Microsoft Entra tenants.

Answer = A

upvoted 2 times

Hot_156 4 months, 2 weeks ago

This is correct!

The three of them can be granted access through B2B BUT not for cross-tenant access settings!

upvoted 1 times

62Juan 6 months, 1 week ago

Selected Answer: D

B2B collaboration lets you invite external partners to access your Microsoft, SaaS, or custom-developed apps. B2B collaboration is especially useful when the external partner doesn't use Microsoft Entra ID or it's not practical or possible to set up B2B direct connect. B2B collaboration allows external users to sign in using their preferred identity, including their Microsoft Entra account, consumer Microsoft account, or a social identity you enable such as Google. With B2B collaboration, you can let external users sign in to your Microsoft applications, SaaS apps, custom-developed apps, and so on.

https://learn.microsoft.com/en-us/entra/external-id/b2b-direct-connect-overview

upvoted 1 times

JBAnalyst 6 months, 3 weeks ago

Selected Answer: D

For external Id : Ms entra id, a Microsoft email account , one time passcode via email of your choice , google, facebook , SAML, and I think apple too

Not sure about apple though, read that somewhere

upvoted 1 times

obaemf 9 months, 1 week ago

Selected Answer: A

https://learn.microsoft.com/en-us/entra/external-id/cross-tenant-access-settings-b2b-collaboration

upvoted 2 times

8de3321 7 months ago

Where exactly does it say that? Please highlight the part, right-click, then click 'Copy link to highlight'.

upvoted 1 times

obaemf 9 months, 3 weeks ago

Answer: A

Cross-tenant access settings is for B2B collaboration between Microsoft Entra organisations.

https://learn.microsoft.com/en-us/entra/external-id/cross-tenant-access-settings-b2b-collaboration

upvoted 2 times

nExoR 11 months ago

"You need to *configure the Cross-tenant access settings* for B2B collaboration." - although Microsoft Account can share files with other providers, you can't set up any global settings/policies. each share must be separately configured during creation. thus C makes most sense - these are 'corporate solutions' giving ability to be configured (settings set).

upvoted 1 times

nExoR 11 months ago

sorry - 'B' makes most sense...

upvoted 1 times

⊟ **pentium75** 11 months ago

Selected Answer: A

"Cross-TENANT access" is about other [Entra] tenants. Of course you can establish trusts with Google Cloud etc., but you cannot grant access to the Google Cloud users already trusted by the other tenant.

upvoted 1 times

⊟ **ruscomike** 11 months, 3 weeks ago

Selected Answer: A

another not clear question:

if the question is "You need to configure the Cross-tenant "access settings*" I will go for A, only Entra ID tenant supports cross-tenant access settings (like trust settings).

If the question is "You need to configure the Cross-tenant access" I will go for D: I can create B2B configuration for all the listed providers

upvoted 2 times

⊟ **ruscomike** 11 months, 3 weeks ago

another not clear question:

if the question is "You need to configure the Cross-tenant "access settings*" I will go for A, only Entra ID tenant supports cross-tenant access settings (like trust settings).

If the question is "You need to configure the Cross-tenant access" I will go for D: I can create B2B configuration for all the listed providers

upvoted 1 times

⊟ **JaridB** 1 year, 2 months ago

D. GCP (Google Cloud Platform, referred to as Google federation), Microsoft accounts, and Microsoft Entra ID. - The identity providers that support cross-tenant access settings for B2B collaboration in Microsoft Entra include Microsoft Entra ID, Microsoft accounts, and Google federation. This means you can configure cross-tenant access to allow guest users to authenticate using their Microsoft Entra accounts, personal Microsoft accounts, or their Google accounts.

upvoted 1 times

⊟ **Apptech** 1 year, 2 months ago

I go with C) GCP accounts are associated with Google Cloud services. they are not directly used for Microsoft Entra cross-tenant collaboration. Within a single tenant it is possible to invite a GCP user but it is not possible to be used for cross tenant scenarios

upvoted 1 times

⊟ **Apptech** 1 year, 1 month ago

In addition: I checked the settings in entra admin center for external identities --> Cross tenant settings. With the organizational settings of the cross-tenant access settings it says: "Use cross-tenant access settings to manage collaboration with external Microsoft Entra tenants. For non-Microsoft Entra tenants, use collaboration settings." In the external collaboration settings you can invite guest users to your tenant. And yes, there you can add GCP users

upvoted 3 times

⊟ **ruscomike** 11 months, 3 weeks ago

for the same reason you can't add Microsoft Accounts. Whan you add an org in cross-tenant access settings you see "Add an external Microsoft Entra tenant by typing one of its domain names or tenant ID if from another Microsoft cloud."

upvoted 1 times

Question #118 *Topic 2*

You have a Microsoft Entra tenant named contoso.com.

You have a partner company that has a Microsoft Entra tenant named fabrikam.com.

You need to ensure that when a user in fabrikam.com attempts to access the resources in contoso.com, the user only receives a single Microsoft Entra Multi-Factor Authentication (MFA) prompt. The solution must minimize administrative effort.

What should you do?

A. From the Azure portal of contoso.com, configure the inbound access default settings.

B. From the Azure portal of contoso.com, configure the External collaboration settings.

C. From the Azure portal of contoso.com, configure the outbound access default settings.

D. From the Azure portal of fabrikam.com, configure the outbound access default settings.

Suggested Answer: *B*

Community vote distribution

A (100%)

pentium75 11 months ago

Selected Answer: A

Not B, "External collaboration settings" are about what guests can access but have nothing to do with MFA prompts. That is in the Cross-tenant access settings.

upvoted 2 times

8de3321 7 months ago

I was wondering if it is B. Thanks for your input.

upvoted 1 times

ruscomike 11 months, 3 weeks ago

Selected Answer: A

agree with A, even if ot could be better modify the setting just for fabrikam and not all the inbound default as suggested in the answer :-P

upvoted 1 times

ceejay12 1 year ago

Selected Answer: A

Agreed, A

upvoted 1 times

NK203 1 year, 1 month ago

Agree A.

Not select B,Reason :https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure

upvoted 3 times

Pamban 1 year, 2 months ago

Selected Answer: A

I would go with A

Trust multi-factor authentication from Microsoft Entra tenants: Select this checkbox to allow your Conditional Access policies to trust MFA claims from external organizations. During authentication, Microsoft Entra ID checks a user's credentials for a claim that the user completed MFA. If not, an MFA challenge is initiated in the user's home tenant.

Link: https://learn.microsoft.com/en-us/entra/external-id/cross-tenant-access-settings-b2b-collaboration#to-change-inbound-trust-settings-for-mfa-and-device-claims

upvoted 3 times

danielklein09 1 year, 2 months ago

Agree, B

upvoted 2 times

Question #119 *Topic 2*

DRAG DROP

-

You have a Microsoft Entra tenant.

On January 1, you configure a multi-factor authentication (MFA) registration policy that has the following settings:

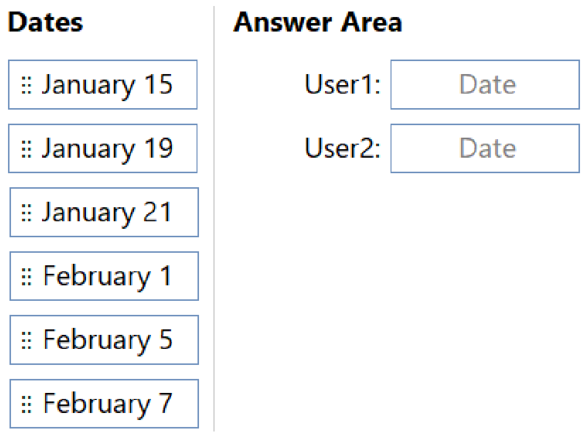
• Assignments: All users
• Require Microsoft Entra ID multifactor authentication registration: Enabled
• Enforce policy: On

On January 3, you create two new users named User1 and User2.

On January 5, User1 authenticates to Microsoft Entra ID for the first time. On January 7, User2 authenticates to Microsoft Entra ID for the first time.

On which date will User1 and User2 be forced to register for MFA? To answer, drag the appropriate dates to the correct users. Each date 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.



Dates

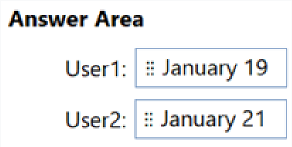
- January 15
- January 19
- January 21
- February 1
- February 5
- February 7

Answer Area

User1: Date

User2: Date

Suggested Answer:



Answer Area

User1: January 19

User2: January 21

SofiaLorean 3 months, 2 weeks ago

https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-mfa-policy

upvoted 1 times

golitech 4 months, 4 weeks ago

From 2025 January:

""We're removing the option to skip multifactor authentication (MFA) registration for 14 days when security defaults are enabled. This means all users will be required to register for MFA on their first login after security defaults are turned on"

https://techcommunity.microsoft.com/blog/microsoft-entra-blog/update-to-security-defaults/4044868

upvoted 4 times

Nhadipour 4 months, 3 weeks ago

So now the correct answers are 5th and 7th, right?

upvoted 3 times

Apptech 8 months, 1 week ago

Correct: https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-mfa-policy

upvoted 4 times

goalkiller 8 months, 1 week ago

correct answer. After 14days of first logon it will be enforced.

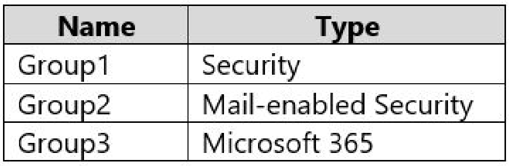
upvoted 3 times

Question #120 Topic 2

HOTSPOT

-

You have a Microsoft Entra tenant that contains the groups shown in the following table.

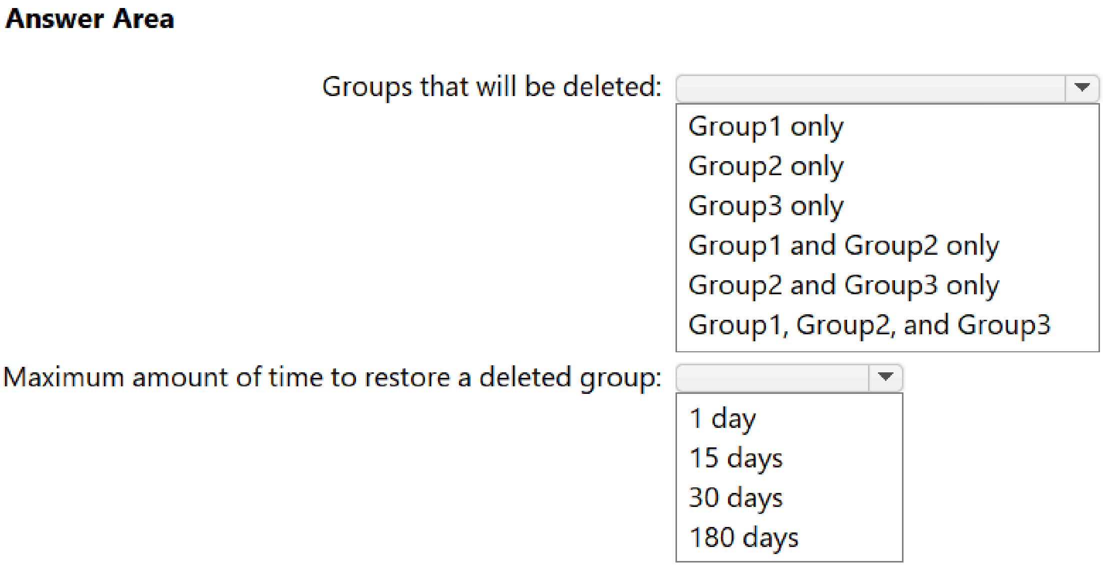


Name	Type
Group1	Security
Group2	Mail-enabled Security
Group3	Microsoft 365

From the Azure portal, you configure a group expiration policy that has a lifetime of 180 days.

Which groups will be deleted after 180 days of inactivity, and what is the maximum amount of time you have to restore a deleted group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

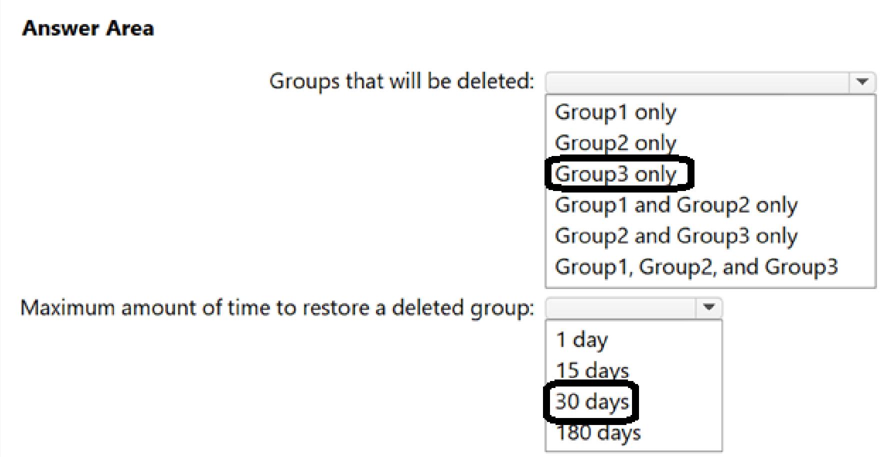


Answer Area

Groups that will be deleted:
Group1 only
Group2 only
Group3 only
Group1 and Group2 only
Group2 and Group3 only
Group1, Group2, and Group3

Maximum amount of time to restore a deleted group:
1 day
15 days
30 days
180 days

Suggested Answer:



Answer Area

Groups that will be deleted:
Group1 only
Group2 only
[✓ Group3 only]
Group1 and Group2 only
Group2 and Group3 only
Group1, Group2, and Group3

Maximum amount of time to restore a deleted group:
1 day
15 days
[✓ 30 days]
180 days

obaemf Highly Voted 9 months, 3 weeks ago

Group 3 only
30 days

You can set an expiration policy only for Microsoft 365 groups in Microsoft Entra ID.
Any Microsoft 365 group that was deleted can be restored within 30 days by the group owners or the administrator.

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

upvoted 8 times

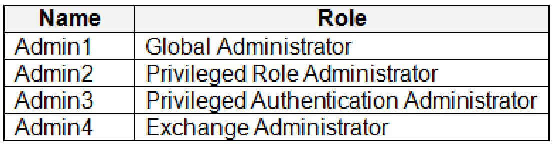
⊟ **ca7859c** 1 month ago

Thank you brother

upvoted 1 times

Question #121 *Topic 2*

You have a Microsoft Entra tenant that uses Microsoft Entra Permissions Management and contains the accounts shown in the following table:



Name	Role
Admin1	Global Administrator
Admin2	Privileged Role Administrator
Admin3	Privileged Authentication Administrator
Admin4	Exchange Administrator

Which accounts will be listed as assigned to highly privileged roles on the Azure AD insights tab in the Entra Permissions Management portal?

A. Admin1 only

B. Admin2 and Admin3 only

C. Admin2 and Admin4 only

D. Admin1, Admin2, and Admin3 only

E. Admin2, Admin3, and Admin4 only

F. Admin1, Admin2, Admin3, and Admin4

Suggested Answer: *C*

Community vote distribution

C (100%)

obaemf Highly Voted 9 months, 3 weeks ago

I go with D

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

https://learn.microsoft.com/en-us/entra/permissions-management/product-privileged-role-insights

Microsoft recommends that organizations have two cloud-only emergency access accounts permanently assigned the Global Administrator role. These accounts are highly privileged and aren't assigned to specific individuals.

So I would say Global Administrator role is highly privileged.

upvoted 11 times

ca7859c Most Recent 2 weeks, 6 days ago

Selected Answer: C

Review highly privileged roles or Review service principals to review information on principal role assignments for the following roles: Application Administrator, Cloud Application Administrator, Exchange Administrator, Intune Administrator, Privileged Role Administrator, SharePoint Administrator, Security Administrator, User Administrator.

https://learn.microsoft.com/en-us/entra/permissions-management/product-privileged-role-insights

upvoted 2 times

Knighthell 2 weeks, 1 day ago

correct

upvoted 1 times

mmmyo 1 month, 3 weeks ago

Selected Answer: D

✅ Global Administrator (Admin1) → Full control over all settings in the tenant, highest privilege. ✅ Privileged Role Administrator (Admin2) → Manages role assignments and elevated access for other administrators. ✅ Privileged Authentication Administrator (Admin3) → Manages authentication-related policies and security configurations.

□ Exchange Administrator (Admin4) is not considered a highly privileged role in this context. While it has control over Exchange Online, it does not manage tenant-wide security or role assignments, so it is excluded from the highly privileged roles list.

upvoted 1 times

Sweet_Caroline 2 months, 2 weeks ago

Selected Answer: D

All except from Exchange admin have the Privileged tag in the Roles and Administrators blade of Entra ID.

upvoted 1 times

espbo 2 months, 3 weeks ago

Selected Answer: D

for sure

upvoted 1 times

espbo 2 months, 3 weeks ago

Selected Answer: D

for sure

upvoted 1 times

randy0077 3 months, 2 weeks ago

Selected Answer: D

Tested in Lab: d is correct ans.

upvoted 1 times

1dd60c0 3 months, 3 weeks ago

Selected Answer: D

This learn doc has an obvious label that says "Privileged" next to those roles that are Highly Privileged. Exchange Administrator doesn't have the "Privileged" label but the other 3 do.

The answer is 100% without doubt D.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

upvoted 2 times

sgomezsan 4 months, 1 week ago

Selected Answer: D

Global Administrator role is highly privileged but not exchange admin.

upvoted 1 times

Hot_156 3 months, 4 weeks ago

It is about the "highly privileged roles on the Azure AD insights" and if you check the documentation and the tab, you will see this

https://learn.microsoft.com/en-us/entra/permissions-management/product-privileged-role-insights#view-information-in-the-microsoft-entra-insights-tab

upvoted 1 times

golitech 4 months, 4 weeks ago

Selected Answer: C

the Insights tab in the Microsoft Entra Permissions Management portal focuses on users assigned to specific highly privileged roles. These roles include:

Application Administrator
Cloud Application Administrator
Exchange Administrator
Intune Administrator
Privileged Role Administrator
SharePoint Administrator
Security Administrator
User Administrator

upvoted 3 times

Renne373 5 months, 1 week ago

Selected Answer: D

D exchange not privileged role
global admin priviliged

upvoted 1 times

62Juan 6 months, 1 week ago

Selected Answer: C

https://learn.microsoft.com/en-us/entra/permissions-management/product-privileged-role-insights#view-information-in-the-microsoft-entra-insights-tab

upvoted 4 times

JBAnalyst 6 months, 3 weeks ago

Selected Answer: D

Exchange is not a privileged role
For list of roles /privileged roles
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

upvoted 4 times

e31180b 8 months ago

Selected Answer: C

According to copilot

In the Microsoft Entra Permissions Management Portal, some of the highly privileged roles include:

Global Administrator: This role has access to all administrative features in Microsoft Entra and other Microsoft services.
Privileged Role Administrator: Manages role assignments in Microsoft Entra, including the ability to assign and remove roles.
Security Administrator: Has permissions to manage security-related features and settings.
Exchange Administrator: Manages mail settings and features in Exchange Online.
SharePoint Administrator: Manages SharePoint Online settings and features.
Intune Administrator: Manages devices and applications through Microsoft Intune.
Application Administrator: Manages application registrations and enterprise applications.
Cloud Application Administrator: Manages cloud applications and their settings.
User Administrator: Manages user accounts and groups

https://learn.microsoft.com/en-us/entra/permissions-management/product-privileged-role-insights

upvoted 2 times

> **golitech** 4 months, 4 weeks ago
>
> u mention "Exchange admin" in ur comment, but it is not in your chosen answer!!!
>
> upvoted 1 times
>
> > **ca7859c** 2 weeks, 6 days ago
> >
> > Admin4 is the Exchange Admin
> >
> > upvoted 1 times

NeoTactics 9 months, 3 weeks ago

Selected Answer: C

From https://learn.microsoft.com/en-us/entra/permissions-management/product-privileged-role-insights#view-information-in-the-microsoft-entra-insights-tab

Select Review highly privileged roles or Review service principals to review information on principal role assignments for the following roles: Application Administrator, Cloud Application Administrator, Exchange Administrator, Intune Administrator, Privileged Role Administrator, SharePoint Administrator, Security Administrator, User Administrator.

So, answer is: C
(Admin2 and Admin4 only)

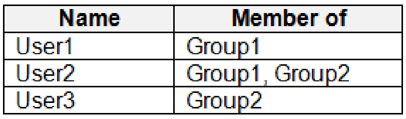
upvoted 2 times

Question #122 *Topic 2*

HOTSPOT

-

You have a Microsoft Entra tenant that contains the user shown in the following table.



Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

You configure a Conditional Access policy that has the following settings:

• Name:CAPolicy1

• Assignments

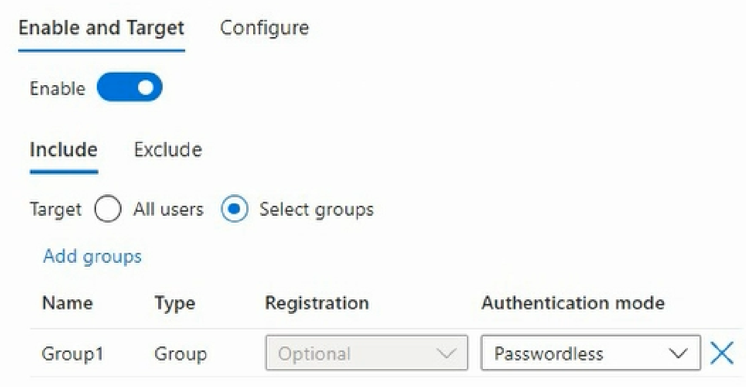
o Users or workload identities: Group1

o Target resources: All cloud apps

• Access controls

o Grant access: Require multifactor authentication

From Microsoft Authenticator settings for the tenant, the Enable and Target settings are configured as shown in the Enable and Target exhibit. (Click the Enable and Target tab.)



Enable and Target Configure

Enable: On

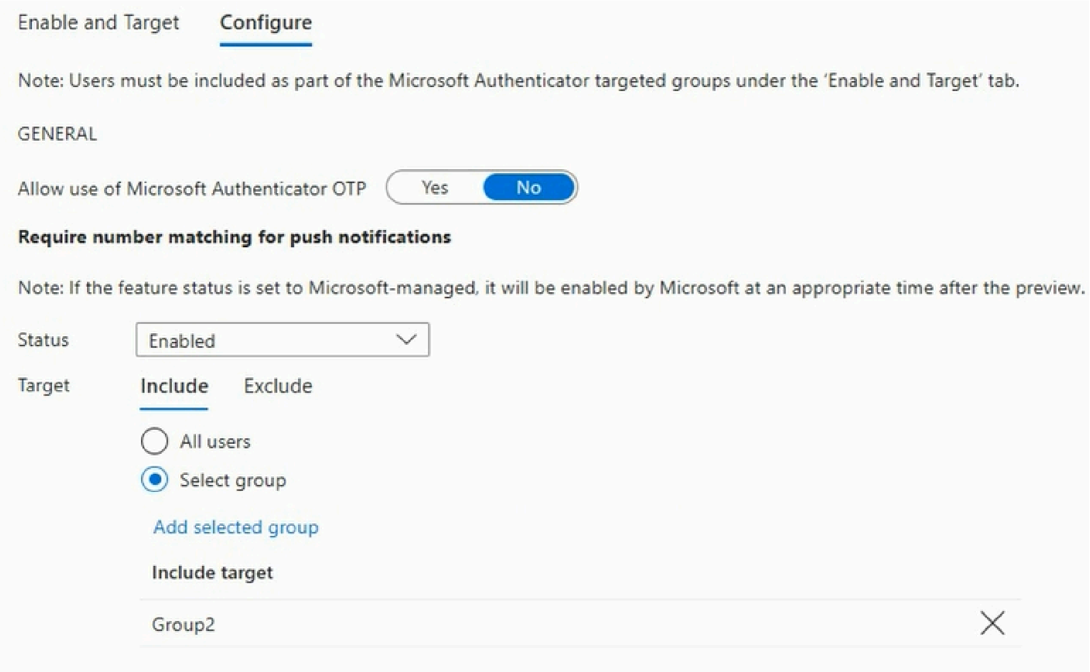
Include Exclude

Target ○ All users ● Select groups

Add groups

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless

From Microsoft Authenticator settings for the tenant, the Configure settings are configured as shown in the Configure exhibit. (Click the Configure tab.)



Enable and Target **Configure**

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the 'Enable and Target' tab.

GENERAL

Allow use of Microsoft Authenticator OTP Yes [✓ No]

Require number matching for push notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview.

Status: Enabled

Target **Include** Exclude

○ All users

● Select group

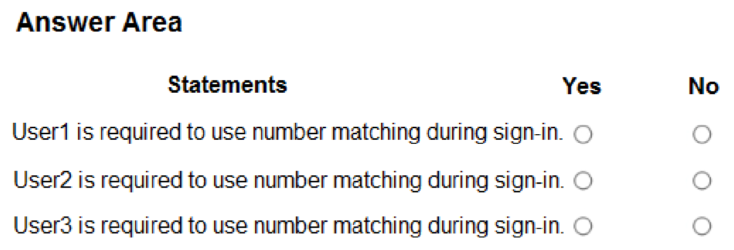
Add selected group

Include target

Group2

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

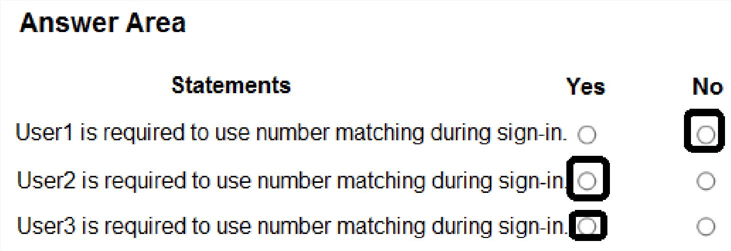
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 is required to use number matching during sign-in.	○	○
User2 is required to use number matching during sign-in.	○	○
User3 is required to use number matching during sign-in.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 is required to use number matching during sign-in.	○	[✓ ○]
User2 is required to use number matching during sign-in.	[✓ ○]	○
User3 is required to use number matching during sign-in.	[✓ ○]	○

⊟ **mmmyo** 1 month, 3 weeks ago

Policy & Settings Breakdown

CAPolicy1 requires MFA for Group1 members (User1, User2).

Group1 is enabled for passwordless authentication (User1, User2).

Microsoft Authenticator settings for Group2:

MFA OTP is disabled.

Number matching is enforced.

User1 (Group1 Member)

Enforced MFA due to CAPolicy1.

Enabled for passwordless authentication.

Not part of Group2, meaning number matching enforcement does not apply.

Answer: No (Not required to use number matching).

User2 (Group1 & Group2 Member)

Enforced MFA due to CAPolicy1.

In Group2, where number matching is enabled in Microsoft Authenticator settings.

Answer: Yes (Required to use number matching).

User3 (Group2 Member Only)

Not part of CAPolicy1, meaning MFA is not enforced.

However, since Group2 is targeted for number matching, if User3 performs any MFA-related authentication, number matching will be enforced.

Answer: Yes (Required to use number matching).

No, Yes, Yes is correct answer.

upvoted 1 times

⊟ **obaemf** 9 months, 3 weeks ago

NYN

User1: Any method

User2: Number matching

User3: CA does not apply to group2

upvoted 3 times

⊟ **obaemf** 9 months, 1 week ago

NYY is correct.

All group 2 members must use number matching

upvoted 3 times

⊟ **2b58229** 6 months, 2 weeks ago

CA does not apply to group2. In second screendump it even states "Note: Users must be included as part of the Microsoft Authenticator Targeted Groups". Going back to screendump 1 you see that only group 1 is targeted.

upvoted 1 times

⊟ **Nxjib** 6 months ago

So meaning answer should be YNN?

upvoted 1 times

⊟ **JBAnalyst** 6 months ago

Given answer is right,

The "Note: Users must be included as part of the Microsoft Authenticator Targeted Groups" is for for the one time password, I believe this can be sent via email to the user, that function is turned off,
so user1 can use all types of passwordless authentication except the OTP

NYY is correct

upvoted 1 times

Question #1 *Topic 3*

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ContReg1.
You enable content trust for ContReg1.
You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.
Which two roles should you assign to User1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. AcrQuarantineReader

B. Contributor

C. AcrPush

D. AcrImageSigner

E. AcrQuarantineWriter

Suggested Answer: *CD*
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

Community vote distribution
CD (100%)

P0d Highly Voted 4 years, 6 months ago
Contributor and AcrPush
upvoted 29 times

temidayo 4 years, 6 months ago
No, you are wrong,

Correct answer is
AcrPush
AcrImageSigner

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
upvoted 89 times

bluetaurianbull 3 years, 11 months ago
Super Confusing and Tricky:-
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles
As per the above link, AcrImageSigner role - only has permission to Sign Images but the text below seems to suggest that usually this permission of "S
principal. This permission is typically combined with push image to allow pushing a trusted image to a registry. For details, see Content trust in Azure

But then the confusion is, "Sign Images" seems usually assigned to an automated process, the question talks about assigning 2 roles (Principle of leas
AcrPush and Contributor. Ofcource Owner can also push an Image, but it will not follow the Principle of least privilege.
upvoted 3 times

eroms 3 years, 7 months ago
its fairly straightforward. No need for any long explanation. Answer is CD. Keyword Least privilege..
upvoted 2 times

gboyega 4 years, 5 months ago
Correct it should be
ArcPush and AcrImageSigner

Because the question states that we should follow the principle of least priviledge
upvoted 14 times

bluetaurianbull 3 years, 11 months ago

Super Confusing and Tricky:-

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

As per the above link, AcrImageSigner role - only has permission to Sign Images but the text below seems to suggest that usually this permission o

service principal. This permission is typically combined with push image to allow pushing a trusted image to a registry. For details, see Content trus

But then the confusion is, "Sign Images" seems usually assigned to an automated process, the question talks about assigning 2 roles (Principle of

AcrPush and Contributor. Ofcource Owner can also push an Image, but it will not follow the Principle of least privilege.

upvoted 1 times

Patchfox 2 years, 11 months ago

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli#:~:text=This%20permission%20is%20typically%20combined%20with%20push%20image%20to%20allow%20pushing%20a%20trusted%20image%20t

upvoted 2 times

rgullini 3 years, 8 months ago

Wrong. Correct answer is

AcrPush

AcrImageSigner

upvoted 47 times

gfhbox0083 Highly Voted 4 years, 6 months ago

C, D, for sure.

upvoted 16 times

hellboysecret Most Recent 3 months, 2 weeks ago

Selected Answer: CD

Role/Permission Access Resource Manager Create/delete registry Push image Pull image Delete image data Change policies Sign images

Owner X X X X X X

Contributor X X X X X X

Reader X X

AcrPush X X

AcrPull X

AcrDelete X

AcrImageSigner X

upvoted 1 times

sgomezsan 4 months, 1 week ago

Selected Answer: CD

Create trusted images: AcrPush and AcrImageSigner

upvoted 1 times

yonie 1 year ago

Selected Answer: CD

AcrPush

AcrImageSigner

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli

upvoted 1 times

JunetGoyal 1 year, 2 months ago

Given ans is correct. CD.

The combination of CD will fulfill required task

Those who are thinking "Contributor and AcrPush" we can give this too,but its not least priviledge.(Note: if you give contributor then you don't even need AcrPush).

So as per Question combination of CD enogh

upvoted 1 times

TheProfessor 1 year, 3 months ago

Selected Answer: CD

C. AcrPush

D. AcrImageSigner

upvoted 3 times

ErikPJordan 1 year, 3 months ago

Selected Answer: CD

Contributor is too much, AcrQuarantineReader/Writer sounds made up :D

upvoted 1 times

ESAJRR 1 year, 4 months ago

Selected Answer: CD

C. AcrPush

D. AcrImageSigner

upvoted 1 times

heatfan900 1 year, 4 months ago

The ability to SIGN images, usually assigned to an automated process, which would use a service principal. This permission is typically combined with PUSH image to allow pushing a trusted image to a registry.

upvoted 1 times

majstor86 1 year, 10 months ago

Selected Answer: CD

C. AcrPush

D. AcrImageSigner

upvoted 2 times

ligu 1 year, 10 months ago

Correct answer are AcrPush and AcrImageSigner (since July 2021)

upvoted 1 times

edurakhan 2 years, 1 month ago

Selected Answer: CD

C, D

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

upvoted 3 times

F117A_Stealth 2 years, 1 month ago

Selected Answer: CD

Correct answer is

AcrPush

AcrImageSigner

upvoted 1 times

koreshio 2 years, 2 months ago

Selected Answer: CD

as explained correctly by others as well.

upvoted 2 times

BlackZeros 2 years, 3 months ago

Selected Answer: CD

correct answer

upvoted 2 times

nitz14 2 years, 5 months ago

Selected Answer: CD

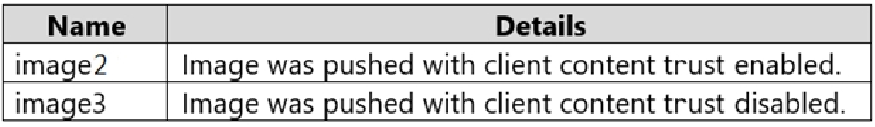
C & D,

reference : https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

upvoted 2 times

Question #2 *Topic 3*

You have an Azure Container Registry named ContReg1 that contains a container image named image1.
You enable content trust for ContReg1.
After content trust is enabled, you push two images to ContReg1 as shown in the following table.



Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

A. image1 and image2 only

B. image2 only

C. image1, image2, and image3

Suggested Answer: *B*
Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.
To push a trusted image tag to your container registry, enable content trust and push the image with docker push.
To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

Community vote distribution
B (100%)

DannyN1 Highly Voted 3 years, 8 months ago
jjeeeejejejee
upvoted 24 times

Adonist Highly Voted 3 years, 6 months ago
Correct answer.
Image1 was created before enabling content trust.
upvoted 8 times

cfsxtuv33 3 years, 5 months ago
Wish I could see Image 1...
upvoted 3 times

JakeCallham 2 years, 9 months ago
Doesnt matter. You should know what is is. If you don't than this question will fail. The whole point about these questions is knowing what a setting is. The description already tells you enough.
upvoted 3 times

DarkCyberGhost 3 years, 5 months ago
image1 is in the container before you enable content trust. and Iamge 3 has content trust disabled. so the answer can only be image 2 because its the only image with content trust enabled.
upvoted 4 times

Forex19 Most Recent 1 month, 3 weeks ago
Selected Answer: B
on exam 09\may\2025
upvoted 1 times

joshuactz 1 year, 2 months ago
Selected Answer: B
Correct Answer: B. image2 only

Explanation:
image1: There is no information provided about how image1 was pushed, whether it was before or after content trust was enabled, and whether it

was signed. Assuming it was in the registry before content trust was enabled and there's no mention of it being re-pushed with signing, it cannot be assumed to be trusted.

image2: As explicitly stated, it was pushed with client content trust enabled, making it a trusted image.

image3: It was explicitly stated that it was pushed with client content trust disabled, so it is not a trusted image.

upvoted 1 times

⊟ **ITFranz** 7 months, 3 weeks ago

The statement says (ContReg1 that already contains a container image named image1.)

hence only option is Image2 because it was uploaded after enabling the content trust.

upvoted 1 times

⊟ **ESAJRR** 1 year, 9 months ago

Selected Answer: B

B. image2 only

upvoted 1 times

⊟ **Self_Study** 1 year, 10 months ago

Selected Answer: B

On exam 7/8/23. Answers are correct.

upvoted 4 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: B

B. image2 only

upvoted 3 times

⊟ **ligu** 2 years, 4 months ago

Answer B is correct

upvoted 1 times

⊟ **01_01_2021** 3 years, 8 months ago

Image 1 settings are not shown.

upvoted 1 times

⊟ **JakeCallham** 2 years, 9 months ago

Well that's part of testing your knowledge. Microsoft validates if you are aware what the setting of image 1 will be AFTER setting contenttrust. Thats the whole point. The setting is also known, you don" t have to see it, as it wasn't enabled.

upvoted 4 times

Question #3 *Topic 3*

SIMULATION -

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

To enable the RDP port in an NSG, follow these steps:

1. Sign in to the Azure portal.
2. In Virtual Machines, select VM1
3. In Settings, select Networking.
4. In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300 -

Name: Port_3389 -

Port(Destination): 3389 -

Protocol: TCP -

Source: Any -

Destinations: Any -

Action: Allow -

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem

Spamuel Highly Voted 👍 4 years, 11 months ago

I would also say to have the source as Service Tag - Internet, so you only allow RDP connections over internet associated IPs rather than from ANY.

upvoted 33 times

planb7000 4 years, 11 months ago

Perfect! That will surely get you extra points.

upvoted 9 times

Nnanna29 4 years, 7 months ago

Definitely! It limits access to only internet instead of 'Any'

upvoted 4 times

hariprasad0511 Highly Voted 👍 3 years, 10 months ago

Its best to configure this way

1. Create VM in a private subnet
2. Create a Azure FW in another subnet
3. Then user NAT-GW to allow traffic from internet to access VM in private subnet via firewall
4. You can configure all rules to reduce attack surface form internet using the azure firewall

upvoted 13 times

91743b3 Most Recent 🕘 10 months, 3 weeks ago

On exam Aug 06 2024

upvoted 2 times

nExoR 11 months ago

bastion is limiting the attact surface even more than NSG...

upvoted 3 times

pentium75 11 months ago

We're asked to "minimize the attack surface", and JIT documentation explicitly mentions that JIT about 'reducing the attack surface' while Bastion documentation does not. As the question tend to follow documentation rather than reality, I'd vote for JIT.

upvoted 1 times

⊟ **TheProfessor** 1 year, 9 months ago

I think the best is JIT.

upvoted 2 times

⊟ **Pupu86** 2 years ago

bastion with JIT (assuming Windows Defender is enabled by default)

upvoted 3 times

⊟ **gbx077** 2 years, 3 months ago

# Exam question March 24, 2023

upvoted 4 times

⊟ **F117A_Stealth** 2 years, 7 months ago

I would actually select Source as "Service Tag" and Set it to "Internet" with Destination to the VM , Protocol as any or TCP and port 3389

upvoted 5 times

⊟ **joanjcanals** 2 years, 9 months ago

Could this question be related to the Just in Time VM access feature?

upvoted 2 times

⊟ **koreshio** 2 years, 8 months ago

exactly my thoughts as well. the key point is "Reduce attack surface". for any access to a VM (RDP port 3389, WinRM-Powershell port 5895,5986), if you need to reduce attack surface you need to ensure only Azure AD authenticated users can request access.

So the best options would be either Bastion access or even better JIT access.

upvoted 6 times

⊟ **Ivanvazovv** 2 years, 10 months ago

Bastion or at least JIT. Leaving 3389 open for internet is a bad idea.

upvoted 5 times

⊟ **OpsecDude** 2 years, 9 months ago

I would say JIT as Bastion is different from RDP

upvoted 1 times

⊟ **mung** 2 years, 7 months ago

How Bastion is different from RDP?
It is basically built for safe RDP connection

upvoted 2 times

⊟ **koreshio** 2 years, 8 months ago

why? they are both used for RDP access.

see these resources:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage?tabs=jit-config-asc%2Cjit-request-asc

https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows

upvoted 1 times

⊟ **imie** 3 years, 5 months ago

in Exam 31 Dec 2021.

upvoted 3 times

⊟ **orallony** 3 years, 9 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 3 times

⊟ **rainmakerho** 3 years, 9 months ago

Enable VM JIT?

upvoted 3 times

⊟ **poplovic** 3 years, 9 months ago

JIT is possible or bastion

upvoted 2 times

am20 4 years, 1 month ago

why not using bastion?

upvoted 4 times

am20 4 years, 1 month ago

https://docs.microsoft.com/en-us/azure/bastion/bastion-overview#architecture

upvoted 2 times

ChinkSantana 4 years ago

Bsstion is a good way.. But i doubt this is what the question was asking.

upvoted 2 times

rsamant 3 years, 6 months ago

i think it should be bastion as else we are not limiting the attack surface except opening rdp port directly to internet

upvoted 3 times

Fred64 4 years, 1 month ago

maybe we can deny all other rules as well?

upvoted 1 times

Question #4 *Topic 3*

SIMULATION -
You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.
To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*
1. In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.
2. When the name of your VM appears in the search results, select it.
3. Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface

111ssy Highly Voted 4 years, 10 months ago

1. In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine that has a network interface that you want to add to, or remove from, an application security group. When the name of your VM appears in the search results, select it.

2. Under SETTINGS, select Networking. Select Application Security Groups then Configure the application security groupselect the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save. Only network interfaces that exist in the same virtual network can be added to the same application security group. The application security group must exist in the same location as the network interface.

upvoted 25 times

gbx077 Highly Voted 2 years, 3 months ago

# Exam question March 24, 2023

upvoted 8 times

91743b3 Most Recent 10 months, 3 weeks ago

On exam Aug 06 2024

upvoted 2 times

imie 3 years, 5 months ago

in Exam 31 Dec 2021.

upvoted 4 times

Question #5 Topic 3

SIMULATION -

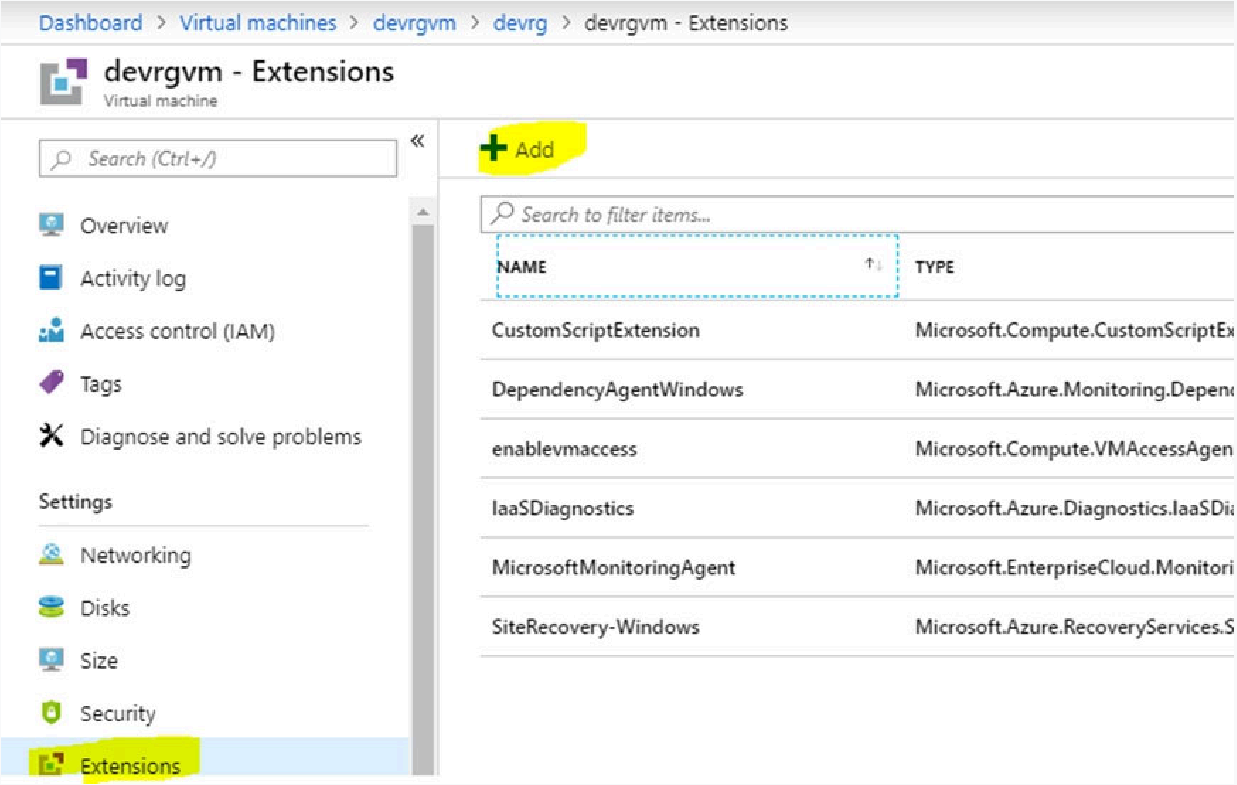
You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

Deploy the Microsoft Antimalware Extension using the Azure Portal for single VM deployment

1. In Azure Portal, go to the Azure VM1's blade, navigate to the Extensions section and press Add.



NAME	TYPE
CustomScriptExtension	Microsoft.Compute.CustomScriptEx
DependencyAgentWindows	Microsoft.Azure.Monitoring.Depen
enablevmaccess	Microsoft.Compute.VMAccessAgen
IaaSDiagnostics	Microsoft.Azure.Diagnostics.IaaSDi
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitori
SiteRecovery-Windows	Microsoft.Azure.RecoveryServices.S

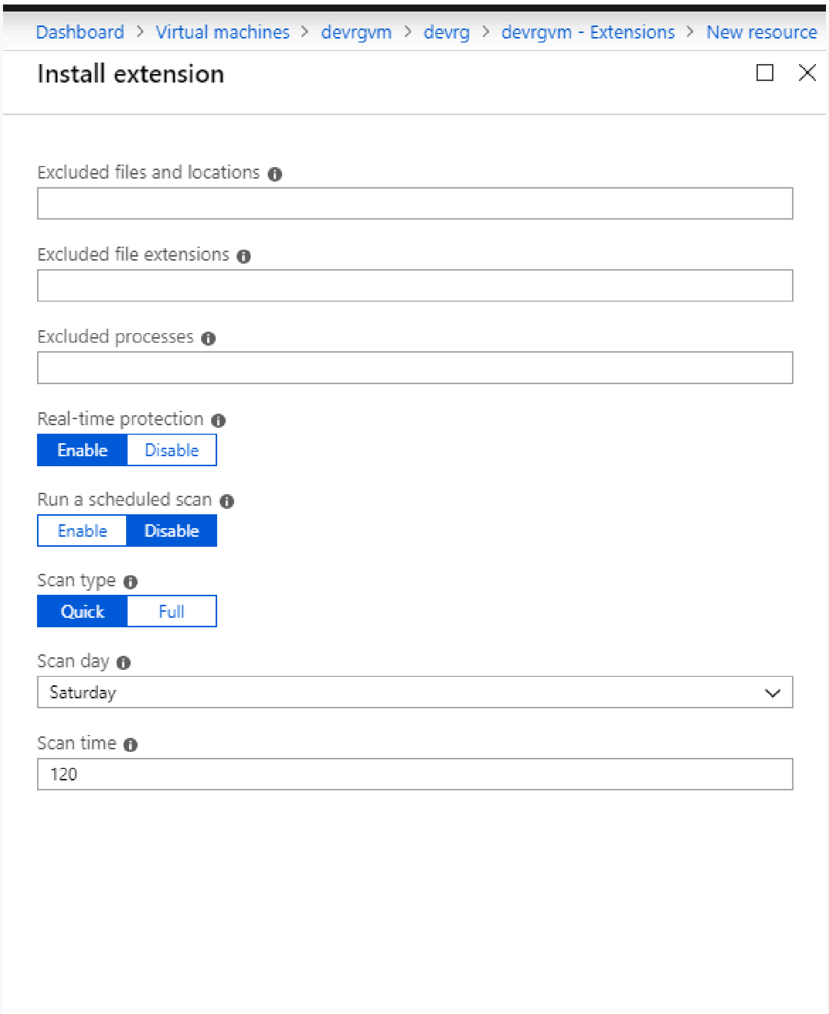
2. Select the Microsoft Antimalware extension and press Create.

3. Fill the ג€Install extensionג€ form as desired and press OK.

Scheduled: Enable -

Scan type: Full -

Scan day: Sunday -



Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions > New resource

Install extension

Excluded files and locations

Excluded file extensions

Excluded processes

Real-time protection: [✓ Enable] Disable

Run a scheduled scan: Enable [✓ Disable]

Scan type: [✓ Quick] Full

Scan day: Saturday

Scan time: 120

Reference:

https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/

⊟ **souvik123** Highly Voted 4 years, 2 months ago

Scan time of 2 AM is taken care with 120 in Scan Time field. The 60 means 1AM 120 means 2AM and each hour in 60 increment.

upvoted 23 times

⊟ **ChinkSantana** 4 years ago

Thanks for the explanation

upvoted 4 times

⊟ **kimalto452** 4 years ago

But why microsoft why ?????

upvoted 22 times

⊟ **awsc** Highly Voted 4 years, 1 month ago

"You need to perform a full malware scan every Sunday at 02:00"

Need to set Scan Type as Full

Also, Enable Schedule

upvoted 15 times

⊟ **ITFranz** Most Recent 10 months, 2 weeks ago

To provide a reference point.

https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/iaas-antimalware-windows

upvoted 1 times

⊟ **pentium75** 11 months ago

We want a full scan on Sunday, but the "correct answer" set it to NOT do a QUICK scan on SATURDAY ;)

upvoted 1 times

⊟ **pentium75** 11 months ago

"Microsoft Antimalware for Virtual Machines", from which century are these questions?

upvoted 1 times

⊟ **Feraso** 1 year, 8 months ago

When to perform the scheduled scan, measured in minutes from midnight (0-1440). For example: 0 = 12AM, 60 = 1AM, 120 = 2AM.

upvoted 1 times

⊟ **r_git** 2 years, 3 months ago

Simulations are back. Just had a friend that got them 03/21/2023.

upvoted 4 times

⊟ **rgbykkk** 2 years, 5 months ago

I think this is outdated now?

upvoted 1 times

⊟ **Ajdlfasudfo0** 2 years, 5 months ago

please use one second to google before writing nonsense

upvoted 1 times

⊟ **NinjaSchoolProfessor** 2 years, 11 months ago

Steps are correct, however to schedule a scan every Sunday, the image should not denote "Saturday" but instead should state "Sunday @ 120"

upvoted 2 times

⊟ **Startkabels** 4 years, 2 months ago

What about the time requirement?

upvoted 1 times

Question #6 *Topic 3*

SIMULATION -

You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1.

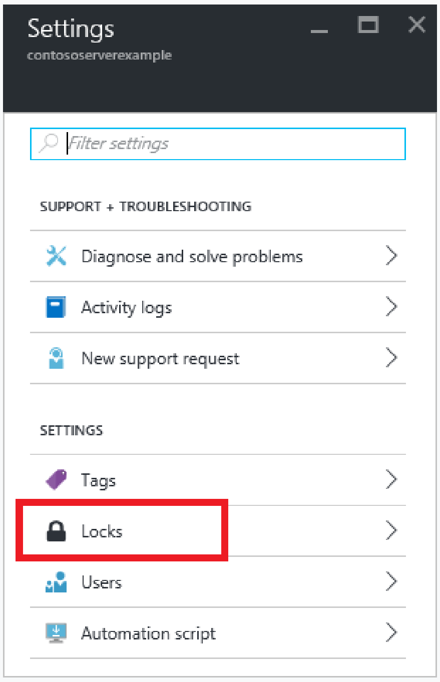
To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

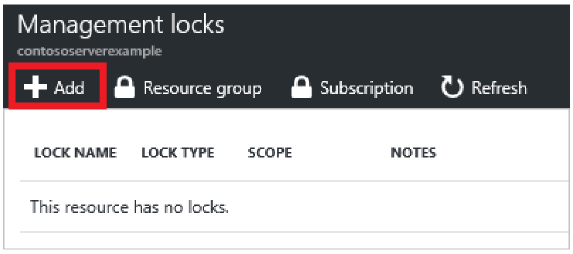
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

1. In the Settings blade for virtual network VNET, select Locks.



2. To add a lock, select Add.



LOCK NAME	LOCK TYPE	SCOPE	NOTES
This resource has no locks.			

3. For Lock type select Delete lock, and click OK

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

STomar Highly Voted 3 years, 11 months ago

Delete lock should be applied as the ask is - Admin user should not be able to delete the resource.

Delete lock = User can read or modify a resource, however cannot delete the same.

upvoted 10 times

pentium75 Most Recent 11 months ago

"Prevent from accidental deletion" is EXACTLY what delete lock is for.

upvoted 1 times

Bryan09 2 years, 1 month ago

it seems both actions might be a solution. Locks affect everyone including admins!

upvoted 1 times

Anarchira 2 years, 2 months ago

what about this?

Go to the Azure portal and open the VNET1 resource page.
Click on the "Access control (IAM)" tab on the left-hand menu.
Click on the "+ Add" button to add a new role assignment.
Select the "Virtual Network Contributor" role from the list of available roles.
In the "Select" field, enter the name of the administrative user or group that you want to add the role assignment to.
Click on the "Save" button to add the new role assignment.

By assigning the "Virtual Network Contributor" role to the administrative users, they will be able to modify the settings of the virtual network but will not be able to delete it. This helps prevent accidental deletions of the resource.
upvoted 3 times

⊟ **eroms** 4 years, 1 month ago
Correct.
Read-only option, as the name implies only allows for read only and not modify.
upvoted 2 times

Question #7 *Topic 3*

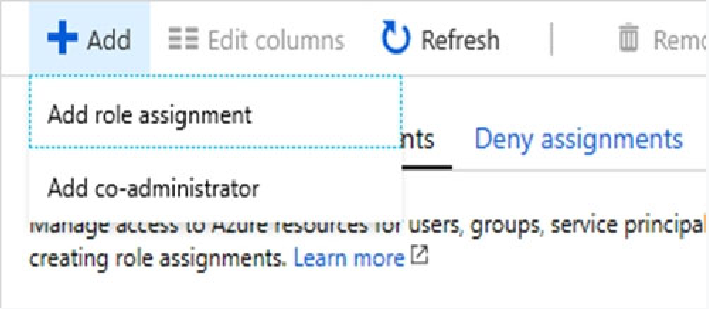
SIMULATION -

You need to grant the required permissions to a user named User2-1234578 to manage the virtual networks in the RG1lod1234578 resource group. The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

1. In Azure portal, locate and select the RG1lod1234578 resource group.
2. Click Access control (IAM).
3. Click the Role assignments tab to view all the role assignments at this scope.
4. Click Add > Add role assignment to open the Add role assignment pane.



Manage access to Azure resources for users, groups, service principal
creating role assignments. Learn more

5. In the Role drop-down list, select the role Virtual Machine Contributor.

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.

6. In the Select list, select user User2-1234578
7. Click Save to assign the role.

Reference:

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

⊟ **F117A_Stealth** Highly Voted 1 year, 7 months ago

Correct Answer:

1. In Azure portal, locate and select the RG1lod1234578 resource group.
2. Click Access control (IAM).
3. Click the Role assignments tab to view all the role assignments at this scope.
4. Click Add > Add role assignment to open the Add role assignment pane.

5. In the Role drop-down list, select the role Network Contributor.

Network Contributor Lets you manage networks, but not access to them.

6. In the Select list, select user User2-1234578
7. Click Save to assign the role.

upvoted 31 times

⊟ **upliftinghut** 1 year, 2 months ago

Should we choose the network instead of resource group in step 1?

upvoted 1 times

⊟ **heatfan900** 10 months ago

Correct. The question is requiring the management of virtual networks not VMs. The network contributor role is the right answer.

upvoted 6 times

⊟ **Kelly8023** Highly Voted 1 year, 8 months ago

Vote for network contributor

upvoted 7 times

⊟ **[Removed]** Most Recent 1 year, 3 months ago

In another question it was deemed that Network Contributor had too high access to be considered least-privileged. The choice is then a Custom role

upvoted 2 times

ltjones12 1 year, 6 months ago

Thank you for all the comments. This one confused me since it was asking to allow the management of Virtual Machines

upvoted 1 times

F117A_Stealth 1 year, 7 months ago

Answer isnt 100% correct. Steps are right, but the role required is Network Contributor: Network Contributor: Lets you manage networks, but not access to them.

upvoted 2 times

jore041 1 year, 7 months ago

network contributor is the correct role to be able to manage virtual network tho..

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles?toc=%2Fazure%2Fvirtual-network%2Ftoc.json#network-contributor

upvoted 2 times

OpsecDude 1 year, 9 months ago

Only network Contributor is needed to comply with least privilege.

Network Contributor: Lets you manage networks, but not access to them.

upvoted 4 times

ikidreamz 1 year, 9 months ago

Network contributor (to manage virtual network) , Virtual machine contributor "This role does not grant you management access to the virtual network or storage account" REF- https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

upvoted 2 times

JakeCallham 1 year, 9 months ago

Doesn't make sense to be bebothered with VM right, only network is needed

upvoted 2 times

Tash95 2 years, 2 months ago

Procedure is correct, but the role would be Virtual Machine Contributor: Lets you manage classic networks, but not access to them.

upvoted 1 times

> **Subbydavid** 2 years, 2 months ago
>
> Why not Network contributor? Question says manage vnet not manage vm
>
> upvoted 1 times
>
> **yooi** 2 years, 2 months ago
>
> I guess the role should be Network contributor: Lets you manage networks, but not access to them.
>
> upvoted 5 times

Question #8 *Topic 3*

SIMULATION -

You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod1234578 Azure Storage account.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

Step 1:

1. In Azure portal go to the storage account you want to secure. Here: rg1lod1234578
2. Click on the settings menu called Firewalls and virtual networks.
3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.
4. Click Save to apply your changes.

Step 2:

1. Go to the storage account you want to secure. Here: rg1lod1234578
2. Click on the settings menu called Firewalls and virtual networks.
3. Check that you've selected to allow access from Selected networks.
4. To grant access to a virtual network with a new network rule, under Virtual networks, click Add existing virtual network, select Virtual networks and Subnets options. Enter the 131.107.0.0/16 subnet and then click Add.

Note: When network rules are configured, only applications requesting data over the specified set of networks can access a storage account.

You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

⊟ **F117A_Stealth** Highly Voted 👍 2 years, 7 months ago

Go to the storage account

Under "Security + networking" SELECT "Networking"

Select "Firewalls and virtual networks" on the top (next to Custom domain)

Under Public network access, CHOOSE the "Enable from selected virtual network and IP addresses RADIO button

Under "Virtual networks" add existing virtual network

add the network with the CIDR.

upvoted 13 times

⊟ **JohnyDoo** Highly Voted 👍 3 years, 1 month ago

I dont think it is correct. It should be configured under Firewall section not Virtual Network section

upvoted 6 times

⊟ **Anil512** Most Recent 🕒 3 months, 3 weeks ago

RG >> Storage Account >> Security + Networking >> Networking >> Firewall and Virtual Networks >> Enable from selected virtual networks and IP addresses >> Address Range ... CIDR IP block ...

upvoted 1 times

⊟ **Viggy1212** 8 months, 3 weeks ago

131.107.0.0/16 is public address space and we are adding this under Vnet. Wondering how it is possible.

upvoted 1 times

⊟ **91743b3** 10 months, 3 weeks ago

On exam Aug 6 2024

upvoted 2 times

⊟ **rosef** 1 year, 7 months ago

Answer is not completely correct. Last step must be performed under Firewall section.

Go to the storage account

Under "Security + networking" SELECT "Networking"

Select "Firewalls and virtual networks" on the top (next to Custom domain)

Under Public network access, CHOOSE the "Enable from selected virtual network and IP addresses RADIO button

Under "Virtual networks" add existing virtual network

add the network with the CIDR.

upvoted 1 times

⊟ **gbx077** 2 years, 3 months ago

# Exam question March 24, 2023

upvoted 3 times

⊟ **Amit3** 2 years, 9 months ago

Firewall and Virtual Network section of Networking in Storage Account.

upvoted 4 times

⊟ **koreshio** 2 years, 8 months ago

yup, this is correct.

upvoted 2 times

Question #9 *Topic 3*

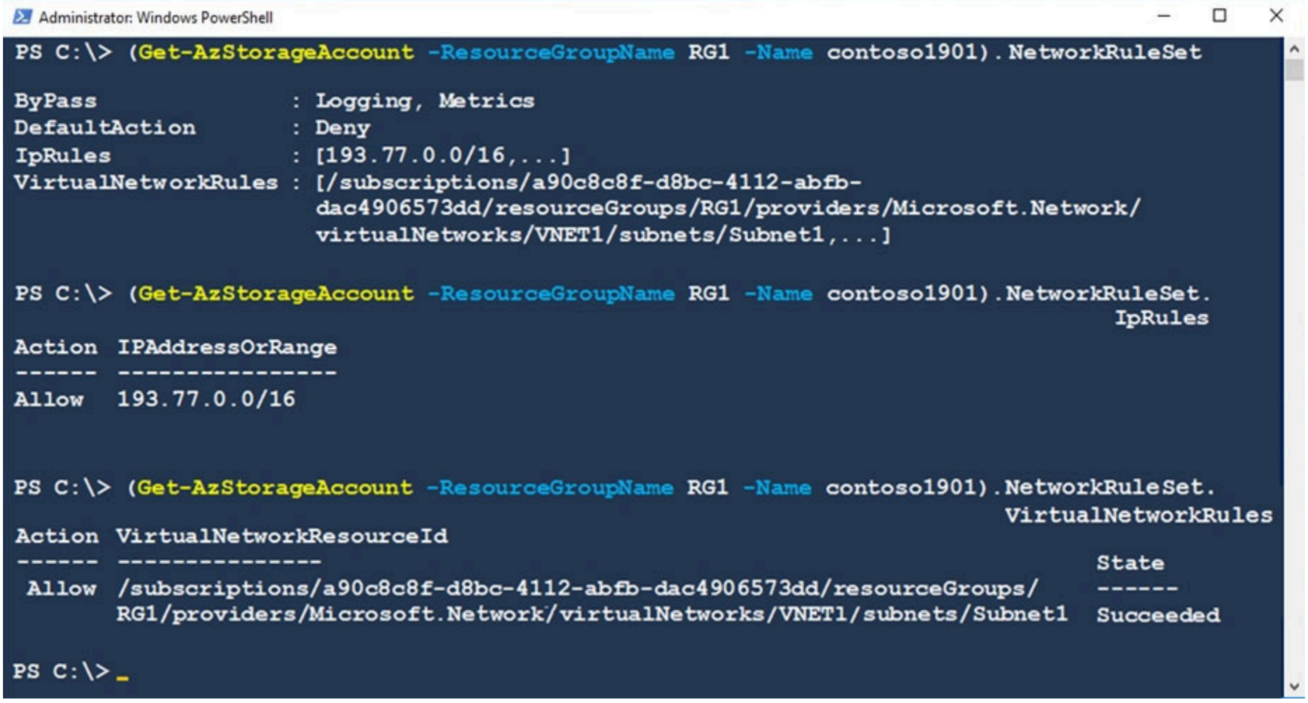
HOTSPOT -

You create resources in an Azure subscription as shown in the following table.

Name	Type	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
Contoso1901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.

Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

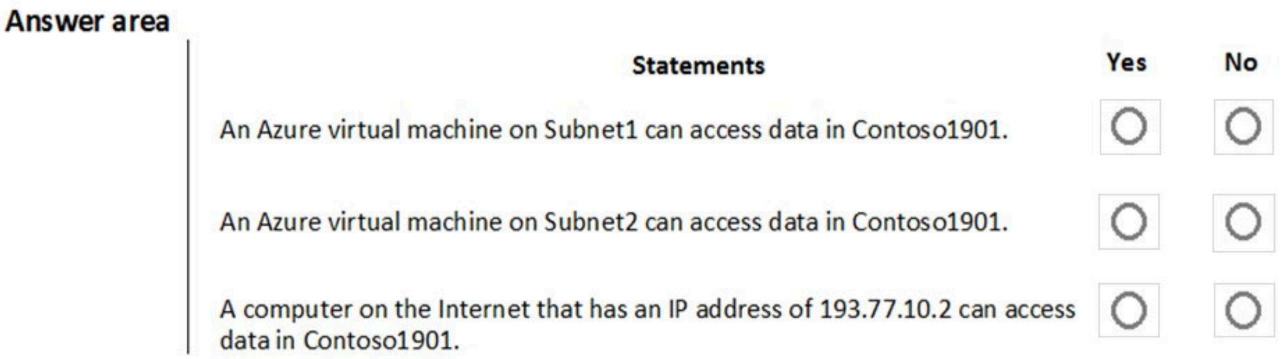


```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass              : Logging, Metrics
DefaultAction       : Deny
IpRules             : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                      dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                      virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                                             IpRules

Action  IPAddressOrRange
------  ----------------
Allow   193.77.0.0/16


PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                                     VirtualNetworkRules
Action  VirtualNetworkResourceId
------  ---------------                                                    State
 Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/  ------
        RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1  Succeeded

PS C:\> _
```

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

NOTE: Each correct selection is worth one point.

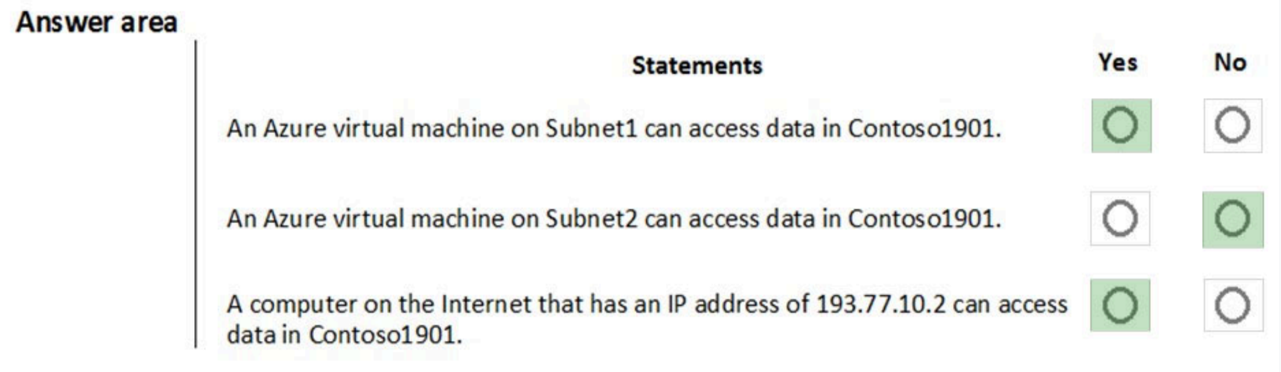
Hot Area:



Answer area

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	○	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	○
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	○	○

Suggested Answer:



Answer area

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	[✓ ○]	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	[✓ ○]
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	[✓ ○]	○

Box 1: Yes -
Access from Subnet1 is allowed.

Box 2: No -
No access from Subnet2 is allowed.

Box 3: Yes -
Access from IP address 193.77.10.2 is allowed.

JohnYinToronto Highly Voted 4 years, 3 months ago

answers correct

upvoted 39 times

poplovic Highly Voted 3 years, 9 months ago

VirtualNetRule allows subnet1. IpRules allow 193.77.0.0/16. default action is deny.
Therefore, Subnet1 yes, Subnet2 no, 193.77.0.2 yes (in the 193.77.0.0./16) range,
details in http://networkcalculator.ca/cidr-calculator.php
Network = 193.77.0.0
Usable IPs = 193.77.0.1
to 193.77.255.254 for 65534
Broadcast = 193.77.255.255
Netmask = 255.255.0.0
Wildcard Mask = 0.0.255.255

upvoted 17 times

hogehogehoge Most Recent 1 year, 9 months ago

I think Box3 is No. Because Default action is Deny.

upvoted 1 times

pentium75 11 months ago

But "default action" is applied only when no rule is matched. Here the client's IP does match the "allowed networks" rule.

upvoted 1 times

heatfan900 1 year, 10 months ago

Y, N, Y
Subnet1 is allowed to access the SA internally.
Subnet2 is NOT allowed to access the SA internally.
Connecting from THE 193.77/16 public network allows access to the SA.

upvoted 2 times

Self_Study 1 year, 10 months ago

On exam 7/8/23. Answers are correct.

upvoted 4 times

majstor86 2 years, 3 months ago

YES
NO
YES

upvoted 4 times

ligu 2 years, 4 months ago

Answers are correct

upvoted 1 times

Sweet_co 2 years, 11 months ago

In exam: 20-7-2022

upvoted 8 times

NinjaSchoolProfessor 2 years, 11 months ago

In exam 15-July-2022

upvoted 6 times

acexyz 2 years, 12 months ago

# IN EXAM - 30/6/2022

upvoted 4 times

alou333 3 years ago

# IN EXAM - 3rd june 2022 (online).

Lot of new questions. Good luck !

upvoted 4 times

bbcc 3 years ago

@alou333 Is there simulations in the online exam?

upvoted 1 times

adamsca 3 years, 6 months ago

# Exam Question 12/10/2021

upvoted 5 times

Jco 3 years, 9 months ago

#exam question # 29 Sep

upvoted 3 times

francis6170 3 years, 9 months ago

Got this in the AZ-500 exam (Sept 2021)! A: Y,N,Y

upvoted 4 times

JChris 3 years, 9 months ago

Hello francis, was there any simulation question? Thanks in advance for your response.

upvoted 1 times

draddo9 3 years, 9 months ago

Hi JChris! I will answer coz I had exam 3 days ago also. There were not any simulation questions. First 3-5 question were the case question (big amount of text, describing company, resources in Azure and ideas and things to create in future by company). I hope it helps :)

upvoted 8 times

Triones 3 years, 11 months ago

can someone explain why the first rule deny didn't take effect? is it overwrite?

upvoted 2 times

Jacquesvz 3 years, 11 months ago

the "first rule" you are referring to means what is the default action to allow access. It's set to deny, which is correct, as you would explicitly deny access and then either grant access to a vnet or ip address, like the example shows. The given answers are correct.

upvoted 7 times

LeeMyungjin 2 years, 2 months ago

"By default, storage accounts accept connections from clients on any network. You can limit access to selected networks or prevent traffic from all networks and permit access only through a private endpoint.

You must set the default rule to deny, or network rules have no effect. However, changing this setting can affect your application's ability to connect to Azure Storage. Be sure to grant access to any allowed networks or set up access through a private endpoint before you change this setting."

Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

upvoted 1 times

kubikula 4 years, 1 month ago

Would be someone so kind to justify with the ip subnet calculation to justify how 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24 are allowed into that range? Thanks in advance. Jacobo

upvoted 2 times

DCarma 4 years ago

Not sure what you mean... the 3rd command shows that Subnet1 is allowed. The range of Subnet1 is 10.0.0.0/24 (10.0.0.0 - 10.0.0.255). Subnet2 10.1.1.0/24 (10.1.1.0 - 10.1.1.255) is not allowed anywhere so the answer is no. Finally, range 193.77.0.0/16 (193.77.0.0 - 193.77.255.255) is allowed, so 193.77.10.2 would be allowed as it is within this range. Hope that helps?

upvoted 8 times

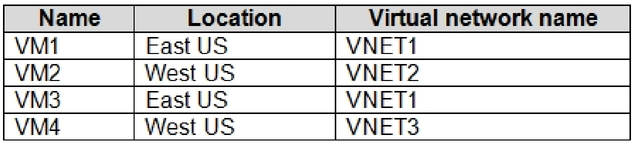
Cyberbug2021 4 years, 2 months ago

YES - NO - YES

upvoted 3 times

Question #10 Topic 3

You have an Azure subscription that contains the virtual machines shown in the following table.



Name	Location	Virtual network name
VM1	East US	VNET1
VM2	West US	VNET2
VM3	East US	VNET1
VM4	West US	VNET3

All the virtual networks are peered.

You deploy Azure Bastion to VNET2.

Which virtual machines can be protected by the bastion host?

A. VM1, VM2, VM3, and VM4

B. VM1, VM2, and VM3 only

C. VM2 and VM4 only

D. VM2 only

Suggested Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

Community vote distribution

A (100%)

gabrialtonka Highly Voted 2 years, 4 months ago

Selected Answer: A

Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peered VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host.

upvoted 37 times

bmanu Highly Voted 3 years, 1 month ago

Great read https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

upvoted 17 times

KikoTeijeiro Most Recent 8 months, 2 weeks ago

Az-500 today on exam. Passed 826/1000. No labs on the online exam. One Case Study with 5 questions.

upvoted 12 times

ESAJRR 9 months ago

Selected Answer: A

A. VM1, VM2, VM3, and VM4

upvoted 2 times

fireb 9 months, 2 weeks ago

Selected Answer: A

Option A is the correct answer.

upvoted 1 times

majstor86 1 year, 3 months ago

Selected Answer: A

A. VM1, VM2, VM3, and VM4

upvoted 2 times

ligu 1 year, 4 months ago

Answer is correct

upvoted 1 times

Matzegnan 1 year, 9 months ago

Selected Answer: A

A is correct as there is peering.

upvoted 1 times

Amit3 1 year, 11 months ago

A is correct given VNet Peering.

upvoted 1 times

Alessandro365 2 years ago

Selected Answer: A

A is correct answer.

upvoted 1 times

salmantarik 2 years ago

Correct answer. Once you peer VNETs, Azure BH can be leveraged with all VNETs.

upvoted 3 times

Adrador 2 years, 3 months ago

The answer is A because they are buddies :)

upvoted 6 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 2 times

amitksinha 2 years, 5 months ago

Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peered VNet

upvoted 1 times

cfsxtuv33 2 years, 5 months ago

Selected Answer: A

Correct answer is........"A"

upvoted 4 times

mhzayt 2 years, 7 months ago

Selected Answer: A

The answer is correct : A

upvoted 3 times

ywlem 2 years, 9 months ago

The answer is correct. However, do note that the Azure Bastion with VNet peering is limited to 500 VNets and the cost is charged on ingress/egress.

upvoted 5 times

Question #11 *Topic 3*

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. device configuration policies in Microsoft Intune

B. Azure Automation State Configuration

C. security policies in Azure Security Center

D. device compliance policies in Microsoft Intune

Suggested Answer: *B*
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.
Reference:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

Community vote distribution

B (100%)

⊟ **Thanveer** Highly Voted 3 years, 3 months ago
Given Answer is correct
upvoted 27 times

⊟ **rgullini** 3 years, 2 months ago
Agreed.
upvoted 3 times

⊟ **ESAJRR** Most Recent 10 months, 3 weeks ago
Selected Answer: B
B. Azure Automation State Configuration
upvoted 2 times

⊟ **majstor86** 1 year, 3 months ago
Selected Answer: B
B. Azure Automation State Configuration
upvoted 2 times

⊟ **ligu** 1 year, 4 months ago
Answer is correct
upvoted 1 times

⊟ **F117A_Stealth** 1 year, 7 months ago
Selected Answer: B
B. Azure Automation State Configuration
upvoted 1 times

⊟ **NinjaSchoolProfessor** 1 year, 11 months ago
B: Azure Automation State Configuration
https://docs.microsoft.com/en-us/azure/automation/overview#azure-automation-state-configuration
upvoted 2 times

⊟ **Eltooth** 2 years, 3 months ago
Selected Answer: B
B is correct answer.
upvoted 3 times

⊟ **Bikey** 2 years, 4 months ago

B. Azure Automation State Configuration

is correct answer.

upvoted 2 times

⊟ **poplovic** 2 years, 9 months ago

Automation is the only way (B) is correct

upvoted 1 times

⊟ **teehex** 3 years, 1 month ago

B - Azure Automation State Configuration is the only supported way in Azure to meet this requiement.

upvoted 1 times

> ⊟ **teehex** 3 years, 1 month ago
>
> Sample well architected framework with state configuration for testing purpose https://docs.microsoft.com/en-us/samples/mspnp/samples/azure-well-architected-framework-sample-state-configuration/
>
> upvoted 2 times

Question #12 *Topic 3*

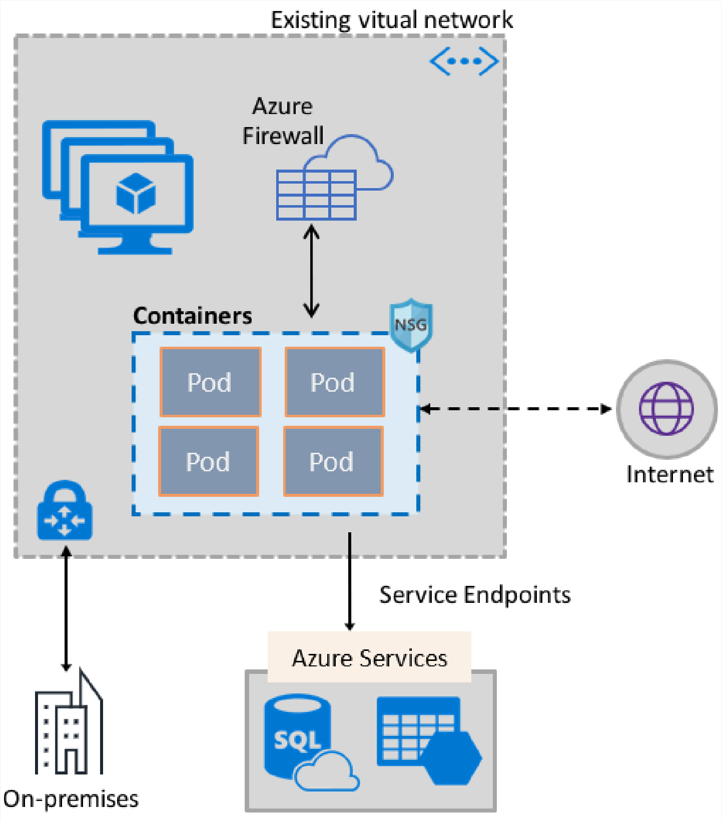
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You create a service endpoint for Microsoft.Storage in Subnet1.
You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.
What should you do on VM1 before you deploy the container?

A. Create an application security group and a network security group (NSG).

B. Edit the docker-compose.yml file.

C. Install the container network interface (CNI) plug-in.

Suggested Answer: *C*
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform.
The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

Community vote distribution
C (100%)

⊟ **Rave763** Highly Voted 4 years, 2 months ago
C is correct
upvoted 23 times

⊟ **gfhbox0083** Highly Voted 3 years, 12 months ago
C, for sure.
Install the container network interface (CNI) plug-in.
upvoted 12 times

zied01 Most Recent 7 months ago

Is that the objective of the cni ????? Because the cni is just to distribute ip adress

So the purpose of the question is the service endpoint that we can enable it only with the activation of the service endpoint in the subnet

upvoted 1 times

JunetGoyal 8 months, 1 week ago

nstall the container network interface (CNI) plug-in, this will give ip to containers from vnet

upvoted 1 times

ESAJRR 10 months, 3 weeks ago

Selected Answer: C

C. Install the container network interface (CNI) plug-in.

upvoted 1 times

Johnvic 1 year, 2 months ago

Exam.6 case studies. 3 true/false questions. 47 multiple questions and no simulations. Alot of new questions thats not up here.

upvoted 4 times

majstor86 1 year, 3 months ago

Selected Answer: C

C. Install the container network interface (CNI) plug-in.

upvoted 2 times

chijokz 1 year, 7 months ago

C is the correct answer.

upvoted 1 times

NinjaSchoolProfessor 1 year, 11 months ago

Selected Answer: C

In exam 15-July-2022

upvoted 2 times

acexyz 1 year, 12 months ago

# IN EXAM - 30/6/2022

upvoted 2 times

MofD 2 years ago

True Story

upvoted 1 times

HazemSbaih 2 years ago

Selected Answer: C

YES is correct

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 1 times

poplovic 2 years, 9 months ago

CNI allows each Pod in the container to have its own private IP and thus seamlessly integrated in the VNET (service endpoint etc)

upvoted 2 times

Vegazbabz 3 years, 4 months ago

Had it in an exam this week

upvoted 9 times

kdkdk 3 years, 6 months ago

in the exams

upvoted 3 times

jbuenoo 3 years, 9 months ago

reference: https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

upvoted 4 times

DA0410 3 years, 7 months ago

Correct. When a Pod comes up in the virtual machine, Azure CNI assigns an available IP address from the pool and connects the Pod to a software bridge in the virtual machine. When the Pod terminates, the IP address is added back to the pool.

upvoted 7 times

Question #13 *Topic 3*

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. device configuration policies in Microsoft Intune

B. an Azure Desired State Configuration (DSC) virtual machine extension

C. application security groups

D. device compliance policies in Microsoft Intune

Suggested Answer: *B*
The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service.
The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring.
Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

Community vote distribution

B (91%) 9%

Ed2learn Highly Voted 4 years, 1 month ago

This is same question as above. The given answer is correct.

upvoted 12 times

pentium75 Most Recent 11 months ago

Selected Answer: B

Exactly for that purpose. Intune would apply only much later, and no one knows if these machines will be enrolled to Intune at all.

upvoted 1 times

ESAJRR 1 year, 10 months ago

Selected Answer: B

B. an Azure Desired State Configuration (DSC) virtual machine extension

upvoted 3 times

kuskumar 2 years ago

Selected Answer: A

Answer is A. Windows features can only be disabled via Intune. https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10

upvoted 1 times

> **pentium75** 11 months ago
>
> It must be done "as instances of the virtual machines are provisioned", not later when they have probably been enrolled to Intune.
>
> upvoted 1 times
>
> **epomatti** 1 year, 6 months ago
>
> The question states Azure Virtual Machine resource. B is more likely to be the correct answer.
>
> upvoted 1 times

majstor86 2 years, 3 months ago

Selected Answer: B

B. an Azure Desired State Configuration (DSC) virtual machine extension

upvoted 1 times

ligu 2 years, 4 months ago

Answer is correct

upvoted 1 times

F117A_Stealth 2 years, 7 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 4 times

⊟ **adamsca** 3 years, 6 months ago

Correct. This is also a duplicate of Q27 Topic3

upvoted 4 times

⊟ **poplovic** 3 years, 9 months ago

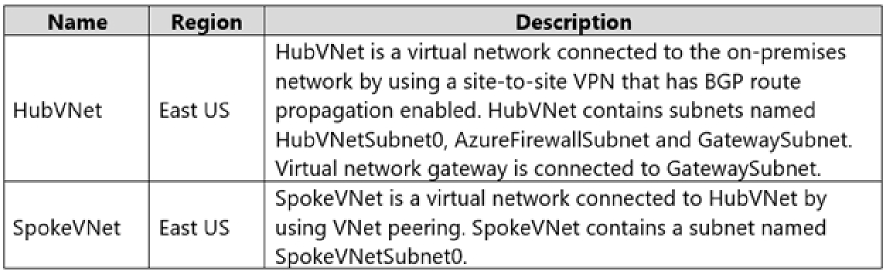
verified in az104. DSC is correct

upvoted 2 times

Question #14 *Topic 3*

DRAG DROP -

You have an Azure subscription that contains the virtual networks shown in the following table.



Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains subnets named HubVNetSubnet0, AzureFirewallSubnet and GatewaySubnet. Virtual network gateway is connected to GatewaySubnet.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

✑ RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address

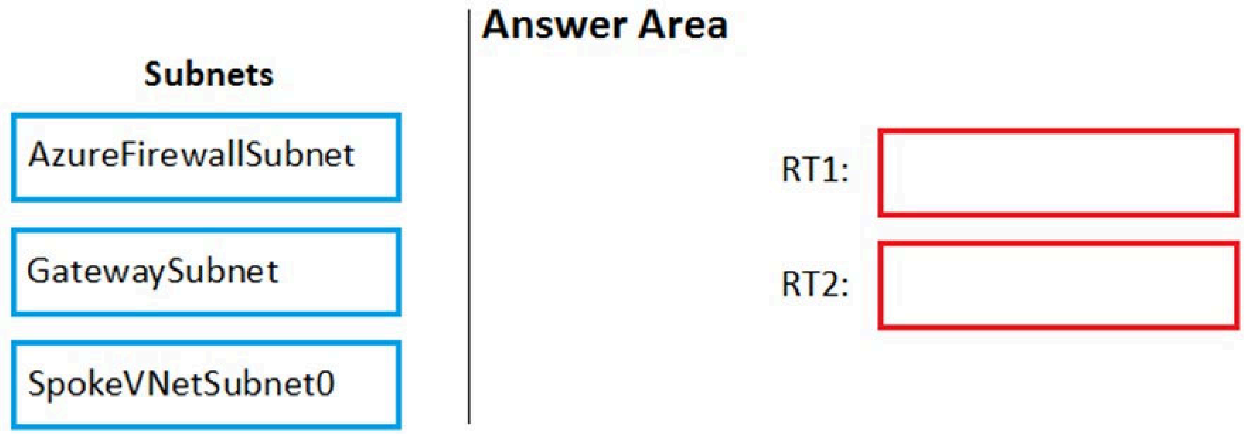
✑ RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Answer Area

Subnets

AzureFirewallSubnet

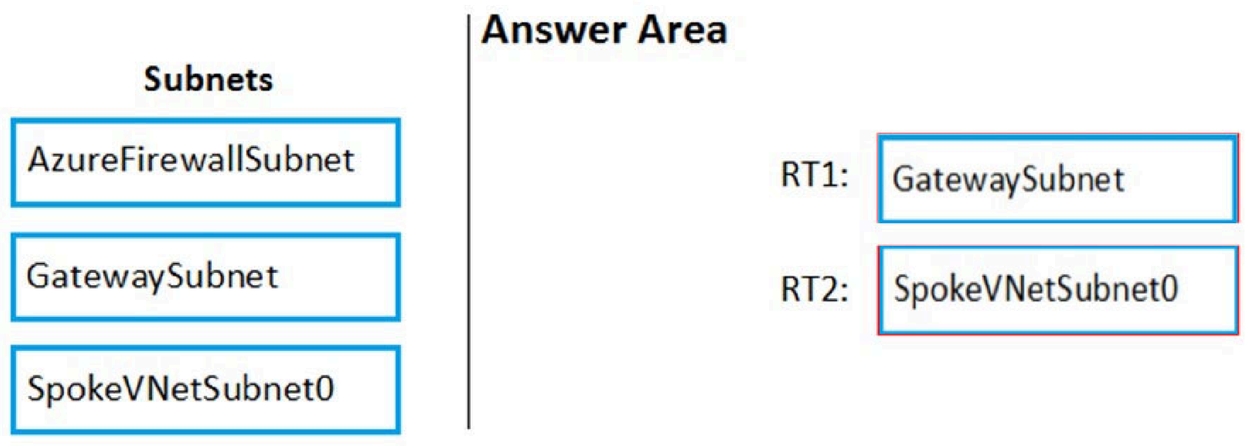
GatewaySubnet

SpokeVNetSubnet0

RT1:

RT2:

Suggested Answer:



Answer Area

Subnets

AzureFirewallSubnet

GatewaySubnet

SpokeVNetSubnet0

RT1: GatewaySubnet

RT2: SpokeVNetSubnet0

Reference:

https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#create-the-routes

⊟ **rsharma007** Highly Voted 3 years, 10 months ago

VNET peering is enabled on Spoke VNET and BGP route propagation is enabled on gateway subnet. So Spoke VNET will use the VPN gateway for BGP routes by default. To prevent this and use Azure FW , we need to disable BGP route propagation for Spoke VNET's Routing table and use Azure FW as the default GW(0.0.0.0/0). To provide bidirectional routing, Gateway subnet will need to use Azure FW for SpokeVNET subnets. In addition Azure FW subnet should have routes for spokeVNET and gateway subnet.

upvoted 34 times

7cc5495 9 months, 2 weeks ago

y cual seria la respuesta entonces

upvoted 1 times

chikorita 2 years, 4 months ago

did not fully understand but atleast made me somewhat confident with your answer

upvoted 5 times

JohnBentass 2 years, 6 months ago

Good explanation

upvoted 1 times

ARDNK 3 years, 4 months ago

when I read this, my head is spinning . (just for laugh)

upvoted 23 times

Hillary_Innocent 2 years, 8 months ago

same here i am not even getting the context of it, every statement is confusing and cant relate to the previous statement lol

upvoted 7 times

gcpbrig01 Highly Voted 4 years, 3 months ago

suggested answer is correct.

RT2 - To route the spoke subnet traffic through the hub firewall, you can use a User Defined route (UDR) that points to the firewall with the Virtual network gateway route propagation option disabled.

RT1 - Configure a UDR on the hub gateway subnet that points to the firewall IP address as the next hop to the spoke networks.

https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#prerequisites

upvoted 21 times

mung 2 years, 7 months ago

Agree with the answer but if route propagation options is disabled on the GatewaySubnet it won't work.

upvoted 1 times

mmmyo Most Recent 1 month, 3 weeks ago

✅ RT1 → SpokeVNetSubnet0

Reason: Traffic originating from SpokeVNetSubnet0 should be directed to the Azure Firewall first before reaching the on-premises network.

By pointing the next hop to the firewall's private IP, outbound traffic will pass through the firewall for inspection.

✅ RT2 → GatewaySubnet

Reason: GatewaySubnet connects to the on-premises network via site-to-site VPN.

Disabling BGP propagation ensures that routes from on-prem do not override firewall rules.

Setting the firewall as the default gateway forces traffic from the on-premises network to pass through the firewall.

upvoted 1 times

Nhadipour 4 months, 3 weeks ago

RT1 → SpokeVNetSubnet0

RT2 → GatewaySubnet

upvoted 1 times

faisal12 1 year, 6 months ago

Traffic flow for RT2 will initiate from SPOKEVNET and will shaped as:

On-Cloud Azure Environment = SPOKEVNET > Azure FW (Default GW) > HUBVNET > site-2-site vpn > On-premise

upvoted 1 times

epomatti 1 year, 6 months ago

This question should not be part of AZ-500...

upvoted 2 times

pentium75 11 months ago

Yeah, it's more networking than security.

upvoted 1 times

⊟ **wardy1983** 1 year, 8 months ago

RT1 - Configure a UDR on the hub gateway subnet that points to the firewall IP address as the next hop to the spoke networks.

RT2 - To route the spoke subnet traffic through the hub firewall, you can use a User Defined route (UDR) that points to the firewall with the Virtual network gateway route propagation option disabled

upvoted 1 times

⊟ **tweleve** 1 year, 8 months ago

in exam 13 Oct

upvoted 5 times

⊟ **Paul_white** 2 years, 2 months ago

i WAS JUST READING THE QUESTION AND IT WAS LIKE I WAS READING A DIFFERENT LANGUAGE :(

upvoted 8 times

⊟ **majstor86** 2 years, 3 months ago

RT1: Gateway subnet

RT2: SpokeVNetSubnet0

upvoted 7 times

⊟ **ligu** 2 years, 4 months ago

Answers are correct

upvoted 1 times

⊟ **arseyam** 2 years, 8 months ago

Route propagation shouldn't be disabled on the GatewaySubnet. The gateway will not function with this setting disabled.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#custom-routes

upvoted 2 times

⊟ **TonytheTiger** 3 years, 9 months ago

## Exam Question - 17 Sept 2021 ##

upvoted 3 times

⊟ **francis6170** 3 years, 9 months ago

Got this in the AZ-500 exam (Sept 2021)! A: GatewaySubnet, SpokeSubnet

upvoted 1 times

⊟ **SecurityAnalyst** 3 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 2 times

⊟ **Socgen1** 3 years, 10 months ago

In exam on 31/08/2021 - given answer are correct

upvoted 3 times

⊟ **kumax** 4 years ago

On exam, May 2021.

upvoted 4 times

Question #15 Topic 3

HOTSPOT -

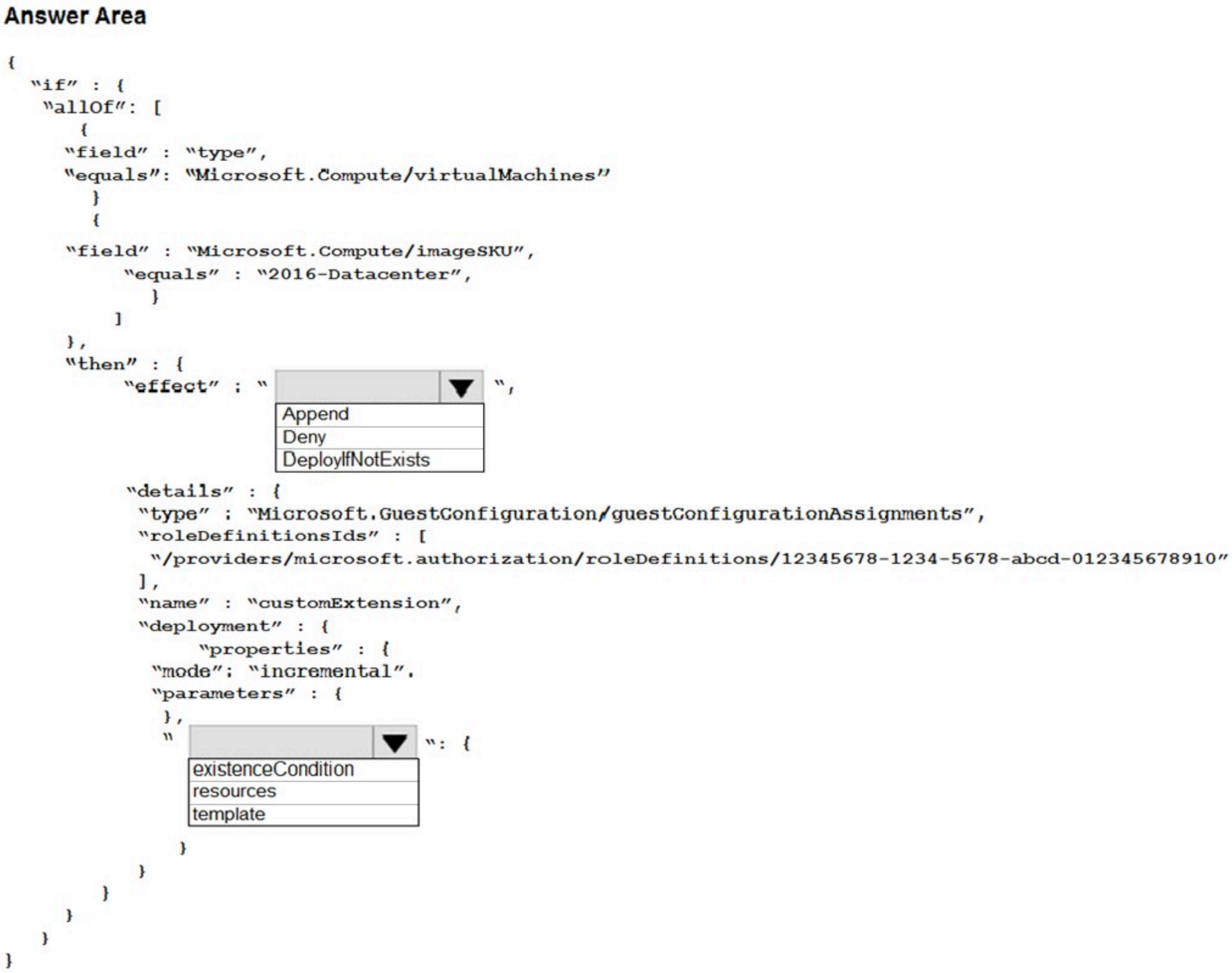
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

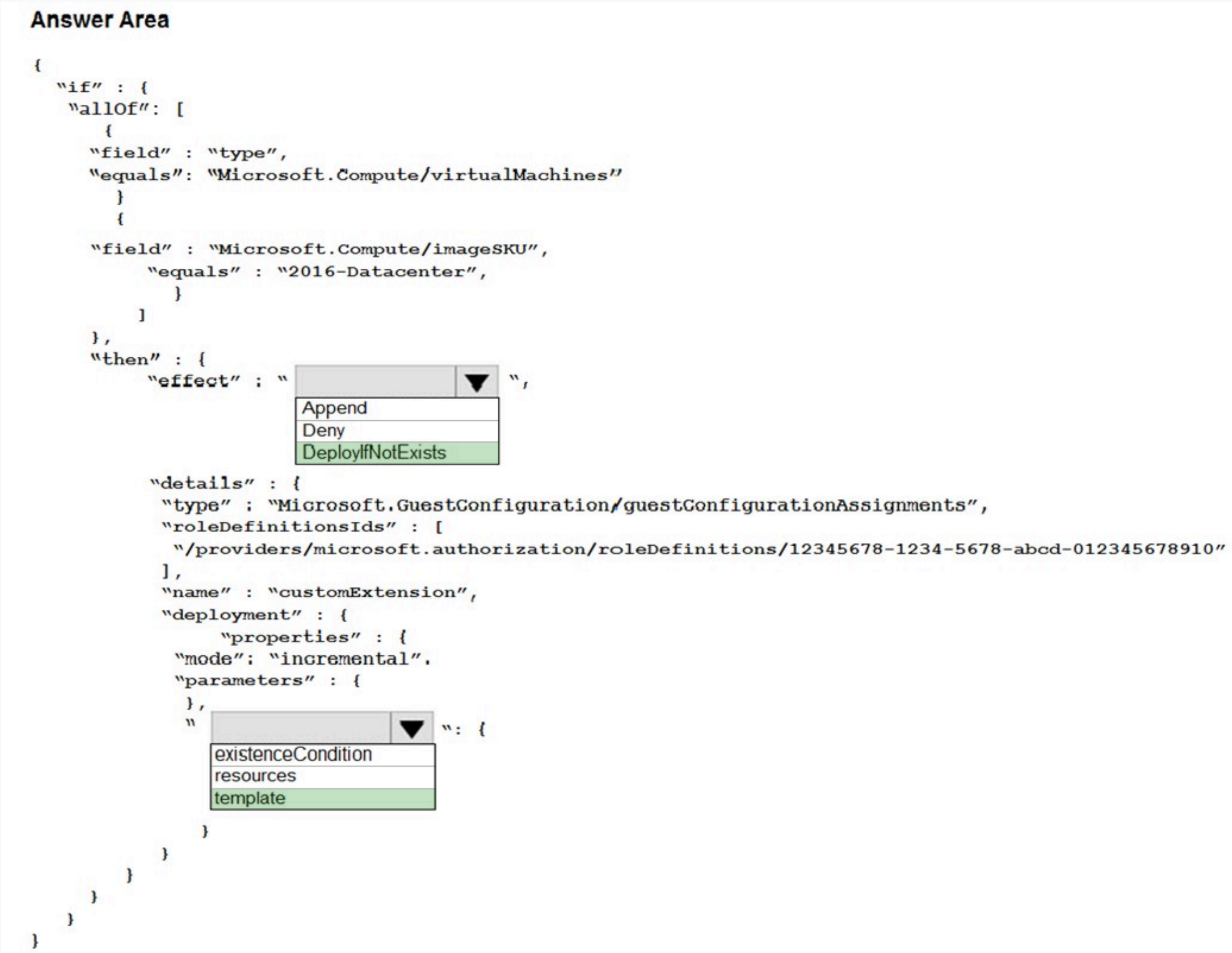
Hot Area:



Answer Area

```
{
  "if" : {
   "allOf": [
      {
    "field" : "type",
    "equals": "Microsoft.Compute/virtualMachines"
       }
       {
    "field" : "Microsoft.Compute/imageSKU",
         "equals" : "2016-Datacenter",
            }
         ]
    },
    "then" : {
         "effect" : "          ▼ ",
                    Append
                    Deny
                    DeployIfNotExists
         "details" : {
          "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
          "roleDefinitionsIds" : [
           "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
          ],
          "name" : "customExtension",
          "deployment" : {
                "properties" : {
           "mode": "incremental",
           "parameters" : {
            },
            "          ▼ ": {
             existenceCondition
             resources
             template
              }
          }
        }
     }
   }
}
```

Suggested Answer:



Answer Area

```
{
  “if” : {
   “allOf”: [
      {
     “field” : “type”,
     “equals”: “Microsoft.Compute/virtualMachines”
       }
       {
     “field” : “Microsoft.Compute/imageSKU”,
          “equals” : “2016-Datacenter”,
            }
          ]
     },
     “then” : {
          “effect” : “                    ”,
          “details” : {
           “type” ; “Microsoft.GuestConfiguration/guestConfigurationAssignments”,
           “roleDefinitionsIds” : [
            “/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910”
           ],
           “name” : “customExtension”,
           “deployment” : {
                “properties” : {
            “mode”: “incremental”.
            “parameters” : {
             },
             “                    ”: {
              }
           }
        }
     }
   }
}
```

Box 1: DeployIfNotExists -

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template -

The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.

Deployment [required]

This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment

References:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

⊟ **gfhbox0083** Highly Voted 3 years, 12 months ago

Answers are correct.

DeployIfNotExist / Template

upvoted 52 times

⊟ **lnn_az** Highly Voted 4 years ago

Correct Answer. Refer https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists-example

upvoted 14 times

⊟ **wardy1983** Most Recent 7 months, 2 weeks ago

Explanation:

Box 1: DeployIfNotExists -

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template -

The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.

Deployment [required]

This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment

Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

upvoted 5 times

majstor86 1 year, 3 months ago

DeployIfNotExist
Template

upvoted 1 times

ligu 1 year, 4 months ago

Answers are correct

upvoted 1 times

Siblark 1 year, 8 months ago

In Exam Oct 05, 2022. Passed

upvoted 3 times

Amit3 1 year, 9 months ago

# In EXAM - 01-Oct-2022

upvoted 3 times

MoFami 1 year, 12 months ago

In Exam 01/07/2022

upvoted 3 times

WhalerTom 2 years, 6 months ago

In exam Dec 21. 40 questions, 1 case study, no labs.

upvoted 6 times

Jco 2 years, 9 months ago

#exam ques # 29 Sep

upvoted 3 times

orallony 2 years, 9 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 5 times

Garry69 2 years, 9 months ago

DeployIfNotExists: deploys a related resource if it doesn't already exist

upvoted 2 times

Sandomj55 2 years, 10 months ago

In Exam 8/4/2021

upvoted 4 times

> **shanti0091** 2 years, 10 months ago
>
> Hi @Sandomj55, how was the exam, seems you wrote this recently. Any sim questions?
>
> upvoted 1 times

johnsm 3 years ago

DeployIfNotExist / Template. Have a look at the built in policy created by microsoft: https://github.com/Azure/azure-policy/blob/master/samples/built-in-policy/deploy-default-antimalware-extension-for-windows-server/azurepolicy.json

upvoted 3 times

teehex 3 years, 1 month ago

Lol no need to argue about template or resource. This is the policy you need https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Compute/VMAntimalwareExtension_Deploy.json#L76

upvoted 3 times

macco455 3 years, 3 months ago

Answer is correct. In looking at https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists-example, I am only seeing mode in reference to template and not resources. This is not the technical answer but just basic reasoning on the wording each command uses. Just my $.02

upvoted 2 times

JohnYinToronto 3 years, 3 months ago

answers correct

upvoted 2 times

Question #16 *Topic 3*

You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use the auto-generated service principal to authenticate to the Azure Container Registry.
What should you create?

A. an Azure Active Directory (Azure AD) group

B. an Azure Active Directory (Azure AD) role assignment

C. an Azure Active Directory (Azure AD) user

D. a secret in Azure Key Vault

Suggested Answer: *B*
When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.
References:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

Community vote distribution
B (100%)

DeepMoon Highly Voted 👍 4 years, 8 months ago
1. When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources.
2. This service principal can already authenticate to AAD (since it was created in AAD).
3. But it needs to be RBAC permissions on the ACR Registry to pull images.
To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.
upvoted 105 times

kiketxu 4 years, 7 months ago
Perfectly explained. Thanks!
upvoted 9 times

gfhbox0083 Highly Voted 👍 4 years, 12 months ago
B for sure.
(Azure AD) role assignment
upvoted 28 times

Jimmy500 Most Recent 🕒 11 months, 3 weeks ago
There is one more question in the bank in topic1 qustion 20 I think here we need to assign RBAC not Azure AD ROLE
upvoted 1 times

ESAJRR 1 year, 9 months ago
Selected Answer: B
B. an Azure Active Directory (Azure AD) role assignment
upvoted 1 times

ITFranz 1 year, 9 months ago
Thank you for the explanation DeepMoon.
The answer is: Azure AD role assignment
upvoted 1 times

majstor86 2 years, 3 months ago
Selected Answer: B
B. an Azure Active Directory (Azure AD) role assignment
upvoted 1 times

ligu 2 years, 4 months ago
You need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry- Answer is correct
upvoted 1 times

Eltooth 3 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

cfsxtuv33 3 years, 4 months ago

Repeat question I believe, I wish I remembered the other question. I think it was the same "role assignment" answer though.

upvoted 1 times

Joshing 3 years, 4 months ago

Selected Answer: B

Azure AD role assignment is the closest answer but is wrong. It would be an Azure role. Not Azure AD role.

upvoted 12 times

Tombarc 3 years, 5 months ago

Well, what makes me confused is the word used in this question. Azure role assignment is different from Azure AD role assignment. Why does the service principal need an Azure AD role assignment?

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-authentication?tabs=azure-cli#service-principal

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-authentication?tabs=azure-cli#authentication-options

https://docs.microsoft.com/en-us/azure/container-registry/authenticate-kubernetes-options

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

upvoted 2 times

adamsca 3 years, 6 months ago

Correct

This is a duplicate Question of Q1 topic3. Slightly different wording but same.

upvoted 2 times

poplovic 3 years, 9 months ago

b is correct

upvoted 1 times

SecurityAnalyst 3 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 4 times

amanp 4 years, 5 months ago

Given Answer is correct.

Service principal must be assigned atleast Reader role to the ACR for deploying to ACI or AKS

upvoted 2 times

DeepMoon 4 years, 8 months ago

1. When you create an AKS cluster, Azure also creates a service principal to support cluster operations with other Azure resources.

2. This service principal can already authenticate to AAD (since it was created in AAD by Azure).
3. But it needs to be RBAC permissions on the ACR Registry to pull images.

4. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.

upvoted 10 times

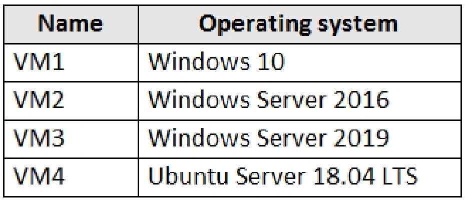
shaheer1991 5 years, 1 month ago

the given answer is the most reasonable between the choices.

upvoted 3 times

Question #17 *Topic 3*

You have an Azure subscription that contains the Azure virtual machines shown in the following table.



Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

You create an MDM Security Baseline profile named Profile1.

You need to identify to which virtual machines Profile1 can be applied.

Which virtual machines should you identify?

A. VM1 only

B. VM1, VM2, and VM3 only

C. VM1 and VM3 only

D. VM1, VM2, VM3, and VM4

Suggested Answer: *A*

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

Community vote distribution

A (80%) B (20%)

DarkCyberGhost Highly Voted 2 years, 5 months ago

Servers are not Mobile and MDM is Mobile Device Management, so the only answer to choose here is Windows 10 as it can be installed on a laptop making it Mobile. HOPE this helps.

upvoted 43 times

NadirM_18 2 years ago

It helped :-)

upvoted 2 times

JohnBentass 1 year, 6 months ago

Good explanation

upvoted 2 times

gcpbrig01 Highly Voted 3 years, 3 months ago

correct answer. intunes enrollment works with windows 10 version 1809 or later

upvoted 31 times

somenick 1 year, 8 months ago

Intune is not a part of the exam anymore: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VC70

upvoted 4 times

wardy1983 Most Recent 7 months, 2 weeks ago

Answer: A

Explanation:

intunes enrollment works with windows 10 version 1809 or later

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

upvoted 2 times

BigShot0 9 months, 1 week ago

Selected Answer: A

Cannot have baselines with Server or Unix

upvoted 3 times

ITFranz 9 months, 1 week ago

You deploy security baselines to groups of users or devices in Intune, and the settings apply to devices that run Windows 10 or 11.

https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines

correct Answer: A (Windows 10)

upvoted 1 times

ESAJRR 10 months, 3 weeks ago

Selected Answer: A

A. VM1 only

upvoted 2 times

tecnicosoffshoretech 1 year, 2 months ago

Selected Answer: B

Is the B. Security baselines can be applied to Windows Servers too. The servers cant be enrolled in Intune but the can be managed from MEM if the MDE connector for intune is configured.

upvoted 2 times

tecnicosoffshoretech 1 year, 2 months ago

https://learn.microsoft.com/en-us/mem/intune/protect/mde-security-integration

upvoted 1 times

BigShot0 9 months, 1 week ago

No, They cannot have a baseline profile. I have tried to configure Conditional Access for servers based on baselines and it is not possible. Recently they enabled defender policies for Server products but that is not the same as baselines.

upvoted 1 times

majstor86 1 year, 3 months ago

Selected Answer: A

A. VM1 only

upvoted 2 times

ligu 1 year, 4 months ago

Answer is correct

upvoted 1 times

boapaulo 1 year, 7 months ago

No exame 28/11/22

upvoted 1 times

F117A_Stealth 1 year, 7 months ago

Selected Answer: A

VM1 Only... Intune or MEM, can apply baselines to Windows 10

upvoted 1 times

Ivanvazovv 1 year, 10 months ago

Shouldn't this be in MS-500 exam rather than AZ-500?

upvoted 4 times

Alessandro365 2 years ago

Selected Answer: A

A is correct answer.

upvoted 1 times

cfsxtuv33 2 years, 5 months ago

This feature applies to:

Windows 10 version 1809 and later

Windows 11

Link: https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

upvoted 2 times

orallony 2 years, 9 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 4 times

Amin_7 3 years ago

Use security baselines to configure Windows 10 devices in Intune

01/29/2021

8 minutes to read

+2

In this article

Available security baselines

About baseline versions and instances

Avoid conflicts

Q & A

Next steps

Use Intune's security baselines to help you secure and protect your users and devices. Security baselines are pre-configured groups of Windows settings that help you apply the security settings that are recommended by the relevant security teams. You can also customize the baselines you deploy to enforce only those settings and values you require. When you create a security baseline profile in Intune, you're creating a template that consists of multiple device configuration profiles.

This feature applies to:

Windows 10 version 1809 and later

https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

upvoted 1 times

⊟ **Deboe07** 3 years ago

servers are not mobile devices

upvoted 7 times

Question #18 *Topic 3*

SIMULATION -

You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

You need to configure the Network Security Group that is associated with subnet0.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to

Virtual Networks in the left navigation pane.

2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.

3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.

4. In the properties of the Network Security Group, click on Inbound Security Rules.

5. Click the Add button to add a new rule.

6. In the Source field, select Service Tag.

7. In the Source Service Tag field, select Internet.

8. Leave the Source port ranges and Destination field as the default values (* and All).

9. In the Destination port ranges field, enter 7777.

10.Change the Protocol to TCP.

11.Leave the Action option as Allow.

12.Change the Priority to 100.

13.Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces.

14.Click the Add button to save the new rule.

Mic8888 Highly Voted 3 years, 2 months ago

All services or type 'network security groups' on the search bar > click your target NSG > on Settings, click 'Inbound security rules' > click + Add > Source: service tag, destination port: 7777, Protocol: TCP, Priority:100, Name:<provide name>, and leave the rest as defaults > click Add

upvoted 14 times

CarlosBarrero Highly Voted 4 years, 4 months ago

the answer is correct

upvoted 8 times

Viggy1212 Most Recent 8 months, 3 weeks ago

Question says Traffic should be allowed from Internet to subnet0. Usage of Destination "Any" will allow traffic to all subnet which is little over the requirement. Hence only CIDR notation of subnet2 only should be mentioned in Destination of Inbound Security rule.

upvoted 1 times

mrt007 1 year, 3 months ago

Sign in to the Azure portal.

In the left-hand menu, click on “All services”.

In the “All services” box, type “Network Security Group”.

Click on the “Network Security Groups” item in the search results.

In the “Network security groups” window, find and click on the network security group that is associated with VNET1\subnet0.

In the settings menu of the selected network security group, click on “Inbound security rules”.

Click on the “+ Add” button to create a new inbound security rule.

In the “Add inbound security rule” window, fill in the following details:

Source: Any

Source port ranges: *

Destination: Any

Destination port ranges: 7777

Protocol: TCP

Action: Allow

Priority: Choose a value less than 65000. Lower numbers have higher priorities.

Name: Choose a name for this rule.

Click on the “Add” button to create the rule.

upvoted 3 times

⊟ **fireb** 1 year, 9 months ago

Answer provided is correct.

upvoted 1 times

⊟ **F117A_Stealth** 2 years, 7 months ago

the answer is correct

upvoted 1 times

⊟ **Patchfox** 3 years, 6 months ago

Correct. All other default rules already block traffic from outside the vnet.

upvoted 1 times

⊟ **orallony** 3 years, 9 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 3 times

⊟ **OldJan** 3 years, 7 months ago

So the simulation questions are back?

upvoted 1 times

⊟ **JAGUDERO** 4 years, 2 months ago

something is missing, This does not restrict the currently deployed resources

upvoted 1 times

⊟ **eroms** 4 years, 1 month ago

Maybe restrict destination field to the Subnet of the connected Vnet1.

upvoted 1 times

⊟ **Ed2learn** 4 years, 1 month ago

Think you misread the question. You do not need to restrict existing resources - you cannot create new resources. In other words you must add rule to existing NSG

upvoted 2 times

Question #19 *Topic 3*

SIMULATION -

You need to prevent administrators from performing accidental changes to the Homepage app service plan.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.

1. In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage. Alternatively, browse to App Service Plans in the left navigation pane.
2. In the properties of the app service plan, click on Locks.
3. Click the Add button to add a new lock.
4. Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.
5. For the Lock type, select Read-only.
6. Click OK to save the changes.

⊟ **Ed2learn** Highly Voted 👍 4 years, 1 month ago

This is correct.

upvoted 9 times

⊟ **randy0077** Most Recent 3 months ago

it should be delete lock:

Read-only (blocks all modifications)

Delete (only prevents deletion)

upvoted 1 times

⊟ **schpeter_091** 8 months ago

App Service Plan --> Locks --> Add

upvoted 2 times

⊟ **F117A_Stealth** 2 years, 7 months ago

Answer is correct. They are testing your knowledge on Locks.

upvoted 3 times

Question #20 *Topic 3*

SIMULATION -

You need to ensure that a user named Danny1234578 can sign in to any SQL database on a Microsoft SQL server named web1234578 by using SQL Server
Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

You need to provision an Azure AD Admin for the SQL Server.

1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web1234578.
Alternatively, browse to SQL Server in the left navigation pane.
2. In the SQL Server properties page, click on Active Directory Admin.
3. Click the Set Admin button.
4. In the Add Admin window, search for and select Danny1234578.
5. Click the Select button to add Danny1234578.
6. Click the Save button to save the changes.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell

F117A_Stealth Highly Voted 2 years, 7 months ago

Confirmed in Prod, this is correct. Steps are right.

upvoted 7 times

schpeter_091 Most Recent 7 months, 1 week ago

In case, don't forget to untick the "Microsoft Entra authentication only"

upvoted 1 times

pentium75 11 months ago

But "sign in to any SQL database" does not necessarily mean that he should have admin permissions ...

upvoted 3 times

Alagong 1 year, 2 months ago

SQL Servers > Microsoft Entra ID > Set admin

upvoted 2 times

Rachy 1 year, 11 months ago

steps are correct

upvoted 3 times

Question #21 *Topic 3*

SIMULATION -

You need to configure a Microsoft SQL server named Web1234578 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

To complete this task, sign in to the Azure portal.

Suggested Answer: *See the explanation below.*

You need to allow access to Azure services and configure a virtual network rule for the SQL Server.

1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web1234578. Alternatively, browse to SQL Server in the left navigation pane.
2. In the properties of the SQL Server, click Firewalls and virtual networks.
3. In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.
4. Give the rule a name such as Allow_VNET01-Subnet0 (it doesn't matter what name you enter for the exam).
5. In the Virtual network box, select VNET01.
6. In the Subnet name box, select Subnet0.
7. Click the OK button to save the rule.
8. Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

⊟ **ylfr** Highly Voted 👍 2 years, 2 months ago

It is no longer up to date..

now it's in SQL SERVER > Networking > Add a virtual network rule

now it's in SQL SERVER > Networking > Add a virtual network rule

upvoted 14 times

⊟ **somboy** 2 years, 2 months ago

Thank you..

upvoted 1 times

⊟ **Anil512** Most Recent 🕒 3 months, 3 weeks ago

Pick Server >> Security >> Networking >> Add a Virtual Network Rule >> Choose VNET and Subnet >> Enable.

upvoted 1 times

⊟ **ITFranz** 4 months, 2 weeks ago

Steps.

1. Navigate to the Azure portal and locate the Web1234578 SQL server.
2. In the server's settings, go to the "Networking" section.
3. Under "Firewalls and virtual networks", select "Selected networks".
4. In the "Virtual networks" section, click "Add existing virtual network".
5. Select VNET01 from the list of virtual networks.
6. Choose Subnet0 from the list of subnets within VNET01.
7. Click "OK" to add the selected subnet.
8. Ensure that "Allow Azure services and resources to access this server" is set to "No" unless specifically required.
9. Remove any existing firewall rules that allow access from other IP ranges.
10. Click "Save" to apply the changes.

upvoted 1 times

⊟ **cris_exam** 11 months, 1 week ago

Also, guys, keep in mind that this setup alone without also setting the Microsoft.SQL Service Endpoint on the Subnet of the VNET will not successfully communicate with the SQL server- in case it's possible to do or to check on the SIM, it's an important piece of the communication config to set up the SQL Service Endpoint.

upvoted 1 times

⊟ **machado** 1 year, 8 months ago

Why not a private endpoint?

upvoted 1 times

⊟ **cris_exam** 11 months, 1 week ago

The private endpoint goal is to give the SQL Server (whish is a PaaS) a place and an identity into a VNET (IAAS), hence integrating the SQL resource to be accessible within that VNET/subnet where you plant it but also form wherever else from your environment as long as there is network connectivity to the Private Endpoint of the SQL PaaS service.

For this exercise purpose, the goal is to only have that specific VNET/Subnet be able to connect to the SQL Server and not make it fully available to the IaaS private network environment.

upvoted 1 times

Macke53 1 year, 8 months ago

Answer is outdated. Current answer is SQL Server>Security>Networking. By default public access is disabled. Change radio button to "Selected Networks" and add Vnet

upvoted 2 times

F117A_Stealth 2 years, 1 month ago

1. SQL Server
2. Under Security Select Networking
3. Under Public Access Tab, you will see Virtual Networks below
4. Click the + on "add a virtual network rule"
5. Enter the data.

upvoted 3 times

Question #22 *Topic 3*

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. device configuration policies in Microsoft Intune

B. an Azure Desired State Configuration (DSC) virtual machine extension

C. security policies in Azure Security Center

D. Azure Logic Apps

Suggested Answer: *B*
The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service.
The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring.
Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

Community vote distribution

B (100%)

⊟ **Ed2learn** Highly Voted 3 years, 1 month ago
third time this question has appeared in this question set but the answer is still correct.
upvoted 17 times

⊟ **madhatter** 1 year, 9 months ago
My guess is that each question "SET" contains similar testing questions if not identical questions. If you notice you'll go through a set of 60ish questions and then the counter resets to 1. I believe there are NO 300+ unique questions in the question pool, just sets that will obviously test you with similar type questions with some repeating.
upvoted 1 times

⊟ **LJack** Highly Voted 3 years, 3 months ago
Correct answer
upvoted 9 times

⊟ **ESAJRR** Most Recent 10 months ago
Selected Answer: B
B. an Azure Desired State Configuration (DSC) virtual machine extension
upvoted 1 times

⊟ **majstor86** 1 year, 3 months ago
Selected Answer: B
B. an Azure Desired State Configuration (DSC) virtual machine extension
upvoted 1 times

⊟ **ligu** 1 year, 4 months ago
Answer is correct
upvoted 1 times

⊟ **chikorita** 1 year, 4 months ago
i've learned the answer to this question even without fully reading the question
if this question wont be on my actual test, i'll be doomed
UGH!!!!!!!!!!
upvoted 1 times

⊟ **F117A_Stealth** 1 year, 7 months ago
Selected Answer: B
B. an Azure Desired State Configuration (DSC) virtual machine extension

upvoted 1 times

⊟ **Alessandro365** 2 years ago

Selected Answer: B

B is correct answer.

upvoted 1 times

⊟ **Eltooth** 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

⊟ **udmraj** 2 years, 4 months ago

Correct Answer-- B

upvoted 1 times

⊟ **cfsxtuv33** 2 years, 6 months ago

Repeat question and the answer is still correct.

upvoted 1 times

⊟ **adamsca** 2 years, 6 months ago

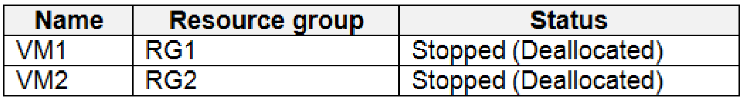
Correct. This is also a duplicate of Q27 Topic3

upvoted 1 times

Question #23 *Topic 3*

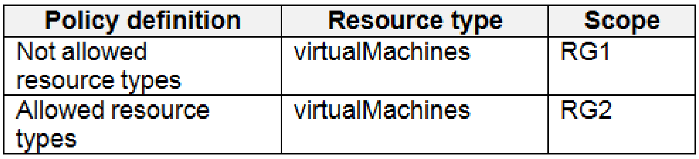
HOTSPOT -

You have an Azure subscription that contains the virtual machines shown in the following table.



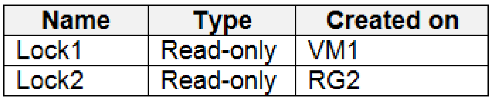
Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.



Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

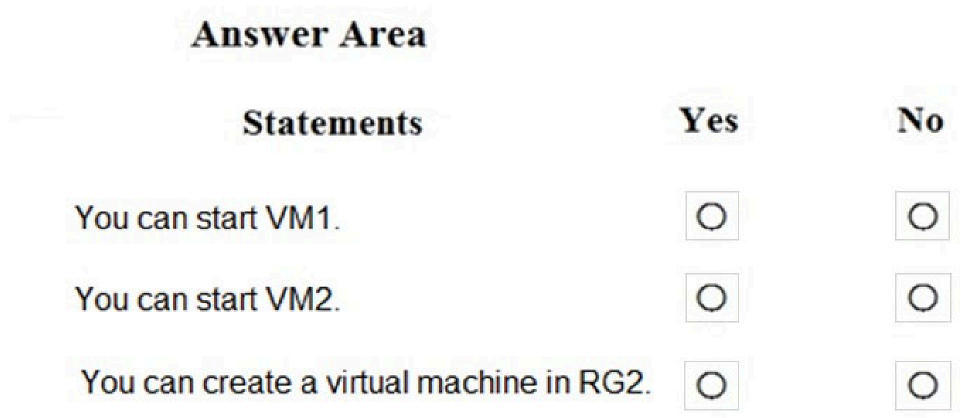


Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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

NOTE: Each correct selection is worth one point.

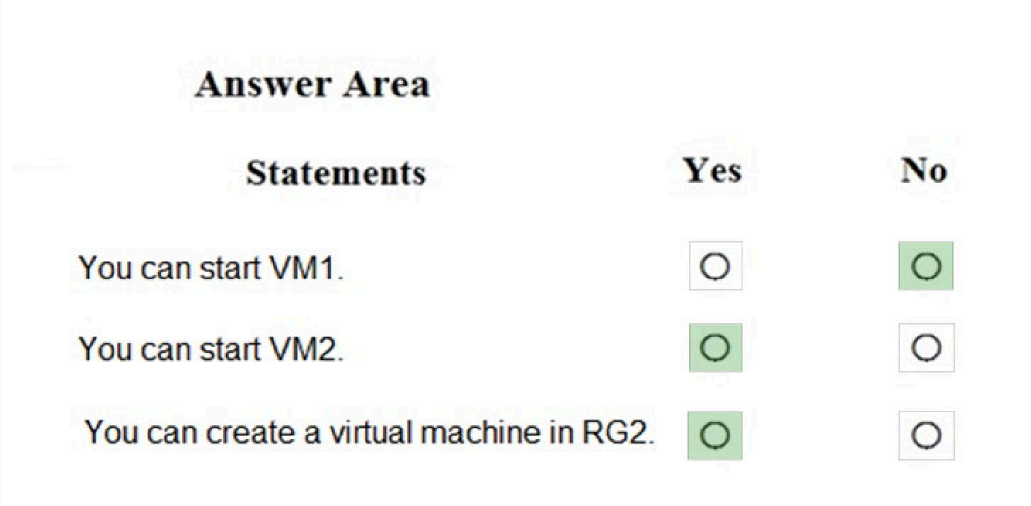
Hot Area:



Answer Area

Statements	Yes	No
You can start VM1.	○	○
You can start VM2.	○	○
You can create a virtual machine in RG2.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
You can start VM1.	○	[✓ ○]
You can start VM2.	[✓ ○]	○
You can create a virtual machine in RG2.	[✓ ○]	○

References:

https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

snelkoppeling Highly Voted 5 years, 1 month ago

You cannot start VM1 because of read only lock on VM1

You cannot start VM2 because of read only lock on RG2

You cannot create a new VM in RG2 because of read only lock on RG2

upvoted 396 times

prd0202 3 years, 8 months ago

No doubt - it is No, No, No

upvoted 14 times

AP_Singh 4 years, 11 months ago

your answers are all correct

ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

upvoted 13 times

sureshatt 3 years, 9 months ago

this is the correct answer.

upvoted 6 times

OpsecDude 2 years, 3 months ago

Exactly, I mean Read only is Read only. I you placed a Read only lock is because you want nothing to be modified at all

upvoted 2 times

xBoy 3 years, 9 months ago

No/No/No. Tested on LAB

upvoted 14 times

jbarszcz Highly Voted 4 years, 9 months ago

just tested it. No/No/No

upvoted 75 times

golitech Most Recent 4 months, 4 weeks ago

NYN

RG2 is read only, but starting a VM can be done (it is an operation), but we cannot create a VM.

RG2 is read-only. it overwrites the policy. Lock is stronger that the policy

upvoted 1 times

Pamban 7 months, 2 weeks ago

NNN

lab tested

upvoted 2 times

bobbywong234 9 months, 3 weeks ago

A lot of fools forgot to read the second table, Azure policy

upvoted 1 times

flafernan 1 year ago

No, No, No.

upvoted 3 times

AZ5002023 1 year ago

tested on lab : NO NO NO

upvoted 4 times

wardy1983 1 year, 2 months ago

You cannot start VM1 because of read only lock on VM1

You cannot start VM2 because of read only lock on RG2

You cannot create a new VM in RG2 because of read only lock on RG2

upvoted 5 times

Feraso 1 year, 2 months ago

Correct Answer

Pay attention to where the look is applied.

Refer to: https://learn.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking#locking-modes-and-states

Read Only Resource group Cannot Edit / Delete The resource group is read only and tags on the resource group can't be modified. Not Locked resources can be added, moved, changed, or deleted from this resource group.

Read Only Non-resource group Read Only The resource can't be altered in any way. No changes and it can't be deleted.

When the lock is applied on the resource itself(VM1), we won't be able to make any changes.
Hence, we can't start it.
However, when the lock is applied on the Resource Group, then VM2 is not locked resource, thus, we will be able to change it.
Therefore, we can start VM2 and we can create a VM in RG2.
upvoted 2 times

⊟ **ErikPJordan** 1 year, 3 months ago
Computer says no no no
upvoted 3 times

⊟ **ESAJRR** 1 year, 4 months ago
1000x
No/No/No
upvoted 2 times

⊟ **heatfan900** 1 year, 4 months ago
n, n, n

Both VMs have READ-ONLY LOCKS
VM1 directly and VM2 via the lock to RG2
The policy plays no part here
upvoted 2 times

⊟ **ykamal** 1 year, 4 months ago
Can the admins fix this exam please? There are too many incorrect answers. For this question it is NNN.
upvoted 3 times

⊟ **Franc_Coetzee** 1 year, 6 months ago
The resource group is read only and tags on the resource group can't be modified. Not Locked resources can be added, moved, changed, or deleted from this resource group.

https://learn.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking
upvoted 1 times

⊟ **Maged_nader12** 1 year, 8 months ago
so why ET leaves these wrong answers on the questions !!! so why are we paying for this shit !
upvoted 5 times

⊟ **mskott** 1 year, 9 months ago
The read-only lock only affects the ability to modify or delete resources within the resource group, but it does not prevent the creation of new resources in the resource group. So, you can create a new VM in the resource group with a read-only lock without any issues.

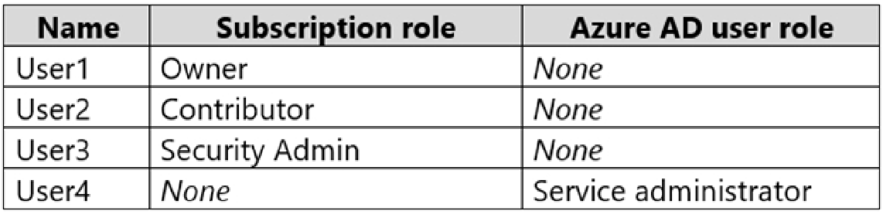
So it is No-No-Yes
upvoted 1 times

⊟ **majstor86** 1 year, 10 months ago
No
No
No
upvoted 2 times

Question #24 Topic 3

HOTSPOT -

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



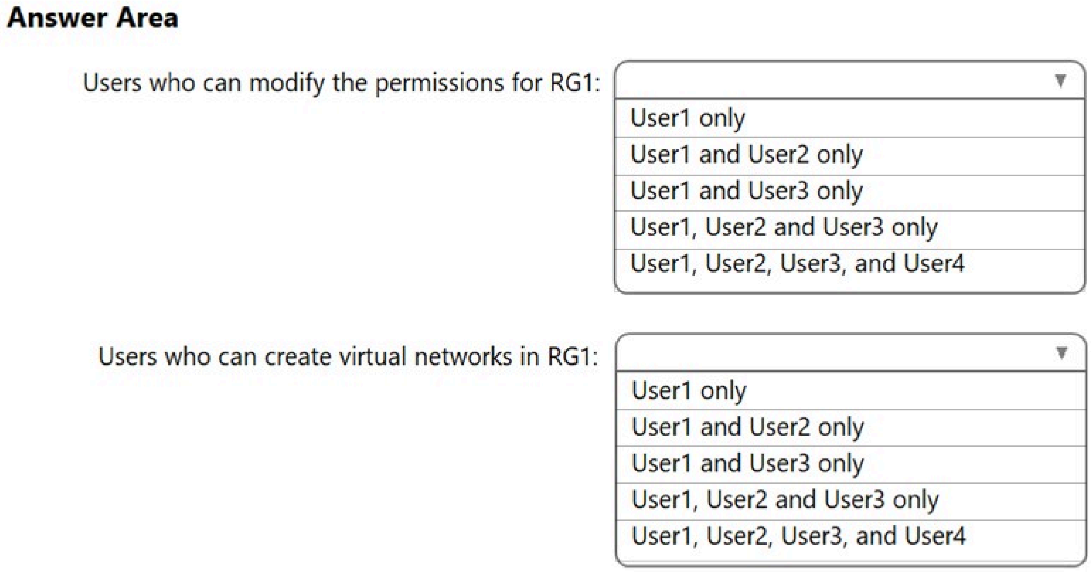
Name	Subscription role	Azure AD user role
User1	Owner	*None*
User2	Contributor	*None*
User3	Security Admin	*None*
User4	*None*	Service administrator

You create a resource group named RG1.

Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

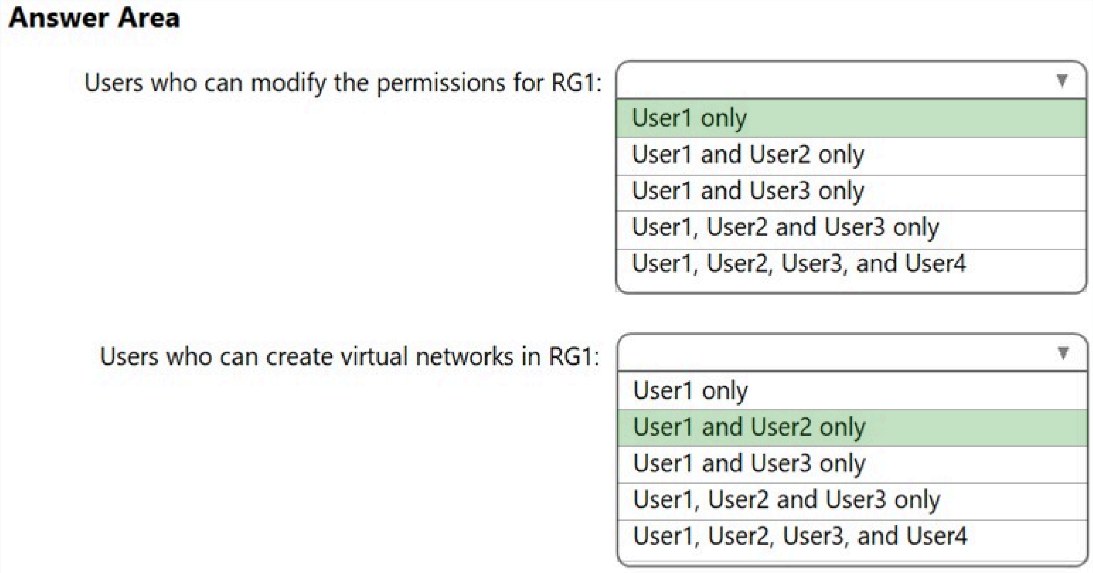
Users who can modify the permissions for RG1:

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Users who can create virtual networks in RG1:

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Suggested Answer:



Answer Area

Users who can modify the permissions for RG1:

- [✓ User1 only]
- User1 and User2 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Users who can create virtual networks in RG1:

- User1 only
- [✓ User1 and User2 only]
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Box 1: Only an owner can change permissions on resources.

Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

JohnYinToronto Highly Voted 2 years, 9 months ago

answers correct

upvoted 41 times

francis6170 Highly Voted 2 years, 3 months ago

Got this in the AZ-500 exam (Sept 2021)! A: U1, U1 and U2

upvoted 17 times

4f13cca Most Recent 3 months, 1 week ago

Please provide a source why the owner is the only one able to modify the permissions

upvoted 1 times

majstor86 10 months ago

User 1 only

User 1 and User 2 only

upvoted 9 times

ligu 10 months, 1 week ago

The answers are correct

upvoted 2 times

samimshaikh 11 months ago

Contributor role: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC... I will go with User1 only,

User1&User2 Only.

upvoted 8 times

Oskarma 1 year, 2 months ago

I think Service administrator can modify permissions and create virtual networks in RG1:

The Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.

The Service Administrator has full access to the Azure portal.

https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles#:~:text=The%20Service%20Administrator%20has%20the%20equivalent%20access%20of%20a%20user%20who%20is%20assigned%20the%20Owner%2

upvoted 1 times

> **Oskarma** 1 year, 2 months ago
>
> I answer to myself. Service Administrator is for the classic deployment (before RBAC). And "The two models aren't compatible with each other."
>
> https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/deployment-models
>
> So the given answers are correct.
>
> upvoted 3 times

zukako 1 year, 4 months ago

Only User Access Admin/Owner can modify permission

upvoted 3 times

Sweet_co 1 year, 5 months ago

In exam: 20-7-2022

upvoted 3 times

NinjaSchoolProfessor 1 year, 5 months ago

In exam 15-July-2022

upvoted 4 times

luckflying 1 year, 6 months ago

The 1st answers is Wrong!

Contributors does not allow you to assign roles, but it can change permission of resources.

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-admin

upvoted 1 times

> **costaluisc** 1 year, 5 months ago
>
> User 1 is "Owner" not "contributor"
>
> upvoted 2 times

Exams_Prep_2021 1 year, 6 months ago

In Exam - 20/6/2022 - 1 Case Study (6) - Lab (10 Tasks)

upvoted 5 times

WhalerTom 2 years ago

In exam Dec 21. 40 questions, 1 case study, no labs.

upvoted 3 times

Jco 2 years, 3 months ago

#exam ques # 29 Sep

upvoted 1 times

TonytheTiger 2 years, 3 months ago

## Exam Question - 17 Sept 2021 ##

upvoted 2 times

JChris 2 years, 3 months ago

Hello, did you get any simulation questions in your exam? Ty.

upvoted 1 times

little_h0rse 2 years, 7 months ago

Only Owner & User Access Administrator access have rights to delegate access to others.
In order to get User Access Administrator, user needs to be Global admin in Azure AD.

upvoted 5 times

dadageer 2 years, 9 months ago

Correct!

upvoted 9 times

Question #25 *Topic 3*

SIMULATION -
You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Suggested Answer: *See the explanation below.*
You need to configure VNet Peering between the two networks. The questions states, ג€The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2ג€. It doesn't say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to
Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Peerings.
3. In the Peerings blade, click Add to add a new peering.
4. In the Name of the peering from VNET1 to remote virtual network box, enter a name such as VNET1-VNET2 (this is the name that the peering will be displayed as in VNET1)
5. In the Virtual Network box, select VNET2.
6. In the Name of the peering from remote virtual network to VNET1 box, enter a name such as VNET2-VNET1 (this is the name that the peering will be displayed as in VNET2).
There is an option Allow virtual network access from VNET to remote virtual network. This should be left as Enabled.
7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.
8. Click the OK button to save the changes.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering

MarioMK Highly Voted 2 years, 7 months ago
To prevent communication to Vnet1 from Vnet2, the option "Traffic to remote virtual network" must be set to Block. A small popup will be shown saying the following: "Resources in Vnet2 cannot communicate to resources in the Vnet1"
upvoted 16 times

Zorag 2 years, 7 months ago
Awesome this does the trick
upvoted 3 times

Pasapugazh 1 year, 2 months ago
This doesn't work for me and While setting the value to Block for "Traffic to remote virtual network" option in Vnet2 it is saying that the "Resources from Vnet1 can not communicate to the resources in Vnet2" but not from Vnet2 to Vnet1.
Tried all the possible options in the peering but none has work worked. In the end creating a NSG in the Vnet1 to block the Vnet2 traffic does the work.
upvoted 1 times

sureshatt Highly Voted 2 years, 9 months ago
Tested the following setting and I can ping from VNET1 to VNET2, but not from VNET2 to VNET1.

VNET1 - peering setting
Traffic to remote virtual network: Allow (default)
Traffic forwarded from remote virtual network: Block traffic that originates from outside this virtual network
Virtual network gateway or Route Server: None (default)

VNET2 - peering setting
Traffic to remote virtual network: Block all traffic to the remote virtual network
Traffic forwarded from remote virtual network: Block traffic that originates from outside this virtual network
Virtual network gateway or Route Server: None (default)
upvoted 12 times

eroms 2 years, 7 months ago

tested it and it failed. You need an NSG rule for this to work

upvoted 4 times

OrangeSG Most Recent 11 months ago

Refer to Microsoft support reply:

In general when Vnet are peered with each other, controlling access between them can be done by using Azure Network Security Groups which filter network traffic to and from Azure resources in an Azure virtual network.

https://learn.microsoft.com/en-us/answers/questions/569509/vnet-one-way-traffic-route-help

upvoted 1 times

Disparate 11 months, 1 week ago

But. This is a lab. On exams actually there is not labs, correct?

upvoted 1 times

r_git 9 months, 1 week ago

Labs are back. A friend of mine took the exam this week. Labs were in it.

upvoted 3 times

Dinraj 11 months, 2 weeks ago

Question doesn't say that not to communicate from VNET2 to VNET1 then why should block that remote traffic to VNET1 from VNET2

I think question phrase is confusing

upvoted 3 times

Ivanvazovv 1 year, 4 months ago

The word "communicate" assumes traffic in both directions.

upvoted 5 times

madhatter 1 year, 3 months ago

Tricky but careful as it only states that VNET1 VMs must communicate to VNET2 VMs. Never says VNET 2 VMS must make communication to VNET1. Wording should state "start communications with VNET X" Implying the ability for one side to start communication with another side. The answer is correct in disabling the ability for VNET2 to contact VNET1. Bi-directional communication from VNET1 to VNET2 from VNET1 sessions is implied.

upvoted 1 times

COVID22 1 year, 5 months ago

Please in the simulation questions on the exam day, will the options for the answers be made available

upvoted 1 times

Joshing 1 year, 10 months ago

Tested this.

Vnet1 -

Traffic to remote virtual network: Allow

Traffic forwarded from remote virtual network: Block

Vnet2 -

Traffic to remote virtual network: Block

Traffic forwarded from remote virtual network: Block

Vnet2 NSG -

Inbound Security Rule - Port: Any, Protocol: Any, Source: {insert subnets}, Destination: VirtualNetwork, Action: Allow.

upvoted 5 times

imie 1 year, 12 months ago

in Exam 31 Dec 2021.

upvoted 2 times

Tash95 1 year, 10 months ago

Did you have to create an NSG for it to be given as OK, or was it enough with the VNet peering settings?

upvoted 2 times

haitao1234 1 year, 8 months ago

It seems Imie has replied in many simulation questions that he did simulation. so the question is: How many simulation do you have in your test?

upvoted 3 times

adamsca 2 years ago

# Exam Question 12/10/2021

upvoted 2 times

JBS 2 years, 2 months ago

This is working as required in the question. Ping is not a right way to test it as ICMP requires allow on both sender and receiver ends. Good way to test it is by doing RDP from VNET1 to VNET2 (this should be allowed) and RDP from VNET2 to VNET1 (this should not be allowed)

VNET1 - peering setting

Traffic to remote virtual network: Allow (default)

Traffic forwarded from remote virtual network: Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server: None (default)

VNET2 - peering setting

Traffic to remote virtual network: Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network: Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server: None (default)

upvoted 2 times

Zorag 2 years, 7 months ago

The way I got this working is doing the below

1. Create a peering between the two VNETS allowing all traffic both sides.
2. Create an NSG and assign it to VNET1 on the subnet where the VMs exist. In my case this was Subnet1.
3. Create an inbound rule on the NSG denying all traffic from the address space on VNET2.
4. Once done you will be able to communicate from VNET1 to VNET2 but not VNET2 to VNET1.

upvoted 4 times

Fred64 2 years, 8 months ago

why in step 6 it is said to not activate bi directional communication?

upvoted 1 times

AZRA068 2 years, 11 months ago

In the step 7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled........This means that the VNET1 won't be included in the VirtualNetwork TAG used in the NSG default rules on each resource, so ok, traffic from VNET1 to VNET2 will be allowed on VNET1 side, but on VNET2 side it won't be allowed by default....so, it won't allow communication from VNET1 to VNET2 at all; you'll need an especific NSG rule in the resources on VNET2 to allow the traffic you need as the VNET1 is not included in the Virtual Networl TAG, just tested it.

upvoted 2 times

AZRA068 2 years, 11 months ago

...or set this configuration as ENABLED, so the VNET1 will be included in the VirtualNEtwork TAG on the VNET2 side also, so the default rules will allow the communication, and yes, also it will allow traffic from VNET2 to VNET1.

upvoted 3 times

gcpbrig01 2 years, 9 months ago

I am inclined to this option when you alow network access from remote network to VNET1. I strongly feel that without toggling this on, even traffic from vnet1 to vnet2 wont be allowed.

upvoted 1 times

Nnanna29 3 years, 1 month ago

The provided answer is correct as VMs in Vnet 1 can communicate with VMs in Vnet 2 and not bi-directional communication

upvoted 2 times

realname007 3 years, 1 month ago

anyone knows the updated answer for this using the current interface ?

upvoted 2 times

Question #26 *Topic 3*

SIMULATION -

You need to deploy an Azure firewall to a virtual network named VNET3.

To complete this task, sign in to the Azure portal and modify the Azure resources.

This task might take several minutes to complete. You can perform other tasks while the task completes.

Suggested Answer: *See the explanation below.*

To add an Azure firewall to a VNET, the VNET must first be configured with a subnet named AzureFirewallSubnet (if it doesn't already exist).

Configure VNET3.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET3. Alternatively, browse to

Virtual Networks in the left navigation pane.

2. In the Overview section, note the Location (region) and Resource Group of the virtual network. We'll need these when we add the firewall.
3. Click on Subnets.
4. Click on + Subnet to add a new subnet.
5. Enter AzureFirewallSubnet in the Name box. The subnet must be named AzureFirewallSubnet.
6. Enter an appropriate IP range for the subnet in the Address range box.
7. Click the OK button to create the subnet.

Add the Azure Firewall.

1. In the settings of VNET3 click on Firewall.
2. Click the Click here to add a new firewall link.
3. The Resource group will default to the VNET3 resource group. Leave this default.
4. Enter a name for the firewall in the Name box.
5. In the Region box, select the same region as VNET3.
6. In the Public IP address box, select an available public IP address if one exists, or click Add new to add a new public IP address.
7. Click the Review + create button.
8. Review the settings and click the Create button to create the firewall.

Reference:

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

⊟ **[Removed]** Highly Voted 👍 3 years, 6 months ago

If you get this question on the exam, make sure to go into VNET3's address space and add another one. If you don't, you will not be able to create the AzureFireWall subnet and you will not complete the Azure Firewall configuration.

upvoted 11 times

> ⊟ **xRiot007** 11 months, 1 week ago
>
> Correct. Az Firewall needs its OWN subnet. There can be nothing else on it.
>
> upvoted 2 times

⊟ **Tombarc** Highly Voted 👍 3 years, 5 months ago

I'm not sure if it makes any difference to the question, but it is recommended the AzureFirewallSubnet subnet has /26 size:

https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#why-does-azure-firewall-need-a--26-subnet-size

https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#why-does-azure-firewall-need-a--26-subnet-size

upvoted 6 times

⊟ **mrt007** Most Recent ⊙ 1 year, 3 months ago

Sign in to the Azure portal: Go to https://portal.azure.com and sign in with your Azure account credentials.

Select “Create a resource”: On the left-hand menu, click on “+ Create a resource”.

Search for “Firewall”: In the “Search the Marketplace” box, type “Firewall” and select “Firewall” from the dropdown menu.

Create firewall: Click the “Create” button to start the Azure Firewall deployment process.

Configure basic settings:

Subscription: Select your Azure subscription.

Resource group: Choose the resource group where VNET3 is located.

Name: Enter a name for the firewall.

Region: Choose the region where VNET3 is located.

Configure networking settings:

Virtual network: Select VNET3 from the dropdown menu.

Public IP address: Create a new public IP address or use an existing one.

Review + create: Review your settings and click “Create” to deploy the Azure Firewall to VNET3.

upvoted 2 times

⊟ **Rhonwen** 1 year, 3 months ago

My questions is, from the VNet, why can't the Firewall be added from the Firewall blade in Settings?

upvoted 1 times

⊟ **Kelly8023** 2 years, 8 months ago

Subnet name needs to be AzureFirewallManagementSubnet

upvoted 2 times

⊟ **GenPatton** 2 years, 6 months ago

AzureFirewallManagementSubnet = With forced tunneling

AzureFirewallSubnet = Without forced tunneling

Determined at creation of firewall - cannot be changed later.

upvoted 1 times

⊟ **MaeseG** 2 years, 7 months ago

Totally wrong my friend, as you can see in the URL (https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-vnet STEP 10) the name for the subnet MUST be AzureFirewallSubnet.

Cheers.

upvoted 5 times

⊟ **macka2005** 2 years, 6 months ago

"Force tunneling requires this virtual network have a subnet named AzureFirewallManagementSubnet" in the Azure portal when tested today

upvoted 2 times

⊟ **lt9898** 1 year, 7 months ago

You will see this message if you've selected 'Basic' as the tier since forced tunnelling is mandated. If you select 'Standard' instead, that message will disappear and you return to requiring 'AzureFirewallSubnet'.

upvoted 1 times

⊟ **Haq47** 3 years, 6 months ago

Just did mine today. When you opened the subnet in vnet 3, you can already see an existing subnet.. i just deleted that and reused the same subnet with the new azurefirewallsubnet

upvoted 3 times

⊟ **adamsca** 3 years, 6 months ago

# Exam Question 12/10/2021

upvoted 4 times

⊟ **vishg** 4 years, 7 months ago

Also Required to add routing rule.

upvoted 3 times

⊟ **Fred64** 4 years, 3 months ago

yes but we don't have enough informations to define the route. What is the next hop?

upvoted 3 times

Question #27 *Topic 3*

SIMULATION -

You need to configure a virtual network named VNET2 to meet the following requirements:

✑ Administrators must be prevented from deleting VNET2 accidentally.

✑ Administrators must be able to add subnets to VNET2 regularly.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Suggested Answer: *See the explanation below.*

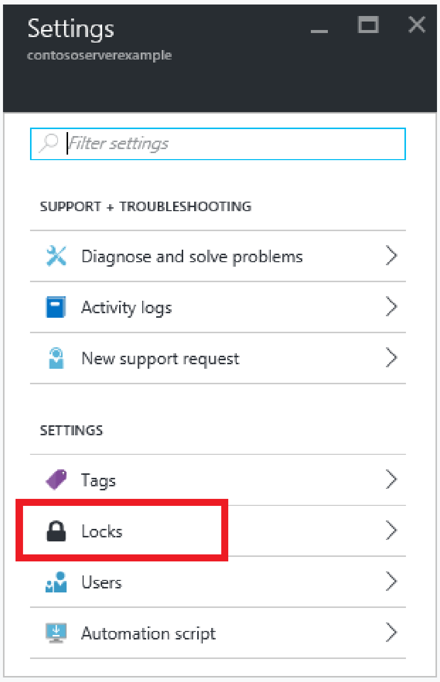
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

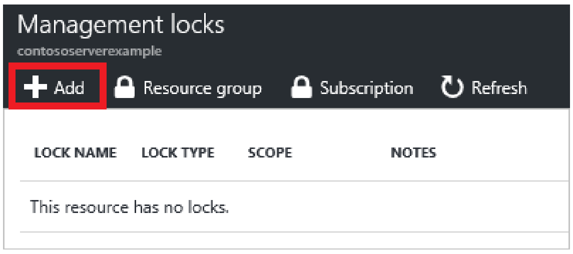
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET2. Alternatively, browse to

Virtual Networks in the left navigation pane.

2. In the Settings blade for virtual network VNET2, select Locks.



3. To add a lock, select Add.



LOCK NAME	LOCK TYPE	SCOPE	NOTES
This resource has no locks.			

4. For Lock type select Delete lock, and click OK

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

LJack Highly Voted 3 years, 9 months ago

This is the correct procedure for requirements outlined.

upvoted 8 times

mrt007 Highly Voted 9 months ago

Sign in to the Azure portal at https://portal.azure.com.

In the left-hand menu, click on “Virtual networks”.

In the virtual networks pane, find and click on VNET2.

To prevent accidental deletion, you can use Locks. Here’s how:

In the VNET2 pane, click on “Locks” under the Settings section.

Click on “+ Add”.

Provide a name for the lock, select “Delete” for the lock type, and click “OK”. This will prevent accidental deletion of VNET2.

To allow administrators to add subnets regularly, you don’t need to do anything special because by default, administrators have the necessary permissions to add subnets. Here’s how to add a subnet:

In the VNET2 pane, click on “Subnets” under the Settings section.

Click on “+ Subnet”.

Provide the necessary details for the subnet and click “OK”.

upvoted 5 times

⊟ **Tash95** Most Recent 2 years, 10 months ago

For the "Administrators must be able to add subnets to VNET2 regularly." part, would admins always have this permission? Or would we have to assign the Network Contributor role to an admin user during the exam?

upvoted 4 times

⊟ **Mugamed** 1 year, 7 months ago

Network contributor is the correct role.

upvoted 2 times

⊟ **Rick_C137** 2 years, 8 months ago

This is to mean that they want you to choose the "Delete" lock type as opposed to the "Read-Only". Both would not allow you to delete but only "Delete" would still allow admins to add subnets.

upvoted 12 times

Question #28 *Topic 3*

You have an Azure virtual machine named VM1.
From Microsoft Defender for Cloud, you get the following high-severity recommendation: `Install endpoint protection solutions on virtual machine`.
You need to resolve the issue causing the high-severity recommendation.
What should you do?

A. Add the Microsoft Antimalware extension to VM1.

B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.

C. Add the Network Watcher Agent for Windows extension to VM1.

D. Onboard VM1 to Microsoft Defender for Endpoint.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection

Community vote distribution

D (54%) A (46%)

Anarchira Highly Voted 2 years, 2 months ago

Selected Answer: D

D: Onboard VM1 to Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint provides advanced threat protection for Windows VMs in Azure, and by onboarding VM1, you can ensure that it is protected against malware and other threats. This will also help you to comply with security policies and regulations.

Option A (Add the Microsoft Antimalware extension to VM1) is incorrect because this option only adds basic antivirus protection to VM1 and may not provide the level of protection required to comply with security policies and regulations.

Option B (Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1) is also incorrect because this option is designed for on-premises System Center environments and may not be applicable to Azure VMs.

Option C (Add the Network Watcher Agent for Windows extension to VM1) is also incorrect because this option is used for network monitoring and troubleshooting and does not provide endpoint protection.

upvoted 20 times

yassou_123 Highly Voted 2 years, 6 months ago

Selected Answer: D

D should be the answer

upvoted 7 times

mmmyo Most Recent 1 month, 3 weeks ago

Selected Answer: D

EDR > Basic Antivirus protection

upvoted 1 times

cassucena 7 months ago

Selected Answer: A

Antimalware

upvoted 1 times

pentium75 11 months ago

Selected Answer: D

Though both A and D would resolve the alert, MS documentation mentions only Defender, System Center Endpoint Protection, TrendMicro, McAfee and Sophos in relation to it.

upvoted 1 times

pentium75 11 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/endpoint-protection-recommendations-technical

upvoted 1 times

JaridB 1 year, 2 months ago

Selected Answer: D

To resolve the high-severity recommendation "Install endpoint protection solutions on virtual machine" in Microsoft Defender for Cloud for your Azure virtual machine named VM1, the appropriate action is to onboard VM1 to Microsoft Defender for Endpoint. This solution aligns with Microsoft's guidance on ensuring that virtual machines have endpoint protection, particularly to address high-severity alerts related to missing endpoint protection solutions.

upvoted 1 times

mrt007 1 year, 3 months ago

The correct answer is A. Add the Microsoft Antimalware extension to VM1.

Microsoft Defender for Cloud recommends installing endpoint protection solutions on your virtual machine. The Microsoft Antimalware extension is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software. By adding this extension to VM1, you can help protect it from threats and thus resolve the high-severity recommendation.

upvoted 2 times

xRiot007 10 months, 3 weeks ago

This is old. Nowadays most of the security is under the Microsoft Defender umbrella, so D is a better answer.

upvoted 1 times

Tognan 1 year, 3 months ago

Selected Answer: D

Add the Microsoft Antimalware extension to VM1: This option might seem relevant, but Microsoft Antimalware is a legacy product replaced by Microsoft Defender for Endpoint. Onboarding to Defender for Endpoint offers a more comprehensive and up-to-date security solution.

Correct answer is D

upvoted 1 times

[Removed] 1 year, 6 months ago

Windows Defender
Defender for Cloud recommends Endpoint protection should be installed on your machines when Get-MpComputerStatus runs and the result is AMServiceEnabled: False

Defender for Cloud recommends Endpoint protection health issues should be resolved on your machines when Get-MpComputerStatus runs and any of the following occurs:

Any of the following properties are false:

AMServiceEnabled
AntispywareEnabled
RealTimeProtectionEnabled
BehaviorMonitorEnabled
IoavProtectionEnabled
OnAccessProtectionEnabled

upvoted 1 times

Obama_boy 1 year, 6 months ago

Selected Answer: D

To resolve the high-severity recommendation from Microsoft Defender for Cloud, you should **onboard VM1 to Microsoft Defender for Endpoint**. So, the correct answer is **D**. This will ensure that the virtual machine has the necessary endpoint protection, which is crucial for maintaining the security and integrity of your system. Microsoft Defender for Endpoint is a holistic, cloud-delivered endpoint security solution that includes risk-based vulnerability management and assessment, attack surface reduction, behavioral-based and cloud-powered next-generation protection, endpoint detection and response (EDR), automatic investigation and remediation, managed hunting services, rich APIs, and unified security management. It provides strong defense against a wide range of threats and sophisticated attacks, fulfilling the recommendation's requirement.

upvoted 1 times

Obama_boy 1 year, 6 months ago

Selected Answer: D

The correct answer is D. Onboard VM1 to Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint is a security platform for intelligent protection, detection, investigation, and response. It can help you to prevent, detect, and respond to advanced cyberthreats on your Azure virtual machines. To use Microsoft Defender for Endpoint, you need to onboard your virtual machines to the service.

Option A is incorrect. The Microsoft Antimalware extension is a legacy solution that provides real-time protection against viruses, spyware, and other malicious software. However, it does not integrate with Microsoft Defender for Cloud and does not provide the same level of protection as Microsoft Defender for Endpoint.

upvoted 1 times

Saadjanjua 1 year, 7 months ago

Selected Answer: D

D answer

upvoted 1 times

flafernan 1 year, 7 months ago

Selected Answer: D

Given the specific high-severity recommendation provided by Microsoft Defender for Cloud, which is "Install endpoint protection solutions on the virtual machine", the answer that best meets these security requirements is:

D. Integrate VM1 with Microsoft Defender for Endpoint.

This option provides a more comprehensive solution, including advanced protection capabilities, advanced threat detection, incident investigation, and automatic threat response. It's a choice more in line with the advanced security needs indicated by Microsoft Defender for Cloud's high severity recommendation.

upvoted 1 times

Feraso 1 year, 7 months ago

Selected Answer: A

Answer A:

It's confusing as from initial look you would go with option D, however, I have tested in the lab and the recommendation was resolved once I installed the Antimalware extension.

upvoted 2 times

tweleve 1 year, 8 months ago

In exam 13 Oct

upvoted 4 times

[Removed] 1 year, 9 months ago

It A tested in lab

upvoted 3 times

ErikPJordan 1 year, 9 months ago

Selected Answer: D

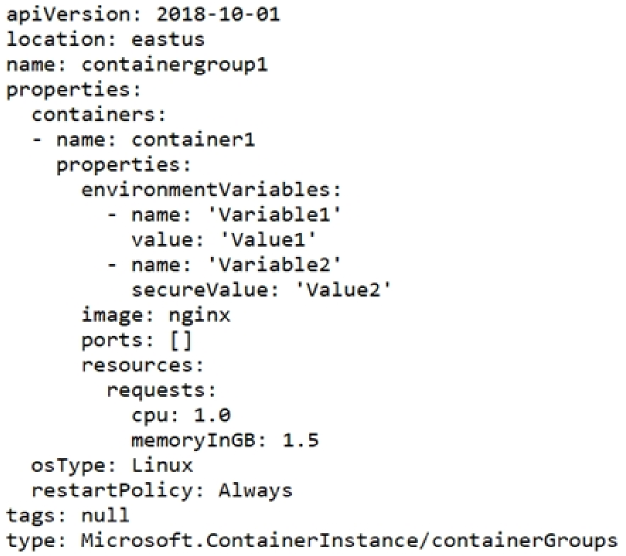
Microsoft Antimalware is not the same as end point protection

upvoted 2 times

Question #29 *Topic 3*

HOTSPOT -

You have a file named File1.yaml that contains the following contents.



```
apiVersion: 2018-10-01
location: eastus
name: containergroup1
properties:
  containers:
  - name: container1
    properties:
      environmentVariables:
        - name: 'Variable1'
          value: 'Value1'
        - name: 'Variable2'
          secureValue: 'Value2'
      image: nginx
      ports: []
      resources:
        requests:
          cpu: 1.0
          memoryInGB: 1.5
  osType: Linux
  restartPolicy: Always
tags: null
type: Microsoft.ContainerInstance/containerGroups
```

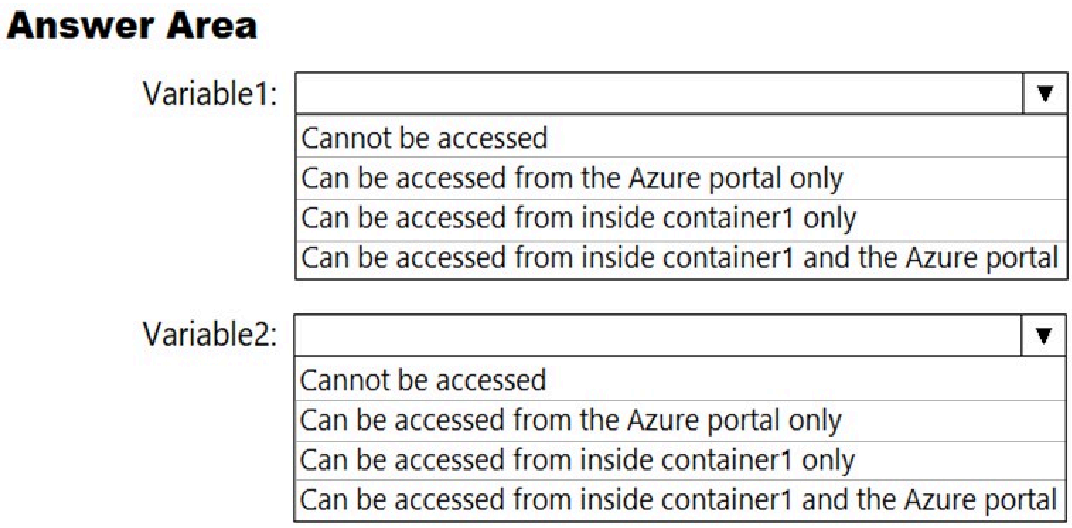
You create an Azure container instance named container1 by using File1.yaml.

You need to identify where you can access the values of Variable1 and Variable2.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

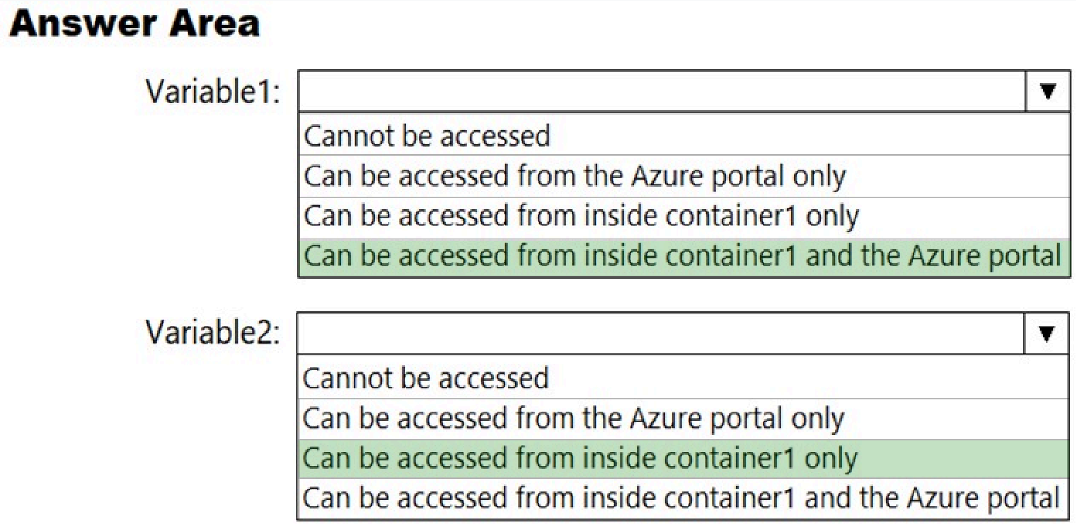
Variable1: ▼

Cannot be accessed
Can be accessed from the Azure portal only
Can be accessed from inside container1 only
Can be accessed from inside container1 and the Azure portal

Variable2: ▼

Cannot be accessed
Can be accessed from the Azure portal only
Can be accessed from inside container1 only
Can be accessed from inside container1 and the Azure portal

Suggested Answer:



Answer Area

Variable1: ▼

Cannot be accessed
Can be accessed from the Azure portal only
Can be accessed from inside container1 only
[✓ Can be accessed from inside container1 and the Azure portal]

Variable2: ▼

Cannot be accessed
Can be accessed from the Azure portal only
[✓ Can be accessed from inside container1 only]
Can be accessed from inside container1 and the Azure portal

Reference:

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables

gcpbrig01 Highly Voted 4 years, 3 months ago

correct answer;

env variable with not-secure value can be accessed in Azure portal and Azure CLI. env variable with secure value can be accessed within container only

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables#secure-values

upvoted 55 times

> **cfsxtuv33** 3 years, 2 months ago
>
> Yup...you are correct: Environment variables with secure values aren't visible in your container's properties--their values can be accessed only from within the container. For example, container properties viewed in the Azure portal or Azure CLI display only a secure variable's name, not its value."
>
> upvoted 4 times

kumax Highly Voted 4 years ago

On exam, May 2021.

upvoted 14 times

xRiot007 Most Recent 10 months, 3 weeks ago

Normal values : container and portal

Secret values : container only

upvoted 1 times

91743b3 10 months, 3 weeks ago

On exam Aug 6 2024

upvoted 3 times

majstor86 2 years, 3 months ago

Variable 1: Can be accessed from inside container1 and the Azure portal

Variable 2: Can be accessed from inside container1 only

upvoted 3 times

ligu 2 years, 4 months ago

Answers are correct

Value= access inside container and the azure portal

SecureValue= access only inside container

upvoted 2 times

jl92 3 years, 7 months ago

# IN EXAM - 19/11/2021

upvoted 4 times

Jco 3 years, 9 months ago

#exam ques # 29 Sep

upvoted 2 times

Sandomj55 3 years, 10 months ago

In Exam 8/4/2021

upvoted 3 times

Cyberbug2021 4 years, 2 months ago

Because - Secret

upvoted 2 times

> **rpm1234567** 4 years ago
>
> hi cyberbug2021,
>
> Could you please share the correct answer. because this month23 i m going right exam.
>
> Now,Is there any lab on this exam.
>
> thanks
>
> upvoted 2 times
>
> > **Jacquesvz** 3 years, 11 months ago
> >
> > Hi rpm1234567. given answers correct; see gcpbrig01's explanation.
> >
> > upvoted 2 times

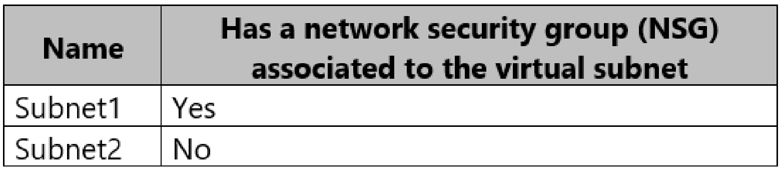
JohnYinToronto 4 years, 3 months ago

answers correct

upvoted 3 times

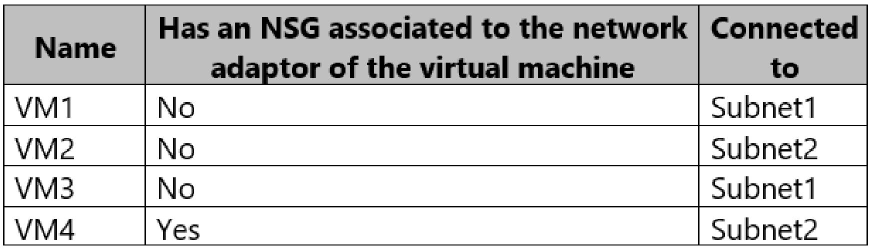
Question #30 *Topic 3*

You have an Azure subscription that contains a virtual network. The virtual network contains the subnets shown in the following table.



Name	Has a network security group (NSG) associated to the virtual subnet
Subnet1	Yes
Subnet2	No

The subscription contains the virtual machines shown in the following table.



Name	Has an NSG associated to the network adaptor of the virtual machine	Connected to
VM1	No	Subnet1
VM2	No	Subnet2
VM3	No	Subnet1
VM4	Yes	Subnet2

You enable just in time (JIT) VM access for all the virtual machines.

You need to identify which virtual machines are protected by JIT.

Which virtual machines should you identify?

A. VM4 only

B. VM1 and VM3 only

C. VM1, VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

Suggested Answer: *C*

An NSG needs to be enabled, either at the VM level or the subnet level.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

Community vote distribution

C (100%)

A365 Highly Voted 4 years, 3 months ago

answer is correct: The service will detect where the temporary exceptions need to be created and act accordingly. The only requirement is that there IS an NSG either on the vmNIC or the subnet to which the required exceptions can be added as required. If there is no NSG then a warning is surfaced via Azure Security Center.

https://www.itprotoday.com/iaaspaas/faqs-closer-look-requirements-and-functions-just-time-vm-access-azure

upvoted 41 times

dadageer Highly Voted 4 years, 3 months ago

correct answer

upvoted 9 times

Jimmy500 Most Recent 1 year ago

Answer is correct , please note that besides NSG , firewall can also come to this question. Either NSG or Azure Firewall integrated can be protected by JIT

upvoted 2 times

yonie 1 year, 6 months ago

Selected Answer: C

VMs that don't support JIT because:

Missing network security group (NSG)

https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage#work-with-jit-vm-access-using-microsoft-defender-for-cloud

upvoted 2 times

Obama_boy 1 year, 6 months ago

Selected Answer: C

because these VMs have NSGs protecting them

upvoted 1 times

ESAJRR 1 year, 10 months ago

Selected Answer: C

C. VM1, VM3 and VM4 only

upvoted 1 times

majstor86 2 years, 3 months ago

Selected Answer: C

VM1, VM3 and VM4 only

upvoted 2 times

ligu 2 years, 4 months ago

Answer is correct. JIT works only when NSW associated at subnet or VM

upvoted 1 times

NinjaSchoolProfessor 2 years, 11 months ago

Selected Answer: C

In exam 15-July-2022

upvoted 5 times

NinjaSchoolProfessor 2 years, 11 months ago

In exam 15-July-2022

upvoted 5 times

Alessandro365 3 years ago

Selected Answer: C

C is correct answer.

upvoted 2 times

salmantarik 3 years ago

Answer is correct. JIT works only when NSW associated at subnet or VM

upvoted 3 times

ishin999 3 years, 5 months ago

answer is correct...NSG at either the subnet or VM interface level

upvoted 3 times

HananS 3 years, 6 months ago

The answer is correct

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets or individual network interfaces (NIC) attached to VMs.

upvoted 1 times

mhzayt 3 years, 7 months ago

To get JIT working you need an NSG either on the subnet level or VM. VM1, VM2, and VM3 have an NSG on the subnet level. VM4 has an NSG on the NIC, so JIT is also working for VM4? What do I see wrong here?

upvoted 2 times

palantony 3 years, 7 months ago

VM1 & VM3 has NSG @ subnet level (Subnet1)

VM4 has NSG @ VM

VM2 which is connected to Subnet2 doesn't have NSG at Subnet level neither on VM

upvoted 10 times

Scryptre 3 years, 7 months ago

Correct!

upvoted 1 times

Cyberbug2021 4 years, 2 months ago

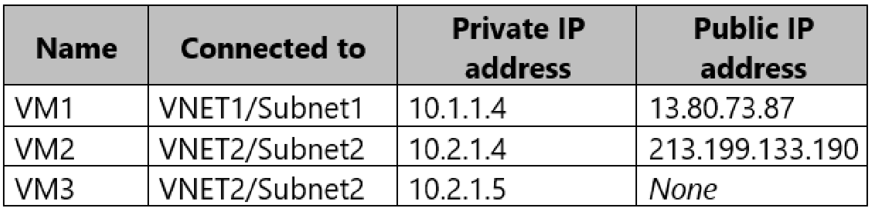
A NSG required for JIT

upvoted 5 times

Question #31 Topic 3

HOTSPOT -

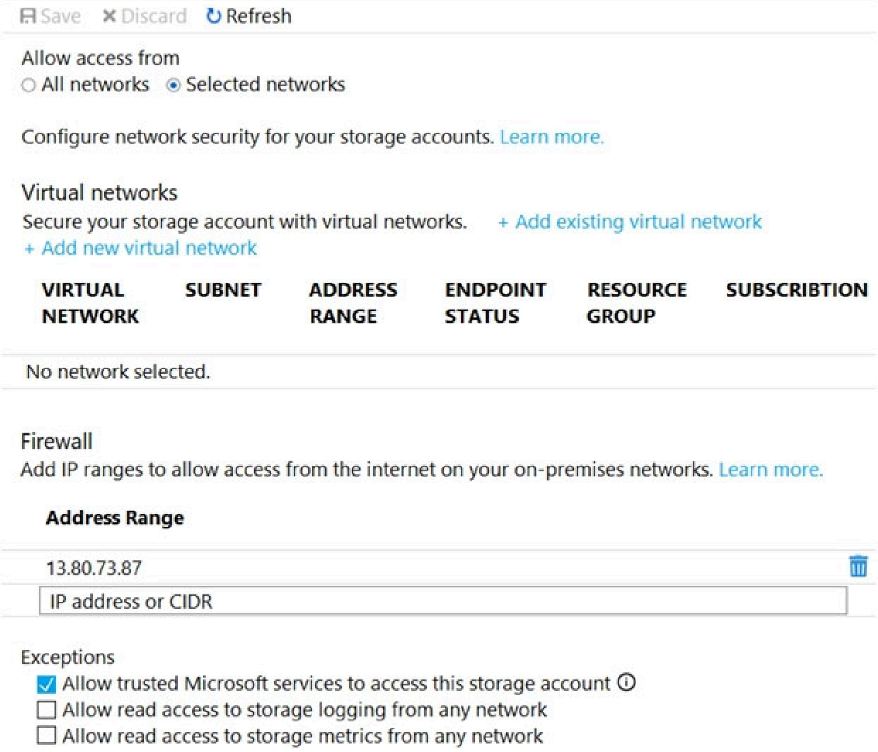
You have an Azure subscription that contains the virtual machines shown in the following table.



Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	*None*

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.



Allow access from
○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more.

Virtual networks
Secure your storage account with virtual networks. + Add existing virtual network
+ Add new virtual network

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIBTION
No network selected.					

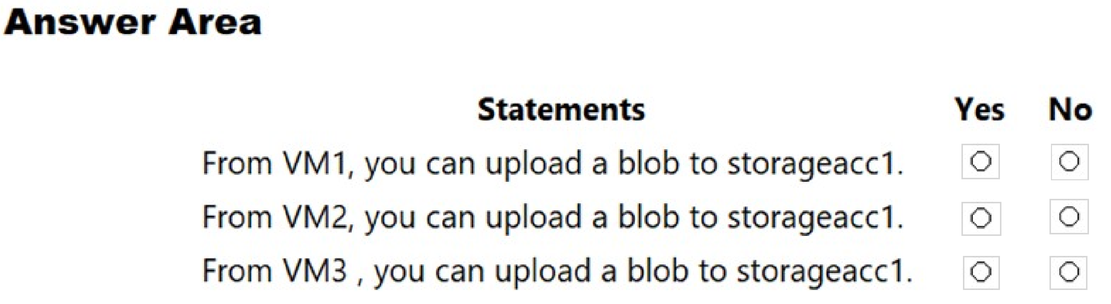
Firewall
Add IP ranges to allow access from the internet on your on-premises networks. Learn more.

Address Range
13.80.73.87
IP address or CIDR

Exceptions
☑ Allow trusted Microsoft services to access this storage account
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

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

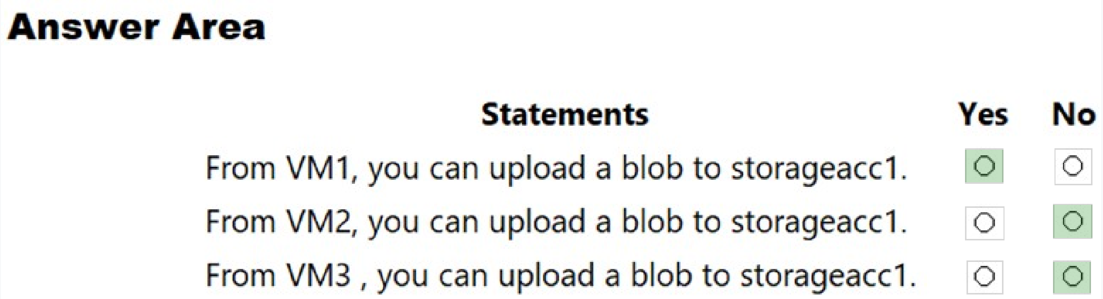
Hot Area:



Answer Area

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	[✓ ○]	○
From VM2, you can upload a blob to storageacc1.	○	[✓ ○]
From VM3 , you can upload a blob to storageacc1.	○	[✓ ○]

Box 1: Yes -

The public IP of VM1 is allowed through the firewall.

Box 2: No -

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No -
The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.
Reference:
https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security

sukhdeep Highly Voted 👍 4 years, 3 months ago
Given answer is correct because they did not select any private network for storage access and VM1 has access via Public IP address.
upvoted 62 times

kimalto452 4 years ago
NO, NO , NO
With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch. Please ensure Azure service firewall rules allow for this switch before setting up service endpoints. You may also experience temporary interruption to service traffic from this subnet while configuring service endpoints.
upvoted 41 times

akp1000 3 years, 8 months ago
Wrong. The question is about service endpoints and not private endpoints
upvoted 9 times

mansc3wth1s 3 years, 4 months ago
"Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet."

IF they were all in the same subnet. Then they all would be y,y,y buuuuut the answer is Y,N,N. Give answer in this question is correct. It's OLD question so be wary if you're new. It may be changed.
upvoted 7 times

mansc3wth1s 3 years, 4 months ago
I CANT EDIT! I MEANT TO SAY IF ON THE SAME VNET! IF THEYRE ON THE SAME VNET.
upvoted 3 times

vj77 3 years, 10 months ago
"Please ensure Azure service firewall rules allow for this switch"; is this condition not met by the firewall rule shown? and so that way the connection should still work?
upvoted 1 times

rawrkadia 3 years, 9 months ago
No, because of the service endpoints on both subnet. They just explained why it doesn't work.
upvoted 2 times

ChinkSantana 4 years ago
Correct. NO, NO, NO
upvoted 12 times

Hot_156 3 months, 2 weeks ago
I DID LAB THIS!!!!

Y - PaaS service and Network/FW configurations work differently then IaaS. If you set a VM to allow specific access within the subnet or no access, any other VM won't be able to access but with PaaS services like service enpoint, it is not the case.
N
N
upvoted 1 times

hang10z Highly Voted 👍 4 years, 3 months ago
In this case the answer would be NO NO NO since service endpoints are configured on the Subnets so traffic between the VM and the storage account is all internal (using private ip not public) Trusted Microsoft Services does not include Virtual Machines. Tricky question!
upvoted 34 times

sureshatt 4 years, 3 months ago

agree with your answer. Its NO, NO, NO. Enabling service endpoints turns all requests to use private IP address.

"Today, Azure service traffic from a virtual network uses public IP addresses as source IP addresses. With service endpoints, service traffic switches to use virtual network private addresses as the source IP addresses when accessing the Azure service from a virtual network."

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#secure-azure-services-to-virtual-networks

upvoted 11 times

schpeter_091 Most Recent 7 months, 1 week ago

Y-N-N

When I use service endpoints, it means that i restrict specific subnets inside the VNET to connect to that storage account. (only the selected ones are allowed) I can add a firewall rule, as the VM's public IP to connect to that storage account. Public IP can co-exist with service endpoints.

upvoted 1 times

pentium75 11 months ago

NO,NO,NO

"With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch."

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 1 times

saira23 11 months, 1 week ago

In the exam 19/07/2024

upvoted 2 times

epomatti 1 year, 6 months ago

NO, NO, NO

Tested and confirmed. I'm afraid the given answer in incorrect.

"With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch. Please ensure Azure service firewall rules allow for this switch before setting up service endpoints. You may also experience temporary interruption to service traffic from this subnet while configuring service endpoints."

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 3 times

[Removed] 1 year, 6 months ago

Tested in the lab 1st is Y as when I don't have the Public IP address of the VM i get the following error
This request is not authorized to perform this operation. RequestId:ac49ad4f-701e-0010-31e0-3110d0000000 Time:2023-12-18T18:33:32.0303933Z
This storage account's 'Firewalls and virtual networks' settings may be blocking access to storage services. Try adding your client IP address
When I add the IP address it starts working

upvoted 3 times

morito 1 year, 6 months ago

After reviewing the current configuration setup, I believe the answer is indeed Y,N,N. Ticking "Allow Azure Services on the trusted services list to access this storage account" does not create service endpoints, but allows Azure Services like Azure Backup to access the storage account. A private endpoint that would link directly into the vnet is not configured, hence no service endpoint connection gets established.

Check this link: https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#trusted-access-for-resources-registered-in-your-subscription to see what counts as a trusted azure service.

upvoted 1 times

pentium75 11 months ago

"Ticking 'Allow Azure Services on the trusted services list to access this storage account' does not create service endpoints" - Yes, but the question specifically says that "Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured."

upvoted 1 times

bob_sez 1 year, 7 months ago

From my research on this: https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#manage-exceptions

By design, access to a storage account from trusted services takes the highest precedence over other network access restrictions.
That said, Compute is not part of the trusted services that are allowed to access storage account based on that setting.

Yes, with a virtual network with service endpoints the communication is over private IP, but those have to be listed in the exception. So, No for all from me.

upvoted 2 times

wardy1983 1 year, 8 months ago

Box 1: Yes -
The public IP of VM1 is allowed through the firewall.
Box 2: No -
The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of
VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.
Box 3: No -
The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a
public IP address so it cannot access storageacc1 over the Internet.

upvoted 5 times

JunetGoyal 1 year, 8 months ago

Y,N,N
Just want to talk about First one other 2 all are okey with N.
Just think even service end point is enable not allowed, still public Ip is allowed. VM1 will behave like any laptop in this case outside of azure.
Definitely you cannot use PRivate Ip, but public Ip will make it work for Blob

upvoted 1 times

JunetGoyal 1 year, 8 months ago

Also Service End point allow backbone Network to communicate through private Ip, does not mean It will block public ip access

upvoted 1 times

InnoMaf 1 year, 9 months ago

The correct answer is No, No, No. By enable service endpoint, the source IP for the VM becomes the private IP space from its VNET and not the public IP. The storage account the allows access of the allowed subnet.
Ref https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 1 times

ESAJRR 1 year, 10 months ago

YES
NO
NO

upvoted 2 times

majstor86 2 years, 3 months ago

YES
NO
NO

upvoted 7 times

ligu 2 years, 4 months ago

Answers are correct

upvoted 1 times

fonte 2 years, 6 months ago

Replicated the scenario in lab and got No, No, No.

"This request is not authorized to perform this operation.

This storage account's 'Firewalls & virtual networks' settings may be blocking access to storage services. Try adding your client IP address to the firewall exceptions, or by allowing access from 'all networks' instead of 'selected networks'. "

For #1 I then tested adding the private subnet and I was then able to access the storage. Removed the subnet and was blocked again.

Definite answer: No, No, No.

upvoted 9 times

⊟ 👤 **JohnBentass** 2 years, 6 months ago

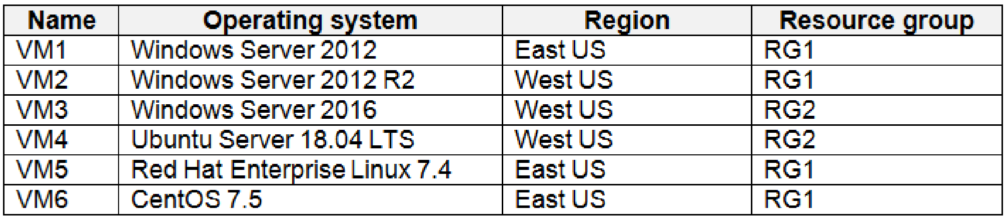
yes,no,no

upvoted 1 times

Question #32 *Topic 3*

HOTSPOT -

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.



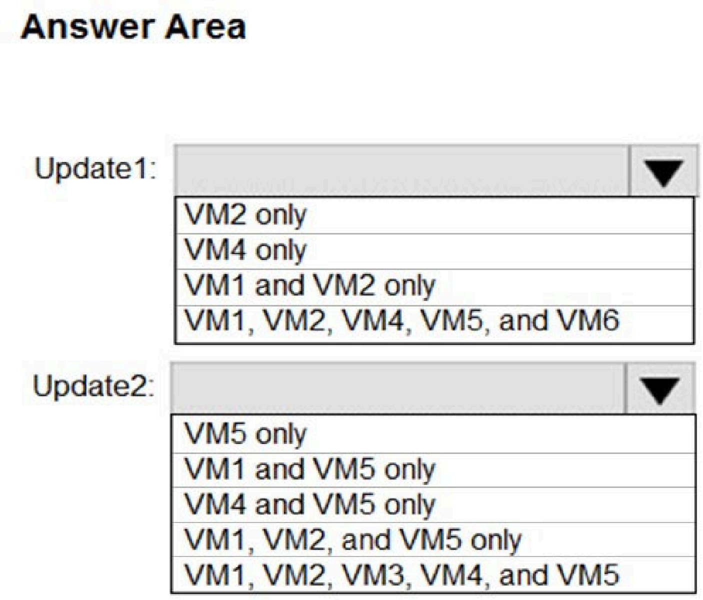
Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

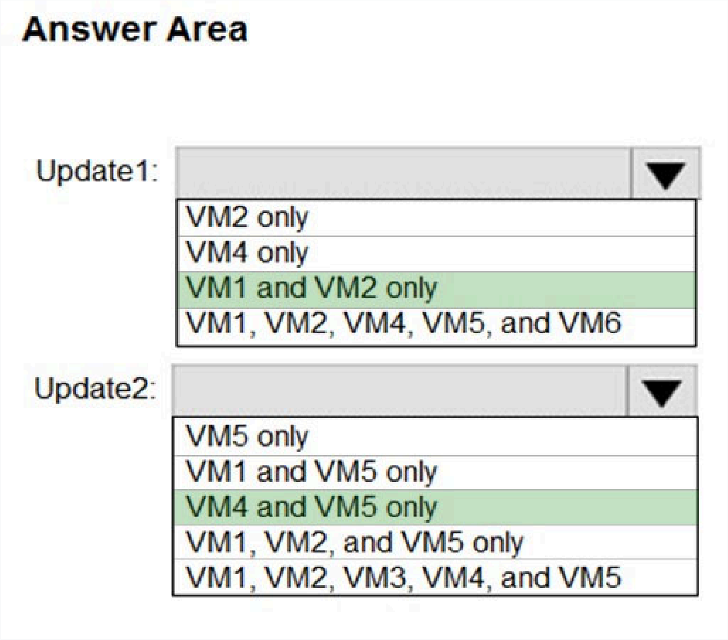


Answer Area

Update1:
- VM2 only
- VM4 only
- VM1 and VM2 only
- VM1, VM2, VM4, VM5, and VM6

Update2:
- VM5 only
- VM1 and VM5 only
- VM4 and VM5 only
- VM1, VM2, and VM5 only
- VM1, VM2, VM3, VM4, and VM5

Suggested Answer:



Answer Area

Update1:
- VM2 only
- VM4 only
- [✓ VM1 and VM2 only]
- VM1, VM2, VM4, VM5, and VM6

Update2:
- VM5 only
- VM1 and VM5 only
- [✓ VM4 and VM5 only]
- VM1, VM2, and VM5 only
- VM1, VM2, VM3, VM4, and VM5

An update deployment can apply to Windows VMs or Linux VMs but not both. The VMs can be in different regions, different subscriptions and different resource groups.

Update1: VM1 and VM2 only -

VM3: Windows Server 2016.

Update2: VM4 and VM5 only -

VM6: CentOS 7.5.

For Linux, the machine must have access to an update repository. The update repository can be private or public.

Reference:

https://docs.microsoft.com/en-us/azure/automation/update-management/overview

azurearch Highly Voted 👍 4 years, 10 months ago

Its based on OS, only windows machines can be added to windows update management group and same applies to linux. the answer is right.

upvoted 89 times

Rave763 Highly Voted 👍 4 years, 8 months ago

Answer is Correct. You can add machines to the update management irrespective of the region and resource group provided they are of same OS time. i think region agnostic is a recent feature

upvoted 20 times

gboyega 4 years, 5 months ago

Correct. Answer is correct

upvoted 10 times

cris_exam Most Recent ⏱ 11 months, 1 week ago

Answers are correct. wardy1983 explained well.

Also, not all OS versions are supported so, here's a link with a list of the supported OS builds.

https://learn.microsoft.com/en-us/azure/virtual-machines/automatic-vm-guest-patching#supported-os-images

upvoted 1 times

wardy1983 1 year, 1 month ago

Explanation:

An update deployment can apply to Windows VMs or Linux VMs but not both. The VMs can be in different regions, different subscriptions and different resource groups.

Update1: VM1 and VM2 only -

VM3: Windows Server 2016.

Update2: VM4 and VM5 only -

VM6: CentOS 7.5.

For Linux, the machine must have access to an update repository. The update repository can be private or public.

Reference:

https://docs.microsoft.com/en-us/azure/automation/update-management/overview

upvoted 5 times

BayaliJihad 1 year, 8 months ago

This is outdated. Now in Azure update management center, you can create maintenance configurations, and it's not OS based, you can add in the same maintenance configuration linux and windows machines

upvoted 6 times

majstor86 1 year, 10 months ago

Update 1: VM1 and VM2 only

Update 2: VM4 and VM5 only

upvoted 2 times

ligu 1 year, 10 months ago

The answers are correct. Updates management on the same OS

upvoted 1 times

Sweet_co 2 years, 5 months ago

In exam: 20-7-2022

upvoted 6 times

NinjaSchoolProfessor 2 years, 5 months ago

In exam 15-July-2022

upvoted 4 times

SecurityAnalyst 3 years, 4 months ago

# IN EXAM - 31/8/2021

upvoted 5 times

Socgen1 3 years, 4 months ago

In exam on 31/08/2021

upvoted 3 times

Deepmindx 3 years, 6 months ago

### IN EXAM ### 29/6/2021

upvoted 10 times

kumax 3 years, 6 months ago

On exam, May 2021.

upvoted 6 times

Cisna 3 years, 7 months ago

in exam 02/05/2021

upvoted 7 times

> **rpm1234567** 3 years, 6 months ago
>
> Hi Cisna,
>
> Can you confirm the correct answer .
>
> upvoted 1 times

milind8451 3 years, 10 months ago

Given answer is correct. Tested in lab, When you create Deployment Schedule in Azure Automation, it asks for "Operating System" which shows that both OS (Win and Linux) can not be selected in one schedule.

upvoted 4 times

milad123 3 years, 10 months ago

correct

upvoted 2 times

JeanTremblay 3 years, 11 months ago

This is a question for the az-104 not the az-500 !!

upvoted 3 times

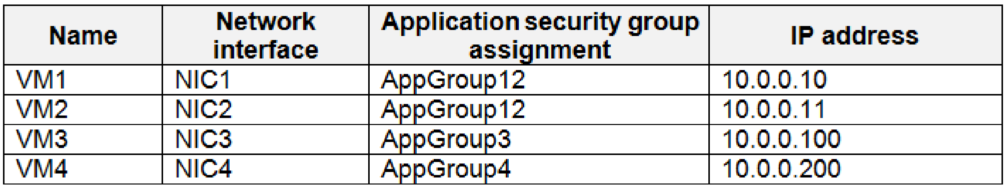
> **KaiserdomTW** 3 years, 6 months ago
>
> Also seen on az - 304
>
> upvoted 2 times

Question #33 *Topic 3*

HOTSPOT -

You have an Azure subscription named Sub1.

You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.



Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

Currently, you have not provisioned any network security groups (NSGs).

You need to implement network security to meet the following requirements:

✑ Allow traffic to VM4 from VM3 only.

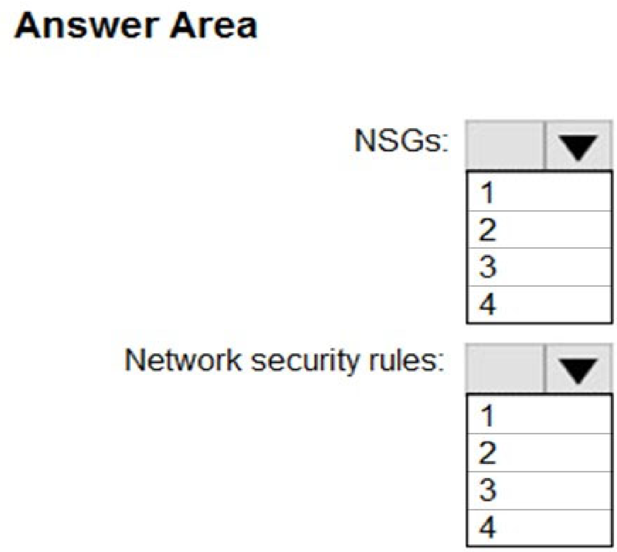
✑ Allow traffic from the Internet to VM1 and VM2 only.

✑ Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

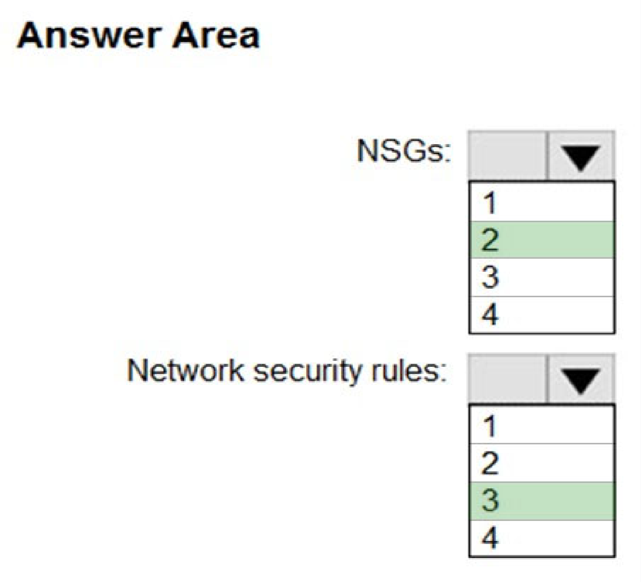


Answer Area

NSGs: ▼
1
2
3
4

Network security rules: ▼
1
2
3
4

Suggested Answer:



Answer Area

NSGs: ▼
1
2
3
4

Network security rules: ▼
1
2
3
4

NSGs: 2 -

Network security rules: 3 -

Not 2: You cannot specify multiple service tags or application groups) in a security rule.

References:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

Oz Highly Voted 5 years, 6 months ago

Sorry, I have to re-post.
Correct answer is this.
1) You can only assign 1 NSG to a subnet, and there is only one subnet in the description. So Box 1 is 1
2) Number of rules in NSG can be any, they are processed in sequence.
Rule 1: You can have AppGroup3 as the source and AppGroup4 as destination in one rule then allow traffic.
Rule 2: You can have Service Tag "Internet" as a source and AppGroup12 as the destination. then allow traffic.
Rule 3: YOu can have source as the subnet range and destination as subnet range then deny all traffic, so only above rules will be allowing traffic.

SO Box 2 is 3.

You still have 3 default rules that allow traffic from VNET, LoadBalancer and deny all other inbound traffic.

upvoted 158 times

azurearch 5 years, 4 months ago

there is no requirement to allow traffic from one appgroup to another, question is just to allow traffic from internet to vm1 and 2.

upvoted 4 times

rgullini 4 years, 1 month ago

This is correct.

upvoted 2 times

abrahamtek 4 years ago

@oz The question doesn't enforce that NSG should be applied to Subnets Only. Therefor Applying the NSG to NIC seems the correct solution

upvoted 1 times

Roy_Batty 4 years, 10 months ago

In agreement that it's possible with 1 NSG and 3 rules, but given the "Tip" in one of the articles people are linking to, would it be better practice to create a separate NSG for the NIC-specific rules, and keep the Subnet-wide NSG to the rule for Internet->ASG?

Does anyone know where the listed answer came from? I'm wondering how hard I should try to 'justify' it, or figure out why it's right (assuming it reflects the actual test answer) or should I go with the answer we've figured out as technically correct if I encounter it on the test?

upvoted 3 times

Oz Highly Voted 5 years, 6 months ago

Correct answer is this.
1) You can only assign 1 NSG to a subnet, and there is only one subnet in the description. So Box 1 is 1
2) You can have AppGroup3 as the source and AppGroup4 as destination in one rule then deny traffic. That's one rule.
You can have Internet tag as a source and AppGroup12 as the destination. That's rule 2.
SO Box 2 is 2 .

upvoted 46 times

gills 4 years, 8 months ago

This is in correct. The communication control between two VMs within the subnet, cannot controlled by a NSG at the subnet level. So there is going to be an NSG assigned to to a NIC. The control of traffic between internet and VM can be controlled by a NSG at the subnet. So there is two NSG for sure!

upvoted 11 times

Arejay 4 years, 4 months ago

Not right - if you put a inbound Deny All rule, it will impact the communication between the VMs in the same subnet. Tested and verified.

upvoted 2 times

Lrrr_FromOmicronPersei8 3 years, 6 months ago

Yes, it can be, refer to https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic, "It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VM's within it."

upvoted 4 times

Hot_156 Most Recent 4 months ago

This is also an option.

NSGs: 2
Network Security Rules: 3

1. NSG1 (Associated with NIC1 and NIC2):
Rule 1:
Source: Internet
Destination: AppGroup12
Action: Allow
(Other settings as appropriate for your desired ports/protocols)

2. NSG2 (Associated with the Subnet):
Rule 2:
Source: AppGroup3
Destination: AppGroup4
Action: Allow
(Other settings as appropriate)
Rule 3:
Source: Any
Destination: Any
Action: Deny
upvoted 1 times

⊟ **Hot_156** 4 months ago
They are in the same Subnet BUT with regular VMs, any NSG within the subnet will evaluate the traffic in the subnet. With endpoints, traffic si routed directly to the endpoint bypassing an NSG in the same subnet
upvoted 1 times

⊟ **pentium75** 11 months ago
I think it is 1 and 3.

First of all, question is 'how many NSGs and rules should you CREATE', so the default rules are excluded from the count.

Minimize number of NSGs:
All NICs are in same VNet, so create 1 NSG for the VNet

Minimize number of rules:
Default allows traffic within the VNet, so to 'allow traffic to VM4 from VM3 only' we need two new rules:
1) allow traffic to VM4 from VM3
2) deny other traffic to VM4
Inbound traffic is denied by default, so for "Allow traffic from the Internet to VM1 and VM2 only" we need only 1 rule:
3) allow traffic to VM1 and VM2 (or AppGroup12) from Internet
upvoted 1 times

⊟ **LZNJ** 1 year, 3 months ago
I think the given answers are correct.
You need 2 NSGs. One for the subnet, one for VM4.
Allow traffic to VM4 only from VM3, this means you need to block all other traffics, even those within the VNET. You cannot have this rule in the subnet NSG, because then you will have to add many other rules to allow other intra-vnet traffic. So it is better to add this deny all traffic rule in the VM4's NSG.

You need 3 rules: (1) allow internet traffic to AppGroup12, in the subnet NSG.
(2) in the VM4 NSG, deny all inbound traffic;
(3) allow traffic from VM3.
upvoted 3 times

⊟ **wardy1983** 1 year, 7 months ago
) You can only assign 1 NSG to a subnet, and there is only one subnet in the description. So Box 1 is 1
2) Number of rules in NSG can be any, they are processed in sequence.

Rule 1: You can have AppGroup3 as the source and AppGroup4 as destination in one rule then allow traffic.
Rule 2: You can have Service Tag "Internet" as a source and AppGroup12 as the destination. then allow traffic.
Rule 3: YOu can have source as the subnet range and destination as subnet range then deny all traffic, so only above rules will be allowing traffic.
Box 2 is 3.
You still have 3 default rules that allow traffic from VNET, LoadBalancer and deny all other inbound traffic.
References:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview
upvoted 3 times

Feraso 1 year, 7 months ago
NSG: 1
Rules: 3

NSG: You can only assign 1 NSG to a subnet, and there is only one subnet in the description.

Rules:
- The first rule (inbound) is to allow traffic initiated from the internet to ASG12.

All traffic initiated from the internet is blocked by default, so in this case, we need to allow it to VM1 and VM2, which are grouped together in ASG12.

- The second rule is to allow traffic initiated from VM3 to VM4.

- The third rule would be to deny all the connections as we have a default rule "AllowVNetInBound" which will allow the access between the VMs. Create one similar to the default one but with action "deny".
upvoted 2 times

TheProfessor 1 year, 9 months ago
In my opinion, there is one NSG and 1 Security Rule.

You need to implement network security to meet the following requirements:

✑ Allow traffic to VM4 from VM3 only.
// By default traffic is enabled within the subnet and all of the VMs are under same subnet. So we don't need to create additional rule.

✑ Allow traffic from the Internet to VM1 and VM2 only.
// Service Tag: Source Internet and destination the ASG group.

✑ Minimize the number of NSGs and network security rules.
There are default deny rules for inbound and outbound traffic.

We could create additional rule to deny traffic within the subnet, but that was not asked, importantly, asked to minimize the rules.
upvoted 1 times

pentium75 11 months ago
"Allow traffic to VM4 from VM3 ONLY". By default, "traffic to VM4" is allowed from all VMs.
upvoted 1 times

Softeng 1 year, 9 months ago
The key word here is 'only'. They are asking you to limit the traffic on those conditions. By default there is a rule that allows all traffic from the VNET, so you must deny it in order to achieve the goal.
upvoted 1 times

heatfan900 1 year, 10 months ago
THE QUESTION CLEARLY STATES HOW MANY YOU NEED TO CREATE. 1 AND 3 IS THE ANSWER.

1 NSG / 3 Rules

1 NSG attached to the subnet1
----
1 Rule for TAG (Internet) as source and ASG12 as dest

1 Rule for VM3 to VM4

1 Rule to DENY all other traffic within Subnet1 as the default deny rules are only there to stop un-stateful traffic from outside the vnet. Without this deny rule all VMs will be able to speak to one another which clearly goes against what the question is asking.

upvoted 5 times

⊟ **JunetGoyal** 1 year, 8 months ago

Agreed!

upvoted 1 times

⊟ **heatfan900** 1 year, 11 months ago

ASG-NSG RULE SETUP EXPLANATION:

-ONE NSG ASSIGNED TO THE ONE VNET.

-TWO RULES ASSIGNED TO THE ONE NSG AGAINST THE ASGs.
>THE FIRST RULE (INBOUND) IS TO ALLOW TRAFFIC INITIATED FROM INTERNET TO ASG12.
>ALL TRAFFIC INITATED FROM THE INTERNET IS BLOCKED BY DEFAULT SO IN
THIS CASE WE NEED TO ALLOW IT TO VM1 AND VM2 WHICH ARE GROUPED
TOGETHER IN ASG12.

>THE SECOND RULE IS TO DENY TRAFFIC INTIATED BY ASG12 TO VM 4.
>THIS WOULD DENY VM1 AND VM2, AGAIN, GROUPED TOGETHER IN ASG12 TO
COMMUNICATE WITH VM4.

-THE PREMISE OF THE QUESTION IS TO TEST YOUR ABILITIES IN USING ASGs EFFICIENTLY
ONE WAY OR THE OTHER.

-NOTE, RULES ARE APPLIED BASED ON PRIORITY AND AN OBJECT THAT DOES MATCH RULE SIMPLY
MOVES ON TO THE NEXT RULE. IF NO RULE APPLIES THE OBJECT WILL EVENTUALLY MATCH THE
DENY OR ALLOW ALL RULE AT THE BOTTOM OF THE LIST WITH THE LOWEST PRIORITY.

upvoted 2 times

⊟ **majstor86** 2 years, 3 months ago

NSGs: 1

Network Security Rules: 3

upvoted 1 times

⊟ **ranbhule** 2 years, 6 months ago

Answer should be 1 & 2

https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

upvoted 4 times

⊟ **junkm** 2 years, 6 months ago

1 NSG for the subnet

3 rules (one from ASG3 to ASG4 / one from tag:Internet to ASG12 / one for deny any to any)

upvoted 6 times

⊟ **mung** 2 years, 7 months ago

The point is “how many rules should you create” not “how many rules should be in NSG”.

So to allow traffic to VM4 from VM3 only we need to create an inbound rule from VM4 to allow VM3 traffic.
And another rule to allow traffic from internet to the VM1 and VM2.

So the answer have to be 1 NSG and 2 rules.

Again, it is asking you how many rules you must create, so you do not count the default rule that you did not created.

upvoted 5 times

⊟ **mung** 2 years, 7 months ago

VM3 and VM4 are in the same subnet so they can communicate by default. However, NSG blcok all incoming traffic from the internet by defualt so we need to create a rule to allow the access from the internet.

So we only need one rule i guess..?

upvoted 1 times

⊟ **Muaamar_Alsayyad** 2 years, 8 months ago

1 NSG

3 Rules

upvoted 1 times

Question #34 Topic 3

HOTSPOT -

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:

✑ Provide a user named User1 with the ability to set advanced access policies for the key vault.

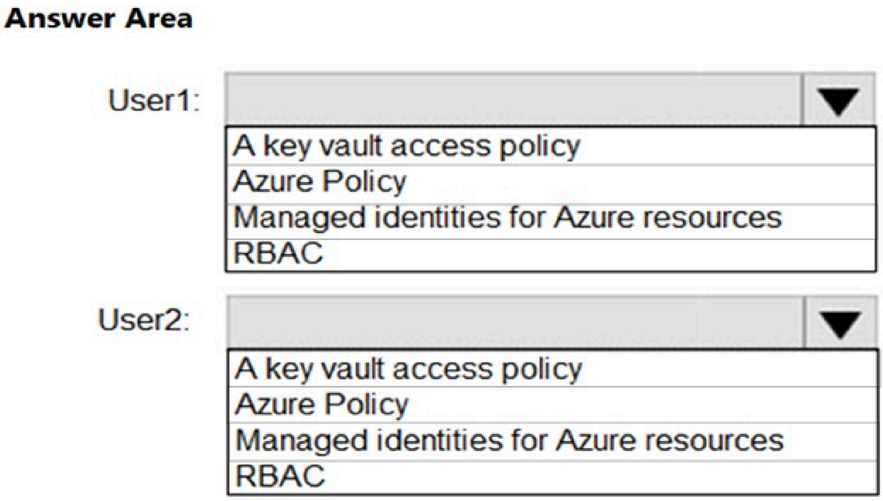
✑ Provide a user named User2 with the ability to add and delete certificates in the key vault.

✑ Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

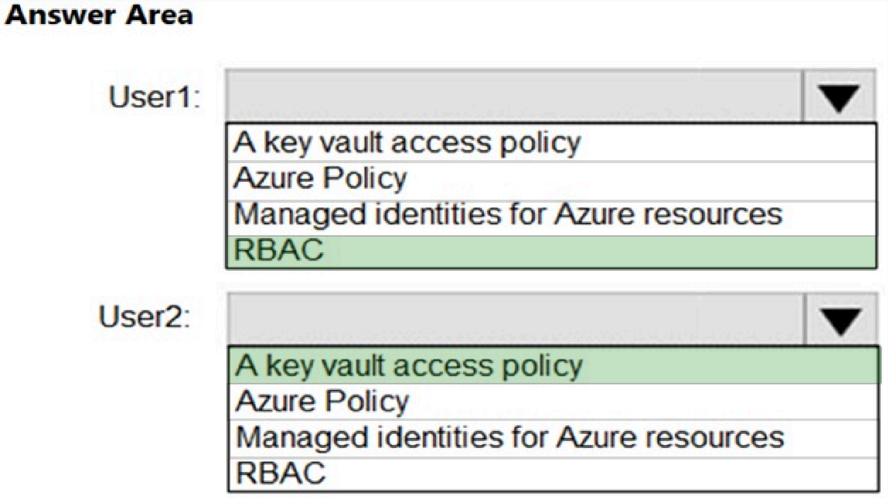


Answer Area

User1:
- A key vault access policy
- Azure Policy
- Managed identities for Azure resources
- RBAC

User2:
- A key vault access policy
- Azure Policy
- Managed identities for Azure resources
- RBAC

Suggested Answer:



Answer Area

User1:
- A key vault access policy
- Azure Policy
- Managed identities for Azure resources
- [✓ RBAC]

User2:
- [✓ A key vault access policy]
- Azure Policy
- Managed identities for Azure resources
- RBAC

User1: RBAC -

RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:

✑ set Key Vault access policies

✑ create, read, update, and delete key vaults

✑ set Key Vault tags

Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

User2: A key vault access policy

A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.

References:

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

⊟ **BayaliJihad** Highly Voted 1 year, 8 months ago

I think this is outdated. Because now you can use RBAC also to handle data plane.

upvoted 22 times

⊟ **JBAnalyst** 5 months, 4 weeks ago

principle of least privilege , RBAC will give more, access policy is granular

upvoted 1 times

francis6170 Highly Voted 3 years, 3 months ago

Got this in the AZ-500 exam (Sept 2021)! A: RBAC, KV access policy

upvoted 19 times

joegie00698 Most Recent 11 months, 3 weeks ago

best practice would be to use RBAC for both management and data plane but depends on the age of the question...so better follow the current one

upvoted 3 times

ESAJRR 1 year, 4 months ago

User1: RBAC

User2: A key vault access policy

upvoted 2 times

Self_Study 1 year, 4 months ago

on exam 7/8/23, I went with the provided answers. Who knows if answers are updated on the MS side.

upvoted 4 times

majstor86 1 year, 10 months ago

User1: RBAC

User2: A key vault access policy

upvoted 4 times

ligu 1 year, 10 months ago

Answers are correct

upvoted 2 times

RocksT 1 year, 10 months ago

RBAC can be used for key vault data plane operations such as certificate management now. Answer should be RBAC for both.

https://learn.microsoft.com/en-us/azure/key-vault/general/security-features

upvoted 4 times

ConanBarb 1 year, 9 months ago

Agree! Actually it is the recommended way (always RBAC over access policies if you can)

upvoted 1 times

ltjones12 1 year, 11 months ago

a source of confusion because I think the recommendation now is to use RBAC for all keyvault access, but I can't seem to find anything definitive

upvoted 2 times

OrangeSG 1 year, 11 months ago

Azure Key Vault access policies can have least privilege assigned for the requirement of “to add and delete certificates in the key vault”.

Please refer to Azure Key Vault access policies assignment UI:

https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal

upvoted 2 times

koreshio 2 years, 2 months ago

hang on, you can use either RBAC or vault access policy when creating the Key vault. But not both.

So if using RBAC, you can't use vault access policy again? right?

ref: https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli#enable-azure-rbac-permissions-on-key-vault

upvoted 5 times

OrangeSG 1 year, 11 months ago

User1 is at management plane; user 2 is at data plane. So they can choose authentication method independantly.

upvoted 1 times

snake_alejo 2 years, 10 months ago

answer is OK

upvoted 3 times

jl92 3 years, 1 month ago

# IN EXAM - 19/11/2021

upvoted 4 times

zioggs 3 years, 1 month ago

Exam - 4/11/21

upvoted 3 times

itbrpl 3 years, 2 months ago

Today 20/10/21...

upvoted 2 times

Jco 3 years, 3 months ago

#exam ques # 29 Sep

upvoted 2 times

JaiSharma 3 years, 3 months ago

In exam today: 27th Sep 2021

upvoted 2 times

Villar 3 years, 3 months ago

RBAC can also be used to grant data plane access by using a Key Vault access policy https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#privileged-access

upvoted 1 times

Question #35 *Topic 3*

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. device compliance policies in Microsoft Intune

B. Azure Automation State Configuration

C. application security groups

D. Azure Advisor

Suggested Answer: *B*
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines. Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on- premises.

Community vote distribution
B (100%)

besha Highly Voted 3 years ago
This question definitely will be in the exam! 4th time here
upvoted 37 times

Anonymousse 1 year, 7 months ago
:-)
:-)
upvoted 2 times

gfhbox0083 Highly Voted 4 years ago
B, for sure.
Same as Topic2 Q2.
The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service
upvoted 21 times

ESAJRR Most Recent 10 months ago
Selected Answer: B
B. Azure Automation State Configuration
upvoted 1 times

majstor86 1 year, 3 months ago
Selected Answer: B
B. Azure Automation State Configuration
upvoted 2 times

F117A_Stealth 1 year, 7 months ago
Selected Answer: B
B. Azure Automation State Configuration
upvoted 1 times

Cloudkrew 1 year, 9 months ago
This is like the 8th time i'm seeing this question.
upvoted 7 times

Alessandro365 2 years ago
Selected Answer: B
B is correct answer.
upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

kimalto452 3 years ago

same question wtff

upvoted 1 times

Rupain 3 years ago

4th time repeating

upvoted 1 times

cmong2005 3 years, 1 month ago

repeated question

upvoted 1 times

zic04 3 years, 5 months ago

Correct

upvoted 4 times

kristiann21 4 years ago

correct answer

upvoted 5 times

ogbeufi1 4 years, 1 month ago

Correct

upvoted 4 times

Question #36 Topic 3

You have an Azure Container Registry named Registry1.
From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.
You perform the following actions:
✑ Push a Windows image named Image1 to Registry1.
✑ Push a Linux image named Image2 to Registry1.
✑ Push a Windows image named Image3 to Registry1.
✑ Modify Image1 and push the new image as Image4 to Registry1.
Modify Image2 and push the new image as Image5 to Registry1.
.
Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Image4

B. Image2

C. Image1

D. Image3

E. Image5

Suggested Answer: *BE*
Only Linux images are scanned. Windows images are not scanned.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration

Community vote distribution
BE (56%) AE (44%)

Oskarma Highly Voted 2 years, 9 months ago
Microsoft Defender for container registries has been deprecated. Now Microsoft Defender for Containers can check windows images too.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-container-registries-introduction
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction
upvoted 22 times

koreshio 2 years, 8 months ago
yup ref: https://zigmax.net/defender-for-containers-can-now-scan-for-vulnerabilities-in-windows-images/
upvoted 1 times

flafernan 1 year, 6 months ago
This is official from Microsoft?
upvoted 1 times

pekay 2 years, 2 months ago
your referenced article https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-container-registries-introduction
still states that Windows images are unsupported. therefore the answer is right.
upvoted 6 times

Rume Highly Voted 3 years, 12 months ago
given answer is correct
upvoted 9 times

ca7859c Most Recent 2 weeks, 5 days ago
Selected Answer: BE
Windows is not supported
Only Linux is
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-container-registries-introduction
upvoted 1 times

ca7859c 1 month ago

Selected Answer: BE

Defender for containers support most of linux Distros & Only Windows Server

https://learn.microsoft.com/en-us/azure/defender-for-cloud/support-matrix-defender-for-containers?tabs=arcva%2Cazurert%2Cazurespm%2Cazurecssc%2Cawsnet#registries-and-images-support-for-vulnerability-assessment

upvoted 1 times

khamrumunnu 1 month ago

Selected Answer: BE

BE'

Key Considerations:
Windows images are NOT scanned by default for vulnerabilities in Azure Container Registry.
Only Linux-based images are supported for vulnerability scanning.
Each time a new Linux image is pushed (even if it's a modification), it will be scanned again.

upvoted 2 times

Jimmy500 1 year ago

Now we can scan Windows images as well this question is outdated also question talks about Azure Container Registery which is already deprecated and now we can scan both Windows and Linux images with Defender for containers.
In the old times answer was BE, now ABCDE.

upvoted 3 times

xRiot007 11 months, 1 week ago

Who told you that ACR is deprecated ? There is no such mention anywhere in the related MS docs.

upvoted 1 times

[Removed] 1 year, 6 months ago

Supported registries and images: Linux images in ACR registries accessible from the public internet with shell access
ACR registries protected with Azure Private Link
Unsupported registries and images: Windows images
'Private' registries (unless access is granted to Trusted Services)
Super-minimalist images such as Docker scratch images, or "Distroless" images that only contain an application and its runtime dependencies without a package manager, shell, or OS
Images with Open Container Initiative (OCI) Image Format Specification
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-container-registries-introduction

upvoted 1 times

morito 1 year, 6 months ago

So there's an update to this. It seems that scanning windows images is now available in preview. On this site: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-architecture?tabs=defender-for-container-arch-aks was a little note pointing here: https://learn.microsoft.com/en-us/azure/defender-for-cloud/support-matrix-defender-for-containers#registries-and-images-support-for-azure---vulnerability-assessment-powered-by-qualys

The referenced table clearly states that " Windows images using Windows OS version 1709 and above (Preview). This is free while it's in preview, and will incur charges (based on the Defender for Containers plan) when it becomes generally available."

upvoted 1 times

Obama_boy 1 year, 6 months ago

Selected Answer: BE

Azure Container Registry vulnerability scanning, when enabled, automatically scans images as they are pushed to the registry. However, it's important to note that Azure Security Center's container scanning typically supports Linux images and does not support Windows images. Given this, the images that will be scanned for vulnerabilities are:

B. Image2 - This is a Linux image which will be scanned upon push to the registry.

E. Image5 - This is also a Linux image (modified from Image2) and will be scanned when it's pushed to the registry.

The Windows images (Image1, Image3, and Image4) will not be scanned by Azure Security Center's container scanning feature, as it does not support Windows images. Therefore, correct answers are Image2 and Image5.

upvoted 1 times

Obama_boy 1 year, 6 months ago

Selected Answer: AE

chatgpt says AE

upvoted 1 times

flafernan 1 year, 7 months ago

Selected Answer: AE

When you enable vulnerability scanning in an Azure Container Registry (ACR), Azure Security Center automatically scans images that are streamed into the registry. This includes scanning the image layers for vulnerabilities.

Based on the actions described:

Image push Windows Image1: Will be checked.
Linux Image2 image push: Will be checked.
Windows Image3 image push: Will be checked.
Modify Image1 and push the new image as Image4: A new image (Image4) will be checked.
Modify Image2 and push the new image as Image5: A new image (Image5) will be checked.
Therefore, all images i.e. Image1, Image2, Image3, Image4 and Image5 will be scanned for vulnerabilities. The correct answers are:

A. Image4

E. Image5

upvoted 1 times

TheProfessor 1 year, 7 months ago

Windows images using Windows OS version 1709 and above (Preview) are also supported.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/support-matrix-defender-for-containers

upvoted 1 times

ESAJRR 1 year, 9 months ago

Selected Answer: BE

B. Image2
E. Image5

upvoted 1 times

alfaAzure 1 year, 10 months ago

Selected Answer: AE

Letter A and E.

Images that were pushed initially (Image1, Image2, Image3) will not be scanned for vulnerabilities retroactively since the scanning process is typically triggered when images are pushed or updated.

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: BE

B. Image2
E. Image5
It was reserved for Linux machines only. Nowadays Windows is supported as well. So question is outdated

upvoted 4 times

danlo 2 years, 6 months ago

Question is old see new details: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-vulnerability-assessment-azure

upvoted 3 times

WMG 3 years, 2 months ago

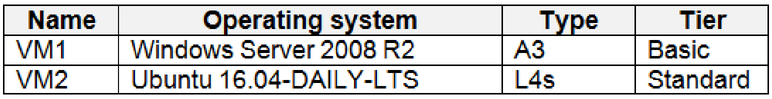
You can now scan Windows images (preview).

upvoted 5 times

Question #37 *Topic 3*

HOTSPOT -

You have two Azure virtual machines in the East US 2 region as shown in the following table.



Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

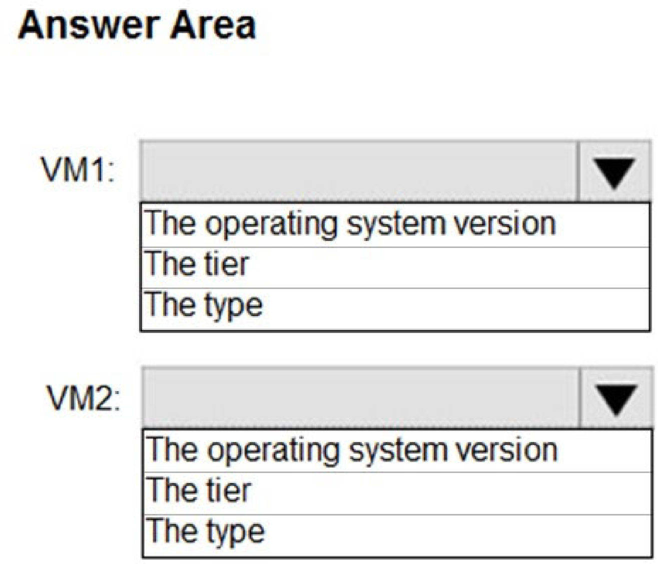
You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

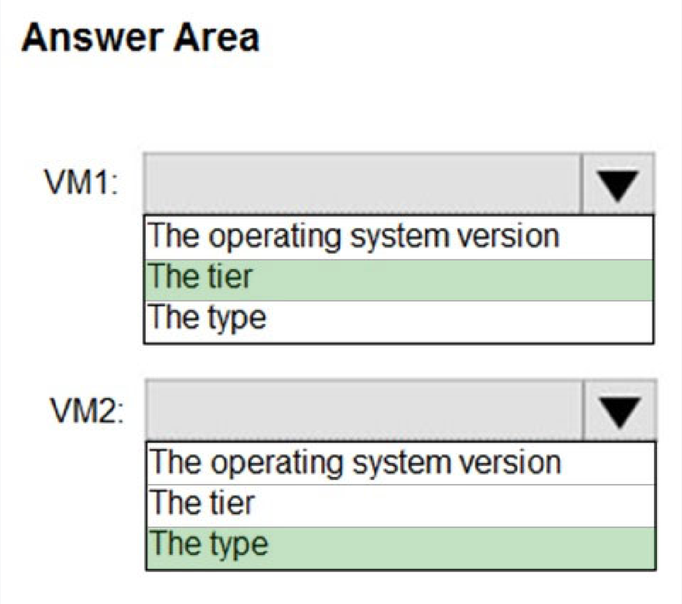


Answer Area

VM1:
- The operating system version
- The tier
- The type

VM2:
- The operating system version
- The tier
- The type

Suggested Answer:



Answer Area

VM1:
- The operating system version
- [✓ The tier]
- The type

VM2:
- The operating system version
- The tier
- [✓ The type]

VM1: The Tier -

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: The type -

Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.

Not the operating system version: Ubuntu 16.04 is supported.

References:

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport

dirgiklis Highly Voted 👍 4 years, 10 months ago

Answer is correct.

VM1: A-series have two tiers Basic and Standard (Basic is not supported)

VM2: L4s is Generation 2 VM size (G2 is not supported)

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/generation-2

upvoted 53 times

> **AZGregor** 3 years, 12 months ago
>
> According to the official AZ-500 Course: "Windows VMs are available in a range of sizes. Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines with a less than 2 GB of memory." Therefore, the Tier and Type does not allow disk encryption on VM1.
>
> upvoted 10 times

> **Patchfox** 3 years ago
>
> Needs an update: L4s is also supported now.
>
> upvoted 8 times
>
> > **costaluisc** 2 years, 5 months ago
> >
> > From MS Docs: "Azure Disk Encryption is supported on Generation 1 and Generation 2 VMs"
> >
> > https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#:~:text=PowerShell%20quickstart.-,Supported%20VMs%20and%20operating%20systems,-Supported%20VMs
> >
> > upvoted 3 times

> **gboyega** 4 years, 5 months ago
>
> this is CORRECT
>
> upvoted 2 times

> **levo017** 4 years, 4 months ago
>
> very thorough, thanks !
>
> upvoted 3 times

Solanki Highly Voted 👍 4 years, 7 months ago

Answers are correct. Below links clearly mentioned this.

Azure Disk Encryption is not available on Basic, A-series VMs.

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview#supported-vms

Azure Disk Encryption is not available on Generation 2 VMs) and Lsv2-series VMs).

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#supported-vms-and-operating-systems

upvoted 13 times

> **aythan09** 4 years, 7 months ago
>
> A L4s is not a LsV2.
>
> https://azure.microsoft.com/en-us/pricing/details/virtual-machines/linux/#lsv2-series
>
> upvoted 3 times

epomatti Most Recent ⊙ 1 year ago

Outdated and wrong.

Generation 2 is now supported.

It's the Ubuntu OS version that is not supported.

https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview

upvoted 3 times

_ajay 1 year ago

Yes, Azure Disk Encryption is supported on L4s VMs. The L4s series is part of the memory-optimized VM sizes1. As per the Azure Disk Encryption documentation, it is supported on Generation 1 and Generation 2 VMs, and is also available for VMs with premium storage. Azure Disk Encryption is supported on the following types of Azure Virtual Machines (VMs):

Generation 1 and Generation 2 VMs123.
VMs with premium storage13.
However, Azure Disk Encryption is not available on:

Basic, A-series VMs13.
Virtual machines with less than 2 GB of memory
upvoted 1 times

wardy1983 1 year, 1 month ago
Explanation:
VM1: The Tier -
The Tier needs to be upgraded to standard.
Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and
Azure Government regions for Standard VMs and VMs with Azure Premium Storage.
VM2: The type -
Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.
Not the operating system version: Ubuntu 16.04 is supported.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview https://docs.micros
oft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport
upvoted 3 times

flafernan 1 year, 1 month ago
Outdated question.
Encrypt entry-level VMs or VMs created using the classic VM creation method.

Windows VMs are available in various sizes. Azure Disk Encryption is supported on Gen 1 and Gen 2 VMs. Azure Disk Encryption is also available for VMs with premium storage.

Azure disk encryption is not available on entry-level A-series VMs or virtual machines with less than 2 GB of memory.
upvoted 1 times

[Removed] 1 year, 3 months ago
VM2 = operating system Ubutuntu 16.04 is not listed here
https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview
upvoted 4 times

majstor86 1 year, 10 months ago
VM1: The tier
VM2: The type

Old question
upvoted 3 times

ben230 3 years, 1 month ago
2nd Answer is wrong. The docs clearly state G2 VMs support disk encryption. L4s is Gen 2, so it does support disk encryption.

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#supported-vms-and-operating-systems
upvoted 3 times

rsharma007 3 years, 4 months ago
For for the first option, it is definitely tier as Basic A Series VMs are not supported(note that it is Basic A series. Standard A Series supports ADE)
For second option, L4s is a storage optimized VM type and hence not in scope of Azure Disk Encryption. HTH
upvoted 2 times

SandroAndrade 3 years, 7 months ago
Now ADE is supported for Generation 2 VM:
https://docs.microsoft.com/en-us/azure/virtual-machines/generation-2#generation-1-vs-generation-2-capabilities
upvoted 3 times

gcpbrig01 3 years, 9 months ago

there is still no clarity as to the compatibility of Ubuntu machine in question. The MS doc clearly says it is compatible.
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#supported-vms

upvoted 1 times

⊟ **milind8451** 3 years, 10 months ago

Given ans seems correct as Azure Disk Encryption is not available on Basic, A-series VMs. Azure Disk Encryption is not available on Generation 2 VMs. L4s is Generation 2 VM size.

upvoted 1 times

⊟ **Sampaiolc** 3 years, 10 months ago

"Linux VMs are available in a range of sizes. Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines that do not meet these minimum memory requirements"

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview

upvoted 1 times

⊟ **certprep2021** 3 years, 11 months ago

the answer is correct

upvoted 1 times

⊟ **Thi** 3 years, 11 months ago

VM1: The type, tier VM2: type
VM1: Azure Disk Encryption is not possible with the A-series virtual machines/ basic tier. If type A3 and tier standard then answer is type, if type A3, and tier basic then answer is both type and tier.
VM2: type because I can't found type L4s in microsoft documentation.

upvoted 1 times

⊟ **nicksu** 3 years, 7 months ago

L4S is there
https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-previous-gen
4 x vCPU & 32Gb RAM, but it is "of previous generation". This could be the key

upvoted 1 times

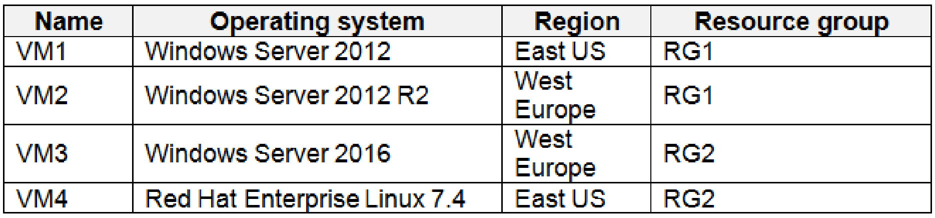
⊟ **B1T3X** 3 years, 11 months ago

ADE isn't available for A-size VMs and Basic tier VMs, therefore both "tier" and type" should be correct in the first answer.

upvoted 2 times

Question #38 Topic 3

You have the Azure virtual machines shown in the following table.



Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.

Which virtual machines can be enrolled in Analytics1?

A. VM1 only

B. VM1, VM2, and VM3 only

C. VM1, VM2, VM3, and VM4

D. VM1 and VM4 only

Suggested Answer: *A*

Note: Create a workspace -

✑ In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input.

Select Log Analytics.

Click Create, and then select choices for the following items:

▪

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.

Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.

For Resource Group, select an existing resource group that contains one or more Azure virtual machines.

Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

Incorrect Answers:

B, C: A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location.

D: VM4 is a different resource group.

References:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access

Community vote distribution

C (100%)

⊟ **Oz** Highly Voted 5 years, 6 months ago

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-overview

It says clearly:

You can deploy Azure VMs from any region. These VMs aren't limited to the regions supported by the Log Analytics workspace.

So correct answer should be: VM1, VM2, VM3 and VM4

upvoted 232 times

⊟ **onlyfunmails** 5 years, 5 months ago

No, your interpretation is wrong, refer below...Its region specific.

https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

Select the Location your VMs are deployed to.

upvoted 1 times

⊟ **Kinanke** 4 years, 4 months ago

correct comment. check: https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-configure-workspace?tabs=CLI#supported-regions

upvoted 2 times

⊟ **[Removed]** 1 year, 10 months ago

Agree with you.
upvoted 3 times

AZGregor 4 years, 6 months ago

Oz is correct, Multiple regions are supported for a single workspace, no matter where the workspace is deployed. Therefore, all four VMs can be connected to the workspace in East US.
upvoted 5 times

junkz Highly Voted 5 years, 8 months ago

vm1 and 4 can, analytics integration is bound by region, not RG
upvoted 62 times

SandroAndrade 4 years, 1 month ago

The correct answer is C, all the VMs can.

You can monitor Azure VMs in any region. The VMs themselves aren't limited to the regions supported by the Log Analytics workspace.
https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-configure-workspace?tabs=CLI#supported-regions
upvoted 2 times

dumdada 3 years, 10 months ago

Regions are just metadata and shouldn't constraint the workspace, hence it's all VMs if I understand correctly
upvoted 3 times

ITFranz Most Recent 10 months, 1 week ago

To support the answer.
https://learn.microsoft.com/en-us/azure/automation/how-to/region-mappings
Answer could be found here.
VMs aren't limited to the regions supported by a given Log Analytics workspace. They can be in any region. Keep in mind that having the VMs in a different region may affect state, local, and country/regional regulatory requirements, or your company's compliance requirements. Having VMs in a different region could also introduce data bandwidth charges.
Answer = VM1, VM2, VM3 and VM4
upvoted 2 times

CletusMaximus 1 year ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/automation/how-to/region-mappings

VMs aren't limited to the regions supported by a given Log Analytics workspace. They can be in any region. Keep in mind that having the VMs in a different region may affect state, local, and country/regional regulatory requirements, or your company's compliance requirements. Having VMs in a different region could also introduce data bandwidth charges.
upvoted 2 times

cris_exam 1 year, 5 months ago

Just tested.

1 workspace in WE Region in RG1
Vm1 in WE Region in RG2
VM2 in UK Region in RG3

I was able with no errors to setup the log analytics workspace to both VMs.

Correct answer is: VM1, VM2, VM3 and VM4
upvoted 5 times

wardy1983 1 year, 8 months ago

ANSWER IS C!!!"

You can monitor Azure VMs in any region. The VMs themselves aren't limited to the regions supported by the
Log Analytics workspace.
https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-configure-workspace?tabs=CLI
upvoted 2 times

ESAJRR 1 year, 9 months ago

Selected Answer: C

C. VM1, VM2, VM3, and VM4

upvoted 2 times

ESAJRR 1 year, 10 months ago

Selected Answer: C

C. VM1, VM2, VM3, and VM4

upvoted 2 times

heatfan900 1 year, 10 months ago

VM1, VM2, VM3, and VM4.

RG does not matter
REGION does not matter

upvoted 1 times

Self_Study 1 year, 10 months ago

Selected Answer: C

on exam 7/8/23
C is correct, all VMs

upvoted 2 times

_fvt 1 year, 11 months ago

Selected Answer: C

Log analytics is a global service not bound by region.
Therefore all VMs are supported.

upvoted 2 times

Mugamed 2 years, 1 month ago

Selected Answer: C

Log analytics can be in any region. The only reason you would want to keep it in the same region is cost.

upvoted 1 times

majstor86 2 years, 3 months ago

Selected Answer: C

C. VM1, VM2, VM3, and VM4

upvoted 2 times

mung 2 years, 7 months ago

Definetely C,
Az104 also have this question and answer is C.

Log analytics is independent from the region.

upvoted 3 times

somenick 2 years, 8 months ago

Selected Answer: C

You can monitor Azure VMs in any region. The VMs themselves aren't limited to the regions supported by the Log Analytics workspace.

upvoted 2 times

Melitajr 2 years, 9 months ago

How about from different resource groups, as VM3 and VM4 are from RG2 and is created in Log Analytics workspace? pls help

upvoted 1 times

chamka 2 years, 9 months ago

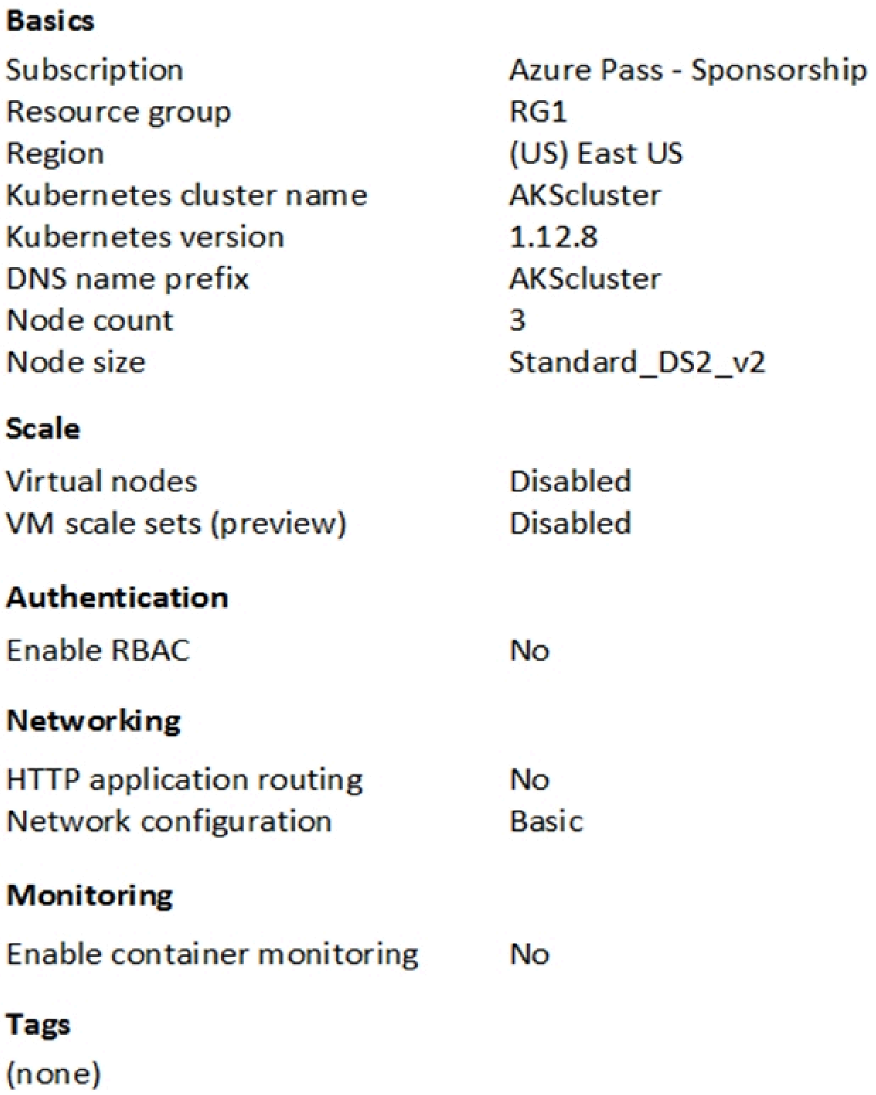
Selected Answer: C

Azure Log Analytics is not region dependent. so all applied.

upvoted 2 times

Question #39 *Topic 3*

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)



Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	(US) East US
Kubernetes cluster name	AKScluster
Kubernetes version	1.12.8
DNS name prefix	AKScluster
Node count	3
Node size	Standard_DS2_v2

Scale

Virtual nodes	Disabled
VM scale sets (preview)	Disabled

Authentication

Enable RBAC	No

Networking

HTTP application routing	No
Network configuration	Basic

Monitoring

Enable container monitoring	No

Tags

(none)

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

A. Create an AKS Ingress controller.

B. Install the container network interface (CNI) plug-in.

C. Create an Azure Standard Load Balancer.

D. Create an Azure Basic Load Balancer.

Suggested Answer: *A*

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

Reference:

https://docs.microsoft.com/en-us/azure/aks/ingress-tls

Community vote distribution

A (100%)

JohnYinToronto Highly Voted 3 years, 3 months ago

answer correct

upvoted 21 times

kumax Highly Voted 3 years ago

On exam, May 2021.

upvoted 7 times

wardy1983 Most Recent 7 months, 2 weeks ago

Answer: A

Explanation:

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

Reference:

https://docs.microsoft.com/en-us/azure/aks/ingress-tls

upvoted 3 times

ESAJRR 10 months ago

Selected Answer: A

A. Create an AKS Ingress controller

upvoted 1 times

Self_Study 10 months, 3 weeks ago

Selected Answer: A

On exam 7/8/23

Ingress correct

upvoted 3 times

majstor86 1 year, 3 months ago

Selected Answer: A

A. Create an AKS Ingress controller.

upvoted 2 times

ligu 1 year, 4 months ago

Answer is correct

upvoted 1 times

Alessandro365 2 years ago

Selected Answer: A

correct

upvoted 2 times

cfsxtuv33 2 years, 6 months ago

Answer is correct, ingress controller provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

upvoted 3 times

itbrpl 2 years, 8 months ago

Today's exam 20/10/21..

upvoted 2 times

TonytheTiger 2 years, 9 months ago

## Exam Question - 17 Sept 2021 ##

upvoted 3 times

francis6170 2 years, 9 months ago

Got this in the AZ-500 exam (Sept 2021)! A: A

upvoted 2 times

Question #40 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines.
Solution: You add an extension to each virtual machine.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.
References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

Community vote distribution
A (100%)

⊟ **lnn_az** Highly Voted 4 years ago
Eventhough adding an extension to each virtual machine meets the goal.

Correct way to do this for 50 virtual machine should be using the below Policy Definition.

Deploy default Microsoft IaaSAntimalware extension for Windows Server
Built-in
This policy deploys a Microsoft IaaSAntimalware extension with a default configuration when a VM is not configured with the antimalware extension.
upvoted 33 times

⊟ **LHU** 1 week, 4 days ago
I think that's the thing; "does it meet the goal"? Yes, it does. Is it a smart way to go about it? Lol, no. But it gets the job done, and that is what matters.
upvoted 1 times

⊟ **GayanWK** 3 years, 6 months ago
or you can use ARM template deployment.
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/iaas-antimalware-windows#template-deployment
upvoted 11 times

⊟ **Solanki** Highly Voted 4 years, 1 month ago
answer is right,

https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware#antimalware-deployment-scenarios
upvoted 14 times

⊟ **ESAJRR** Most Recent 10 months ago
Selected Answer: A
A. Yes
upvoted 2 times

⊟ **majstor86** 1 year, 3 months ago
Selected Answer: A
A. Yes
upvoted 1 times

⊟ **ligu** 1 year, 4 months ago
Answer is correct

upvoted 1 times

F117A_Stealth 1 year, 7 months ago

Selected Answer: A

Yes answer is correct. Although a lengthy way (they are better ways to do this), its still correct. Unless they asked for least admin effort.

upvoted 5 times

Ivanvazovv 1 year, 10 months ago

Nowhere in the statement "You add an extension to each virtual machine" is described that you have to add the extension manually on each machine. You can add it with policy, templates, automation and probably more (I'm not sure about Logic Apps).

upvoted 3 times

Fal991l 1 year, 7 months ago

Agree!. just confusing wording

upvoted 1 times

Edgecrusher77 2 years, 5 months ago

Correct but not efficient at all!

upvoted 9 times

glowglow 3 years, 3 months ago

"You add an extension to each virtual machine." Really? I guess 50 VM is not bad but what if you have 100+vms? you are going to add an extension to each one?

upvoted 2 times

Super_Pun 3 years, 3 months ago

It's correct, Microsoft Antimalware is the extension attached to the Windows Server

upvoted 1 times

sureshatt 3 years, 4 months ago

We do this for our VMs. So the answer is correct.

upvoted 2 times

sukhdeep 3 years, 4 months ago

Visual studio option is available only with Visual studio VMs. This option is not available with all VMs. We can enable Antimalware extension from Azure portal as well.

The Microsoft Antimalware Client and Service is not installed by default in the Virtual Machines platform and is available as an optional feature through the Azure portal and Visual Studio Virtual Machine configuration under Security Extensions.

upvoted 1 times

zic04 3 years, 5 months ago

Correct A

upvoted 2 times

kiketxu 3 years, 7 months ago

right answer. DSC extension is the way

upvoted 4 times

gboyega 3 years, 12 months ago

ANSWER IS CORRECT

upvoted 6 times

jakobaszek 4 years, 1 month ago

The answer is A

upvoted 1 times

Otto_Aulicino 4 years, 5 months ago

I am not sure where the Visual Studio came from in the answer to this question. It sounds more like resource manager to do that.

upvoted 3 times

azurearch 4 years, 4 months ago

https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

upvoted 2 times

Question #41 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines.
Solution: You connect to each virtual machine and add a Windows feature.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Microsoft Antimalware is deployed as an extension and not a feature.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

Community vote distribution

B (100%)

⊟ **kiketxu** Highly Voted 4 years, 7 months ago

Windows feature is not for DSC extensions. NO is the correct answer.

upvoted 11 times

⊟ **schpeter_091** Most Recent 7 months ago

Selected Answer: A

Microsoft Antimalware and Microsoft Defender Antivirus(Windows Defender) are essentially the same, with Microsoft Defender Antivirus being the modern name for Microsoft's comprehensive antimalware solution.

To add this Server feature(nowadays I can see it's installed by default)

Open Server Manager: Click on the Start button, type Server Manager, and press Enter.
Add Roles and Features: In Server Manager, click on Add Roles and Features.
Select Installation Type: Choose Role-based or feature-based installation and click Next.
Select the Server: Choose the server where you want to install Microsoft Defender Antivirus and click Next.
Select Roles: In the Roles section, click Next without selecting any roles.
Select Features: In the Features section, scroll down and check the box for Windows Defender Antivirus under Windows Defender Features. Click Add Features and then Next.
Confirm Selections: Review your selections and click Install.

upvoted 1 times

⊟ **Mugamed** 2 years, 1 month ago

Selected Answer: B

Answer is correct

upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: B

B. No is correct

upvoted 1 times

⊟ **ligu** 2 years, 4 months ago

Answer is correct

upvoted 1 times

⊟ **F117A_Stealth** 2 years, 7 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

Alessandro365 3 years ago

Selected Answer: B

B is correct answer.

upvoted 2 times

gboyega 4 years, 12 months ago

B IS CORRECT

upvoted 4 times

gfhbox0083 4 years, 12 months ago

B, for sure

upvoted 3 times

rajatw 5 years, 1 month ago

Correct Answer. It's B

upvoted 4 times

Question #42 *Topic 3*

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Kubernetes Service (AKS) cluster AKS1.
You discover that AKS1 cannot be accessed by using accounts from Contoso.com.
You need to ensure AKS1 can be accessed by using accounts from Contoso.com. The solution must minimize administrative effort.
What should you do first?

A. From Azure, recreate AKS1.

B. From AKS1, upgrade the version of Kubernetes.

C. From Azure AD, implement Azure AD Premium P2

D. From Azure AD, configure the User settings.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

Community vote distribution

A (100%)

SteroidalRED Highly Voted 4 years, 6 months ago

Answer is correct

The following limitations apply:
Azure AD can only be enabled on Kubernetes RBAC-enabled cluster.
Azure AD legacy integration can only be enabled during cluster creation.

upvoted 34 times

153a793 8 months, 3 weeks ago

i understand since june 1, 2023, Microsoft provided option to integrate AKS later on with Entra ID. pls refer document with "Enable Azure managed identity authentication for Kubernetes clusters with kubelogin"

upvoted 1 times

tuta Highly Voted 4 years, 6 months ago

A is correct - though question has been repeated

upvoted 17 times

khamrumunnu Most Recent 1 month ago

Selected Answer: A

A

You cannot enable AAD integration on an existing AKS cluster unless it was originally created with that option or manually configured (which is more complex and not recommended for minimizing effort).

AKS supports Azure AD integration for Kubernetes RBAC only if specified at creation time (or with significant manual steps afterward, which contradicts the “minimize administrative effort” requirement).

Options like enabling AAD Premium P2 or changing user settings in Azure AD do not directly resolve the issue of an AKS cluster not being accessible via AAD.

upvoted 2 times

golitech 4 months, 4 weeks ago

Selected Answer: D

D. From Azure AD, configure the User settings.

Here's why:
Azure AD Authentication for AKS:

Azure AD can be used to enable Azure AD authentication for AKS clusters. This allows users in your Azure AD tenant to access the AKS cluster without needing to manage additional Kubernetes RBAC users.

In this case, you need to ensure that the proper User settings are configured in Azure AD to enable access from the users in your tenant.

Implementation Steps:

You'll need to configure AKS to integrate with Azure AD for Kubernetes RBAC, which involves setting up Azure AD authentication and ensuring that the correct users from Contoso.com are allowed to access the AKS cluster.

upvoted 2 times

⊟ **pentium75** 11 months ago

Deprecated question it seems

upvoted 2 times

⊟ **Jinkx** 1 year, 6 months ago

To ensure that AKS1 can be accessed by accounts from Contoso.com, you should:

C. From Azure AD, implement Azure AD Premium P2

Explanation:

Azure AD Premium P2: Azure AD Premium P2 provides advanced identity protection capabilities, including features such as Conditional Access and Identity Protection. These features can be essential for securing access to resources, including AKS clusters.

upvoted 1 times

⊟ **wardy1983** 1 year, 7 months ago

Answer: A

Explanation:

you can only integrate AAD with AKS during cluster creation time (using --enable-aad in your CLI code), not

after it has been created.

Reference:

https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

upvoted 2 times

⊟ **ESAJRR** 1 year, 9 months ago

Selected Answer: A

A. From Azure, recreate AKS1.

upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: A

A. From Azure, recreate AKS1.

upvoted 2 times

⊟ **Alessandro365** 3 years ago

Selected Answer: A

A is correct answer.

upvoted 2 times

⊟ **alou333** 3 years ago

# IN EXAM - 3rd june 2022 (online).

Lot of new questions. Good luck !

upvoted 8 times

⊟ **fahrulnizam** 2 years, 6 months ago

how many questions come from here?

upvoted 2 times

⊟ **mshehata** 3 years, 4 months ago

it is now a legacy feature, this can be enabled on existing aks

https://docs.microsoft.com/en-us/azure/aks/managed-aad#enable-aks-managed-azure-ad-integration-on-your-existing-cluster

upvoted 6 times

⊟ **upliftinghut** 2 years, 2 months ago

Agree, now we can enable AD with existing AKS cluster using az aks update command

upvoted 1 times

⊟ **ranhara** 3 years, 2 months ago

No other answer leads to AAD integration of AKS

upvoted 3 times

⊟ **zioggs** 3 years, 7 months ago

Exam - 4/11/21

upvoted 4 times

⊟ **itbrpl** 3 years, 8 months ago

Today's exam 20/10/21..

upvoted 3 times

⊟ **Sandomj55** 3 years, 10 months ago

In Exam 8/4/2021

upvoted 4 times

⊟ **aftab7500** 4 years, 2 months ago

Azure AD can only be enabled on Kubernetes RBAC-enabled cluster.

Azure AD legacy integration can only be enabled during cluster creation.

upvoted 3 times

⊟ **g2d2** 4 years, 3 months ago

As of today, you can only integrate AAD with AKS during cluster creation time (using --enable-aad in your CLI code), not after it has been created.

So Ans A is correct.

upvoted 7 times

Question #43 *Topic 3*

You have an Azure subscription that contains an Azure Container Registry named Registry1. Microsoft Defender for Cloud is enabled in the subscription.

You upload several container images to Registry1.

You discover that vulnerability security scans were not performed.

You need to ensure that the container images are scanned for vulnerabilities when they are uploaded to Registry1.

What should you do?

A. From the Azure portal, modify the Pricing tier settings.

B. From Azure CLI, lock the container images.

C. Upload the container images by using AzCopy.

D. Push the container images to Registry1 by using Docker.

Suggested Answer: *A*

Reference:

https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/

Community vote distribution

A (100%)

w00t Highly Voted 👍 3 years, 10 months ago

Commenting again because I found this.

Answer is A -- Follow this link for a good explanation. I think this question is missing a portion in it that the subscription uses Standard tiering:

https://www.examtopics.com/discussions/microsoft/view/39932-exam-az-500-topic-2-question-48-discussion/

upvoted 16 times

ITFranz 5 months, 3 weeks ago

There is anything in the question that states what subscription type. Hard to get the right answer.

Thankyou w00t for the input.

upvoted 1 times

OpsecDude 2 years, 9 months ago

This question needs more context as you mentioned, they'd have mentioned the tier was Standard.

upvoted 3 times

JakeCallham 2 years, 9 months ago

Even without that info, the other answers dont make sense at all, this one at least does.

upvoted 7 times

JaiSharma Highly Voted 👍 3 years, 9 months ago

In exam today!

upvoted 10 times

schpeter_091 Most Recent 🕒 7 months ago

Selected Answer: A

Support for answer 'A'.

"The Basic tier of Azure Container Registry does not include vulnerability scanning. To enable vulnerability scanning for your container images, you need to be on the Standard tier or higher."

upvoted 1 times

91743b3 10 months, 3 weeks ago

On exam Aug 6 2024

upvoted 2 times

flafernan 1 year, 7 months ago

Selected Answer: A

Microsoft Defender for Cloud in its standard version does not have Defender for Kubernetes enabled. If you want your container images to be scanned when the images are uploaded, you will need to enable it and add this new “tier” to your monthly cost.

https://learn.microsoft.com/pt-br/azure/defender-for-cloud/defender-for-kubernetes-introduction

upvoted 2 times

be9z 1 year, 8 months ago

The answer is A because fee tier for Microsoft Defender expires after 30 days, hence the vulnerability scanning will stop working. You will need to get a paid tier (standard)

upvoted 2 times

ESAJRR 1 year, 9 months ago

Selected Answer: A

A. From the Azure portal, modify the Pricing tier settings.

upvoted 1 times

majstor86 2 years, 3 months ago

Selected Answer: A

A. From the Azure portal, modify the Pricing tier settings.

upvoted 2 times

ligu 2 years, 4 months ago

Answer is correct.

upvoted 1 times

OrangeSG 2 years, 5 months ago

Selected Answer: A

Defender for Cloud offers basic, and many enhanced security features that can help protect your organization against threats and attacks.

When you enable the enhanced security features (paid), Defender for Cloud can provide unified security management and threat protection across your hybrid cloud workloads, including: Container security features

Container security features - Benefit from vulnerability management and real-time threat protection on your containerized environments. Charges are based on the number of unique container images pushed to your connected registry. After an image has been scanned once, you won't be charged for it again unless it's modified and pushed once more.

Reference

Basic and enhanced security features

https://learn.microsoft.com/en-us/azure/defender-for-cloud/enhanced-security-features-overview

upvoted 1 times

gentos 3 years, 4 months ago

Selected Answer: A

Need to enable scanning for container registries from pricing tier.

upvoted 3 times

TonytheTiger 3 years, 9 months ago

## Exam Question - 17 Sept 2021 ##

upvoted 6 times

francis6170 3 years, 9 months ago

Got this in the AZ-500 exam (Sept 2021)!

upvoted 7 times

kakakayayaya 3 years, 10 months ago

Not C because: Azure Defender will then scan all images when they're pushed to the registry, imported into the registry, or pulled within the last 30 days.

https://docs.microsoft.com/en-us/azure/security-center/defender-for-container-registries-introduction

upvoted 1 times

> **kakakayayaya** 3 years, 10 months ago
>
> Answer A fists mostly but I don like the way how question presented by Microsoft.
>
> upvoted 5 times

w00t 3 years, 10 months ago

Does anyone have proper insight as to why the answer is apparently "A"? I'm confused here.

upvoted 1 times

⊟ **rsharma007** 3 years, 10 months ago

Since in this case even with Azure Defender enabled, new images are not scanned, it could be that defender is currently setup with Container registry plan to "Off".

upvoted 2 times

⊟ **epic13131** 3 years, 11 months ago

How is it not C?

upvoted 1 times

Question #44 *Topic 3*

From Azure Security Center, you create a custom alert rule.
You need to configure which users will receive an email message when the alert is triggered.
What should you do?

A. From Azure Monitor, create an action group.

B. From Security Center, modify the Security policy settings of the Azure subscription.

C. From Azure Active Directory (Azure AD), modify the members of the Security Reader role group.

D. From Security Center, modify the alert rule.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

Community vote distribution
A (100%)

dumpmaster Highly Voted 5 years, 2 months ago
Right, I use Azure monitor for some of my clients.
upvoted 22 times

cunlu Highly Voted 4 years, 6 months ago
An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered. Various alerts may use the same action group or different action groups depending on the user's requirements.
upvoted 16 times

schpeter_091 Most Recent 7 months, 1 week ago
What I can see now, I can set the emails for users who get a notification:
from MS Defender for Cloud - environmental settings - select the subscription - email notifications
upvoted 1 times

ESAJRR 1 year, 9 months ago
Selected Answer: A
A. From Azure Monitor, create an action group.
upvoted 1 times

Mugamed 2 years, 1 month ago
Selected Answer: A
Correct, I've been creating a lot of alerts recently and this is exactly where you decide who gets notified.
upvoted 2 times

majstor86 2 years, 3 months ago
Selected Answer: A
A. From Azure Monitor, create an action group.
upvoted 2 times

Tombarc 3 years, 5 months ago
Custom alerts should be done through Workflow Automation (left panel), the automation is executed based on new alerts on Microsoft Defender for Cloud. This question is outdated, I just hope it's not part of the exam. :)
upvoted 4 times

> **danlo** 2 years, 6 months ago
> Agreed, question seems outdated
> upvoted 1 times

Incredible99 3 years, 7 months ago
Alert rules in Azure Monitor use action groups, which contain unique sets of recipients and actions that can be shared across multiple rules.
upvoted 3 times

⊟ **vaaws** 3 years, 10 months ago

outdated question

https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

upvoted 3 times

⊟ **vj77** 3 years, 10 months ago

I can replicate the action group in lab as suggested in the solution ref

upvoted 2 times

⊟ **MarioMK** 4 years, 1 month ago

I think this queston is a bit obsolete. I wasnt able to find a place in Security Center where I can create the custom rules. The only option avaiable is in Pricing & Settings

upvoted 1 times

⊟ **Payday123** 3 years, 4 months ago

I wasn't able to find Security Center! :)

upvoted 3 times

⊟ **Cyberbug2021** 4 years, 2 months ago

what about this

https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

email notifications for security alerts from security center. pricing & settings

upvoted 1 times

⊟ **inf** 4 years, 5 months ago

Answer: A (By elimination)

A: Correct - assumes ASC is configured to stream logs to Azure monitor.

B: Incorrect - (badly worded) - "security policy defines the desired configuration of your workloads and helps ensure you're complying with the security requirements of your company or regulators" - nothing to do with alerts

C: Incorrect - Security Reader role group membership does not imply receiving email notifications

D: Incorrect - Security Center alert rules don't specify recipients.

Best solution would be to use ASC Pricing and Settings, which sadly isn't an option

upvoted 6 times

⊟ **inf** 4 years, 5 months ago

Notes

Azure Security Center | Pricing and Settings allows direct configuration of email alerts

https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

More complicated to configure Azure Monitor integration

https://charbelnemnom.com/how-to-integrate-azure-security-center-with-azure-monitor-alerts/

Creating custom alerts, emails are triggered on the selected severity, as with inbuilt rules

https://www.microsoftpressstore.com/articles/article.aspx?p=2923216&seqNum=3

upvoted 2 times

⊟ **Awraith** 4 years, 11 months ago

I believe answer is correct, by elimination, but I think best way to set notifications is to go to Pricing & Setting in ASC and Settings | Email notifications.

upvoted 3 times

⊟ **hstorm** 4 years, 9 months ago

That is very very wrong. Best solution is definately to define an action group

upvoted 4 times

⊟ **joilec435** 5 years, 1 month ago

sentinel

upvoted 3 times

⊟ **JohnCrawford** 5 years, 8 months ago

Custom alerts were in preview and are deprecated as of end of June 2019. https://docs.microsoft.com/en-us/azure/security-center/security-center-features-retirement-july2019#menu_investigate

upvoted 3 times

Question #45 *Topic 3*

You are configuring and securing a network environment.
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.
You need to ensure that all network traffic is routed through VM1.
What should you configure?

A. a system route

B. a network security group (NSG)

C. a user-defined route

Suggested Answer: *C*
Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.

Note: User Defined Routes -
For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:
✑ Force tunneling to the Internet via your on-premises network.
✑ Use of virtual appliances in your Azure environment.
✑ In the scenarios above, you will have to create a route table and add user defined routes to it.
Reference:
https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md

Community vote distribution

C (100%)

Jhonsteve83 Highly Voted 👍 4 years, 7 months ago
answer is correct
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview
upvoted 27 times

kdkdk Highly Voted 👍 4 years ago
in the exams
upvoted 20 times

InfoSecGuy93 Most Recent ⏱ 6 months, 3 weeks ago
Inexam. A lot of questions are from here. One case study and 52 total questions
upvoted 7 times

ESAJRR 1 year, 3 months ago
Selected Answer: C
C. a user-defined route
upvoted 1 times

Self_Study 1 year, 4 months ago
On an exam on 7/8/23, agree with the answer provided.
upvoted 2 times

majstor86 1 year, 9 months ago
Selected Answer: C
C. a user-defined route
upvoted 2 times

ligu 1 year, 10 months ago
Answer is correct
upvoted 1 times

chijokz 2 years, 1 month ago

"all network traffic is routed through VM1"

Has to be User defined route.

upvoted 1 times

⊟ **Alessandro365** 2 years, 6 months ago

Selected Answer: C

C is correct answer.

upvoted 1 times

⊟ **Alessandro365** 2 years, 6 months ago

Selected Answer: C

answer: C

upvoted 1 times

⊟ **Eltooth** 2 years, 9 months ago

Selected Answer: C

C is correct answer - UDR.

upvoted 2 times

⊟ **omw2wealth** 3 years ago

Damn im so confident bout da pass

upvoted 6 times

⊟ **cfsxtuv33** 3 years ago

Do it to it...my brotha from anotha motha!

upvoted 9 times

⊟ **Jco** 3 years, 3 months ago

#exam ques # 29 Sep

upvoted 3 times

⊟ **Socgen1** 3 years, 4 months ago

In exam on 31/08/2021 - User defined

upvoted 3 times

⊟ **zic04** 3 years, 11 months ago

C correct

upvoted 4 times

⊟ **deegadaze1** 3 years, 11 months ago

Custom routes==>User-defined

You create custom routes by either creating user-defined routes or by exchanging border gateway protocol (BGP) routes between your on-premises network gateway and an Azure virtual network gateway.

User-defined

You can create custom, or user-defined(static), routes in Azure to override Azure's default system routes, or to add additional routes to a subnet's route table.

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

upvoted 3 times

⊟ **gboyega** 4 years, 5 months ago

C IS CORRECT

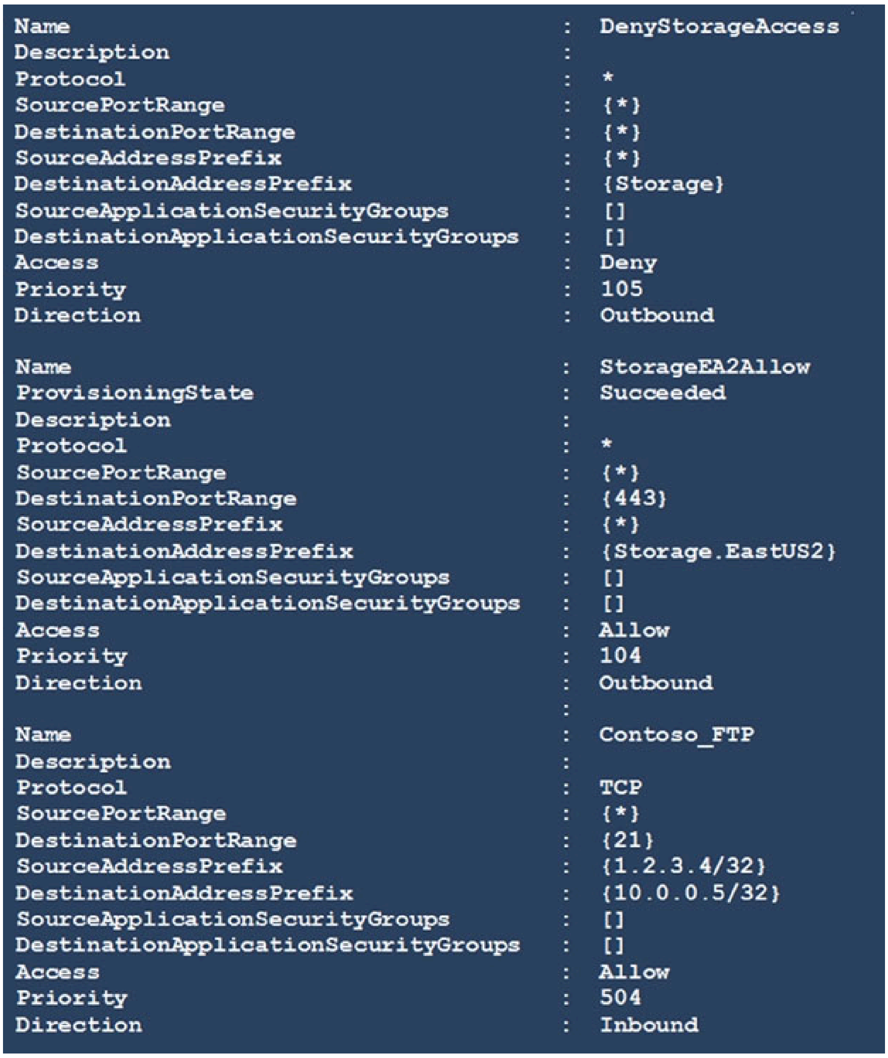
upvoted 3 times

Question #46 *Topic 3*

HOTSPOT -

You have a network security group (NSG) bound to an Azure subnet.

You run Get-AzNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

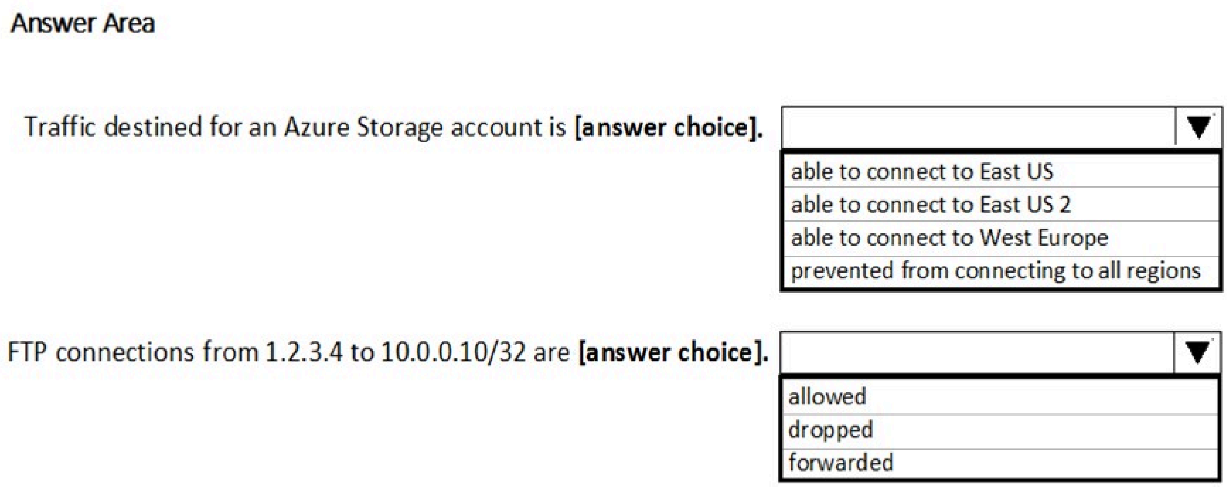


```
Name                                  :  DenyStorageAccess
Description                           :
Protocol                              :  *
SourcePortRange                       :  {*}
DestinationPortRange                  :  {*}
SourceAddressPrefix                   :  {*}
DestinationAddressPrefix              :  {Storage}
SourceApplicationSecurityGroups       :  []
DestinationApplicationSecurityGroups  :  []
Access                                :  Deny
Priority                              :  105
Direction                             :  Outbound

Name                                  :  StorageEA2Allow
ProvisioningState                     :  Succeeded
Description                           :
Protocol                              :  *
SourcePortRange                       :  {*}
DestinationPortRange                  :  {443}
SourceAddressPrefix                   :  {*}
DestinationAddressPrefix              :  {Storage.EastUS2}
SourceApplicationSecurityGroups       :  []
DestinationApplicationSecurityGroups  :  []
Access                                :  Allow
Priority                              :  104
Direction                             :  Outbound
                                      :
Name                                  :  Contoso_FTP
Description                           :
Protocol                              :  TCP
SourcePortRange                       :  {*}
DestinationPortRange                  :  {21}
SourceAddressPrefix                   :  {1.2.3.4/32}
DestinationAddressPrefix              :  {10.0.0.5/32}
SourceApplicationSecurityGroups       :  []
DestinationApplicationSecurityGroups  :  []
Access                                :  Allow
Priority                              :  504
Direction                             :  Inbound
```

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

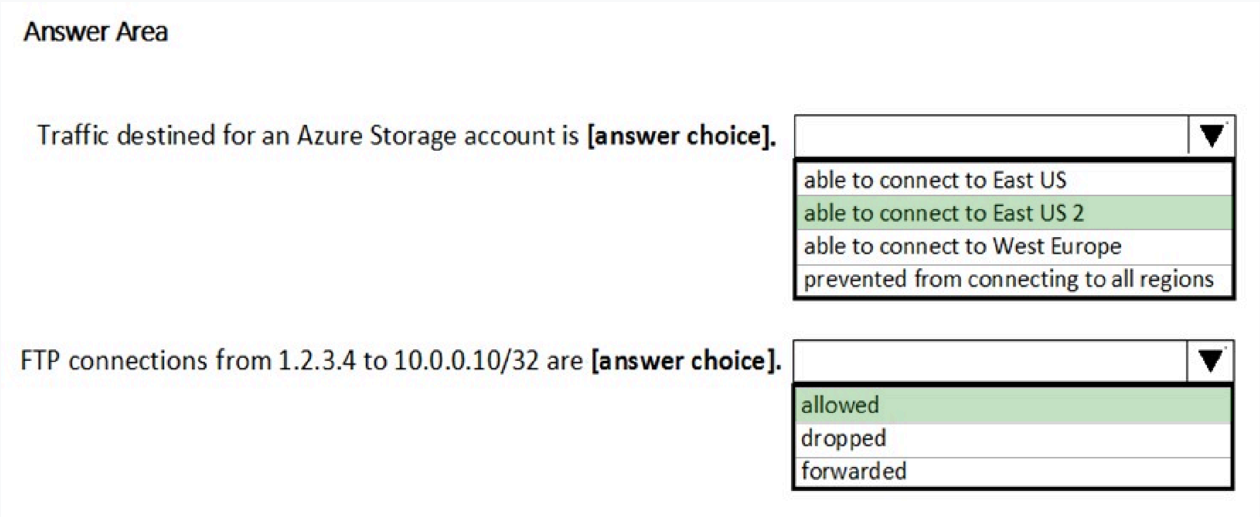
Traffic destined for an Azure Storage account is **[answer choice]**.

- able to connect to East US
- able to connect to East US 2
- able to connect to West Europe
- prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are **[answer choice]**.

- allowed
- dropped
- forwarded

Suggested Answer:



Answer Area

Traffic destined for an Azure Storage account is **[answer choice].**

- able to connect to East US
- [✓ able to connect to East US 2]
- able to connect to West Europe
- prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are **[answer choice].**

- [✓ allowed]
- dropped
- forwarded

Box 1: able to connect to East US 2

The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2}

Box 2: allowed -

TCP Port 21 controls the FTP session. Contoso_FTP has SourceAddressPrefix {1.2.3.4/32} and DestinationAddressPrefix {10.0.0.5/32}

Note:

The Get-AzureRmNetworkSecurityRuleConfig cmdlet gets a network security rule configuration for an Azure network security group.

Security rules in network security groups enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

JohnCrawford Highly Voted 4 years, 8 months ago

The second part of your answer is incorrect. The FTP traffic is coming from 1.2.3.4/32 and going to 10.0.0.10/32. The NSG rule for port 21 allows traffic from 1.2.3.4 to 10.0.0.5 NOT 10.0.0.10. 10.0.0.5/32 equates to a single IP address. 10.0.0.5. There is no rule allowing FTP traffic to 10.0.0.10.

upvoted 164 times

rgullini 3 years, 2 months ago

This is correct. But I also thing is typo. Nevertheless, if it is not a typo the answer for second point is "dropped"

upvoted 11 times

GraceCyborg 3 years, 4 months ago

i believe its a typo..

upvoted 7 times

gboyega Highly Voted 3 years, 12 months ago

should be

1. ABLE TO CONNECT TO EAST US2

2. DROPPED (because the cidr notation is a /32 which means only one IP, which is different from the IP in the rule. so the packet would be dropped.

upvoted 46 times

wardy1983 Most Recent 8 months ago

Box 1: able to connect to East US 2

The StorageEA2Allow has DestinationAddressPrefix Storage/EastUS2

Box 2: DROPPED

because the cidr notation is a /32 which means only one IP, which is different from the IP in the rule. so the packet would be dropped.

upvoted 2 times

Hot_156 4 months, 2 weeks ago

Direction for the BOX 1 is Outbound. There is not an Inbound rule for the storage account.

upvoted 1 times

ESAJRR 9 months ago

1. ABLE TO CONNECT TO EAST US2

2. DROPPED

upvoted 3 times

heatfan900 10 months ago

east US2 as specified in STORAGE NSG rule

Denied since the FTP NSG rule clearly states connections are only allowed to 10.0.0.5/32. That is a single host address.

upvoted 2 times

majstor86 1 year, 3 months ago

Box 1: able to connect to East US 2

Box 2: dropped

upvoted 8 times

ligu 1 year, 4 months ago

1 - Able to connect to east US2 because priority is 104

2 - dropped because 10.10.0.10/32 is not allow

upvoted 3 times

junkm 1 year, 6 months ago

- storage allowed to East US2 - rule sequence is before storage deny rule
- FTP is dropped, policy allows traffic to 10.0.0.5 not 10.0.0.10

upvoted 2 times

F117A_Stealth 1 year, 7 months ago

1 - is correct. the direction is indeed outbound FROM the subnet TO the Azure storage (hence outbound from the perspective of a NSG attached to the subnet in question).

2. is incorrect, look at the CIDR (/32) is diff.

SIMPLE!

upvoted 2 times

bacana 1 year, 9 months ago

Both are wrong. 1 - Direction is outbound and not inbound. 2 dropped because IP address

upvoted 1 times

> **koreshio** 1 year, 8 months ago
>
> 1 - is correct. the direction is indeed outbound FROM the subnet TO the Azure storage (hence outbound from the perspective of a NSG attached to the subnet in question).
>
> upvoted 2 times

MoFami 1 year, 12 months ago

In Exam 01/07/2022

upvoted 2 times

Alessandro365 2 years ago

I think it has a typo, if you look at the explanation of the answers it says the "DestinationAddressPrefix" is 10.0.0.5/32.

In this case, the answer to the second question is "Allow".

If the IP is really "10.0.0.10/32" as it is in the question, then the answer would be "Dropped".

upvoted 1 times

> **Alessandro365** 2 years ago
>
> Answer: 1 - ABLE TO CONNECT TO EAST US2
>
> 2 - ALLOW (if IP 10.0.0.5/32) or DROPPED (if IP 10.0.0.10/32)
>
> upvoted 2 times

RiteshAg 2 years, 5 months ago

Forget about IP range, the priority of denying will overtake the 3rd rule. Therefore, the traffic will be dropped for the 2nd point.

upvoted 9 times

> **arseyam** 1 year, 8 months ago
>
> Denying is targeting storage accounts not FTP
>
> upvoted 1 times

omw2wealth 2 years, 6 months ago

Super easy, its freestyle question

upvoted 2 times

⊟ **SecurityAnalyst** 2 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 3 times

⊟ **Socgen1** 2 years, 10 months ago

In exam on 31/08/2021 - answer is correct

upvoted 4 times

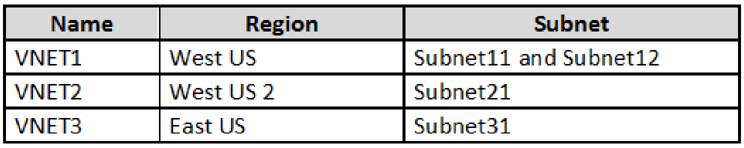
⊟ **aftab7500** 2 years, 10 months ago

Second answer is Dropped: Reason is there is only 1 address in IP address range: 10.0.0.5-10.0.0.5.

upvoted 3 times

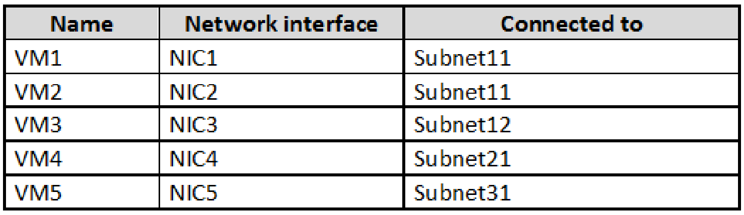
Question #47 *Topic 3*

You have an Azure subscription that contains the virtual networks shown in the following table.



Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

The subscription contains the virtual machines shown in the following table.



Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1.

On which other network interfaces can you configure ASG1?

A. NIC2 only

B. NIC2, NIC3, NIC4, and NIC5

C. NIC2 and NIC3 only

D. NIC2, NIC3, and NIC4 only

Suggested Answer: *C*

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

Community vote distribution

C (100%)

HarryD Highly Voted 4 years, 2 months ago

https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

• All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

upvoted 36 times

maj79 4 years ago

hence answer A is correct

upvoted 7 times

maj79 4 years ago

Correction : hence answer C is correct

upvoted 23 times

rgullini 3 years, 2 months ago

You corrected yourself below. So, just for the ones reading, correct answer is C

upvoted 8 times

David_986969 4 years ago

Application ecurity group is assign at the resource group level

upvoted 2 times

Anamak2 4 years ago

You cannot add network interfaces from different virtual networks to the same application security group.

So given ans is correct - C. NIC1,NIC2 and NIC3 are in same VNET

upvoted 21 times

gboyega Highly Voted 3 years, 12 months ago

C is Correct

They are part of the Same VNET

Confirmed in the Lab

upvoted 26 times

wardy1983 Most Recent 7 months, 2 weeks ago

Answer: C

Explanation:

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

upvoted 1 times

ESAJRR 9 months ago

Selected Answer: C

C. NIC2 and NIC3 only

upvoted 2 times

zellck 1 year, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups#allow-database-businesslogic

Application security groups have the following constraints:

- All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You can't add network interfaces from different virtual networks to the same application security group.

upvoted 1 times

majstor86 1 year, 3 months ago

Selected Answer: C

C. NIC2 and NIC3 only

upvoted 1 times

ligu 1 year, 4 months ago

Answer is correct

upvoted 1 times

F117A_Stealth 1 year, 7 months ago

Selected Answer: C

Correct Answer: NIC2 and NIC3 only

They are part of the Same VNET (VNET1 has Subnets 11 & 12 >>> NIC1 = Subnet11 & NIC3 = Subnet12)

upvoted 1 times

MoFami 1 year, 12 months ago

In Exam 01/07/2022

upvoted 6 times

Alessandro365 2 years ago

Selected Answer: C

C is correct answer.

upvoted 2 times

observador081 2 years, 1 month ago

You have an Azure subscription that includes following resources:

VNet1, a virtual network

Subnet1, a subnet in VNet1

VM1, a virtual machine

NIC1, a network interface of VM1

LB1, a load balancer

You create a network security group named NSG1.

To which two Azure resources can you associate NSG1?

Selecione todas as respostas aplicáveis.

(A)LB1

(B)VM1

(C)NIC1

(D)VNet1

(E)Subnet1

upvoted 5 times

⊟ **Eltooth** 2 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 1 times

⊟ **SecurityAnalyst** 2 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 3 times

⊟ **kumax** 3 years ago

On exam, May 2021.

upvoted 6 times

⊟ **MarioMK** 3 years, 1 month ago

The given answer is correct. All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

upvoted 3 times

⊟ **glowglow** 3 years, 3 months ago

C is correct. Vnet1 has subnet11 and 12

upvoted 4 times

⊟ **scarw7** 3 years, 5 months ago

same typo in explanation at vcpguide. who is copying from whom? :-)

upvoted 1 times

Question #48 *Topic 3*

You have 15 Azure virtual machines in a resource group named RG1.
All the virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines.
What should you do?

A. Apply an Azure policy to RG1.

B. From Azure Security Center, configure adaptive application controls.

C. Configure Azure Active Directory (Azure AD) Identity Protection.

D. Apply a resource lock to RG1.

Suggested Answer: *B*
Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security
Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

Community vote distribution
B (100%)

kristiann21 Highly Voted 👍 4 years, 7 months ago
correct answer
upvoted 29 times

gboyega Highly Voted 👍 4 years, 5 months ago
B is Correct
upvoted 11 times

Knighthell Most Recent 🕒 2 weeks ago
Selected Answer: B
outdate , now is defender for cloud --> Defender for Servers P2 --> Microsoft Defender for Endpoint extension

Agentless machine scanning
upvoted 2 times

ITFranz 5 months, 3 weeks ago
Selected Answer: B
To support the answer.
Adaptive Application Controls is an intelligent security feature in Microsoft Defender for Cloud that helps protect Azure and non-Azure virtual machines against malware and unauthorized software. Key aspects include:
1. Machine learning: Uses AI to analyze applications running on VMs and create a baseline of known-safe applications.
2. Automated whitelisting: Generates and maintains a list of allowed applications, reducing manual overhead.
3. Grouping: Automatically groups similar VMs to apply consistent policies across multiple servers.
4. Alerting: Detects and alerts on applications not in the approved list, without enforcing blocking.
5. Multi-platform support: Works on Windows and Linux VMs, both in Azure and on-premises (via Azure Arc).
6. Continuous learning: Adapts to changes in application behavior and usage patterns over time.

Answer: B
upvoted 1 times

Ivan80 11 months ago
In exam 1/28/24
upvoted 3 times

ESAJRR 1 year, 3 months ago

Selected Answer: B

B. From Azure Security Center, configure adaptive application controls.

upvoted 1 times

ESAJRR 1 year, 3 months ago

Selected Answer: B

B. From Azure Security Center, configure adaptive application controls.

upvoted 1 times

ServerBrain 1 year, 4 months ago

Selected Answer: B

100% B, the other answers have nothing to do with vulnerability..

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls#what-are-adaptive-application-controls
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the following instructions.

upvoted 4 times

zellck 1 year, 7 months ago

Gotten this in May 2023 exam.

upvoted 3 times

MarMarRaf 1 year, 9 months ago

was in march 2023 on exam

upvoted 4 times

majstor86 1 year, 9 months ago

Selected Answer: B

B. From Azure Security Center (Defender for cloud), configure adaptive application controls.

upvoted 2 times

stepman 1 year, 8 months ago

I chose this. On exam 4/27 along with the new user experience exam

upvoted 2 times

ligu 1 year, 10 months ago

Now, Defender for cloud, configure adaptive application controls
Answer is correct

upvoted 1 times

F117A_Stealth 2 years, 1 month ago

Selected Answer: B

Correct Answer: From Azure Security Center, configure adaptive application controls.

upvoted 1 times

WMG 2 years, 8 months ago

This question has to come from some b-level "training", as official MS documentation states that this can _not_ enforce, and only serves as an alert & compliance tool.

upvoted 1 times

Eltooth 2 years, 9 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

SecurityAnalyst 3 years, 4 months ago

# IN EXAM - 31/8/2021

upvoted 5 times

⊟ **rsharma007** 3 years, 4 months ago

Adaptive app control by ASC is the best choice , but not 100% correct. Question asks for preventing apps from running. App control only alerts on unsafe applications. There is no enforcement or prevention of unsafe apps.

upvoted 2 times

Question #49 *Topic 3*

You have a web app hosted on an on-premises server that is accessed by using a URL of https://www.contoso.com.
You plan to migrate the web app to Azure. You will continue to use https://www.contoso.com.
You need to enable HTTPS for the Azure web app.
What should you do first?

A. Export the public key from the on-premises server and save the key as a P7b file.

B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.

C. Export the public key from the on-premises server and save the key as a CER file.

D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements

Community vote distribution
B (69%) D (27%) 4%

⊟ **wongtony** Highly Voted 3 years, 5 months ago
Upvote here if you was shocked the correct answer is not D (I know if you actually have read the document it's B)
upvoted 142 times

⊟ **PointsE** 3 years, 1 month ago
Ironic, as this is a security focused exam...
upvoted 11 times

⊟ **cfsxtuv33** 2 years, 11 months ago
I'm in agreement 100%
upvoted 6 times

⊟ **cfsxtuv33** 2 years, 11 months ago
Shocked...yeah, absolutely
upvoted 6 times

⊟ **EM1234** 2 years, 1 month ago
I would have never thought that it was like this. I am so glad I saw this. Sad though, that it is this way.
upvoted 1 times

⊟ **madhatter** 2 years, 2 months ago
Still picking AES256 for the principal. I don't care about getting the answer wrong here. Sticking to industry standard, yes I am dead serious LOL
upvoted 16 times

⊟ **Coldriver** Highly Voted 3 years, 11 months ago
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate

Private certificate requirements:
Azure Web Apps does not support AES256 and all pfx files should be encrypted with TripleDES.
upvoted 55 times

⊟ **costaluisc** 2 years, 5 months ago
Its supported now. The documentation has been updated.
upvoted 8 times

⊟ **Panno** 2 years, 4 months ago
It hasn't been updated, it is still 3DES in the link provided by MS.
upvoted 4 times

⊟ **Strive_for_greatness_kc** 11 months, 2 weeks ago
Both are supported now :
"Exported as a password-protected PFX file, encrypted using triple DES."

Note : OpenSSL v3 changed default cipher from 3DES to AES256, but this can be overridden on the command line -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -macalg SHA1. OpenSSL v1 uses 3DES as default, so the PFX files generated are supported without any special modifications."

Even if I will be wrong I will answer D at the exam

upvoted 2 times

randy0077 Most Recent 3 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-certificate?tabs=apex%2Crbac%2Cazure-cli#:~:text=from%20the%20internet.-,Private%20certificate%20requirements,custom%20domain%20in%20a%20TLS%20binding%2C%20the%20certificate%20
additional%20requirements%3A

upvoted 1 times

mrt007 9 months ago

To enable HTTPS for the Azure web app, you should first export the private key from the on-premises server and save the key as a PFX file. This is because the private key is required to establish the secure connection. The encryption method can be either TripleDES or AES256, but AES256 is more secure. So, the correct answer is D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256. After that, you can upload this PFX file to your Azure Web App.

upvoted 3 times

TheProfessor 1 year, 1 month ago

OpenSSL v3 changed default cipher from 3DES to AES256, but this can be overridden on the command line -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -macalg SHA1. OpenSSL v1 uses 3DES as default, so the PFX files generated are supported without any special modifications.

upvoted 4 times

ESAJRR 1 year, 3 months ago

Selected Answer: B

B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.

upvoted 1 times

[Removed] 1 year, 3 months ago

Private certificate requirements

The free App Service managed certificate and the App Service certificate already satisfy the requirements of App Service. If you choose to upload or import a private certificate to App Service, your certificate must meet the following requirements:

Exported as a password-protected PFX file, encrypted using triple DES.

https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-certificate?tabs=apex

upvoted 2 times

ITFranz 1 year, 3 months ago

Very surprised about this answer.

I picked AES256 as well.

The answer is right, listed in the documentation. B

upvoted 2 times

alfaAzure 1 year, 4 months ago

Selected Answer: D

Letter D.

When migrating a web app to Azure and continuing to use the same URL with HTTPS (https://www.contoso.com), you will need to configure an SSL certificate for the Azure web app. To do this, you need to export the private key from the on-premises server, create a PFX file containing the private key and the associated public key (certificate), and ensure that it's encrypted using a strong encryption algorithm like AES256.

Once you have the PFX file with the private key and certificate, you can upload and configure the SSL certificate in the Azure web app to enable HTTPS for the domain.

upvoted 2 times

ServerBrain 1 year, 4 months ago

TripleDES all day.

upvoted 1 times

massnonn 1 year, 6 months ago

Yes, Microsoft Azure supports AES-256 encryption for securing data at rest. Azure provides various services that can be used to build web applications, and depending on the specific service you are using, AES-256 encryption can be implemented. For example, if you are using Azure App Service to host your web application, you can enable Azure Storage Service Encryption (SSE) for the underlying storage account. SSE automatically encrypts data at rest using AES-256 encryption. Additionally, you can also implement client-side encryption within your web application to further secure sensitive data before storing it in Azure. It's worth noting that encryption is a multi-layered approach, and while AES-256 is a strong encryption algorithm, it's important to consider other security measures such as access controls, network security, and secure coding practices to ensure a comprehensive security posture for your web application.

upvoted 1 times

Qadour 1 year, 6 months ago

"OpenSSL v3 creates certificate serials with 20 octets (40 chars) as the X.509 specification allows. Currently only 10 octets (20 chars) is supported when uploading certificate PFX files. OpenSSL v3 also changed default cipher from 3DES to AES256, but this can be overridden on the command line. OpenSSL v1 uses 3DES as default and only uses 8 octets (16 chars) in the serial, so the PFX files generated are supported without any special modifications."

Correct Answer for me is D

upvoted 1 times

_fvt 1 year, 5 months ago

No it says exactly that the correct answer is B - Triple DES. Telling you that if you use OpenSSLv3 you can usehttps://www.examtopics.com/exams/microsoft/az-500/view/20/# command-line argument to override the cipher back to 3DES. OR use OpenSSL v1 so that you don't need to change anything.

upvoted 1 times

_fvt 1 year, 5 months ago

Sorry, fixing my comment without the link in the middle...:

No it says exactly that the correct answer is B - Triple DES.

Telling you that if you use OpenSSLv3 you can use command-line argument to override the cipher back to 3DES. OR use OpenSSL v1 so that you don't need to change anything.

upvoted 1 times

Metwally 1 year, 7 months ago

Selected Answer: B

Reference https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-certificate?tabs=apex%2Cportal#private-certificate-requirements

upvoted 1 times

zellck 1 year, 7 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-certificate?tabs=apex%2Cportal#private-certificate-requirements

If you choose to upload or import a private certificate to App Service, your certificate must meet the following requirements:

- Exported as a password-protected PFX file, encrypted using triple DES.

upvoted 2 times

CKR135 1 year, 7 months ago

Selected Answer: B

Exported as a password-protected PFX file, encrypted using triple DES.

upvoted 1 times

Macke53 1 year, 8 months ago

Selected Answer: B

It is still triple DES

Exported as a password-protected PFX file, encrypted using triple DES.

Contains private key at least 2048 bits long

Contains all intermediate certificates and the root certificate in the certificate chain.

https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-certificate?tabs=apex%2Cportal#private-certificate-requirements

upvoted 2 times

majstor86 1 year, 9 months ago

Selected Answer: B

Correction.

B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.

In official documentation only triple DES encryption is supported : https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-certificate?tabs=apex%2Cportal

upvoted 2 times

Question #50 *Topic 3*

You plan to deploy Azure container instances.

You have a containerized application that is comprised of two containers: an application container and a validation container. The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.

You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.

What should you include in the deployment?

A. application security groups

B. network security groups (NSGs)

C. management groups

D. container groups

Suggested Answer: *D*

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

Community vote distribution

D (100%)

wizardoX Highly Voted 2 years, 5 months ago

The answer is correct, as with container groups one can define in which ports those 2 containers should communicate and restrict otherwise.

upvoted 9 times

flafernan Most Recent 7 months, 2 weeks ago

Selected Answer: D

“Container groups” in Azure Container Instances (ACI) allow you to define and deploy multiple containers as a unit. By using a container group, you can ensure that containers within the same group are deployed together and share the same network, allowing them to communicate with each other.

upvoted 4 times

ESAJRR 9 months ago

Selected Answer: D

D. container groups

upvoted 1 times

zellck 1 year, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-container-groups#what-is-a-container-group

A container group is a collection of containers that get scheduled on the same host machine. The containers in a container group share a lifecycle, resources, local network, and storage volumes. It's similar in concept to a pod in Kubernetes.

upvoted 4 times

majstor86 1 year, 3 months ago

Selected Answer: D

D. container groups

upvoted 1 times

ligu 1 year, 4 months ago

Answer is correct

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

Within a container group, container instances can reach each other via localhost on any port, even if those ports aren't exposed externally on the group's IP address or from the container.

Optionally deploy container groups into an Azure virtual network to allow containers to communicate securely with other resources in the virtual network.

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups#networking

upvoted 2 times

⊟ **sleekdunga** 2 years, 4 months ago

D, https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

upvoted 4 times

⊟ **orcnylmz** 1 year, 8 months ago

Here is explanation from document:

Within a container group, container instances can reach each other via localhost on any port, even if those ports aren't exposed externally on the group's IP address or from the container.

upvoted 1 times

⊟ **daluadanilo** 2 years, 5 months ago

i would vote NSG

upvoted 2 times

⊟ **WhalerTom** 2 years, 6 months ago

In exam Dec 21. 40 questions, 1 case study, no labs.

upvoted 2 times

⊟ **o2091** 2 years, 6 months ago

it seems correct, what do you think?

upvoted 1 times

Question #51 *Topic 3*

DRAG DROP -

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

You need to implement VPN gateways for the virtual networks to meet the following requirements:

✑ VNET1 must have six site-to-site connections that use BGP.

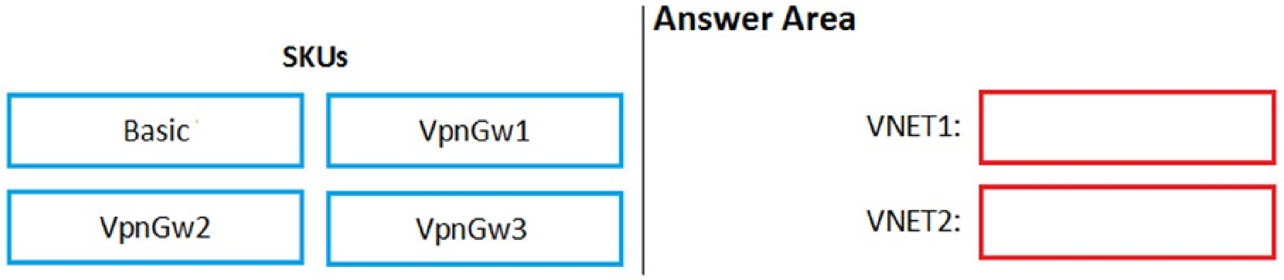
✑ VNET2 must have 12 site-to-site connections that use BGP.

✑ Costs must be minimized.

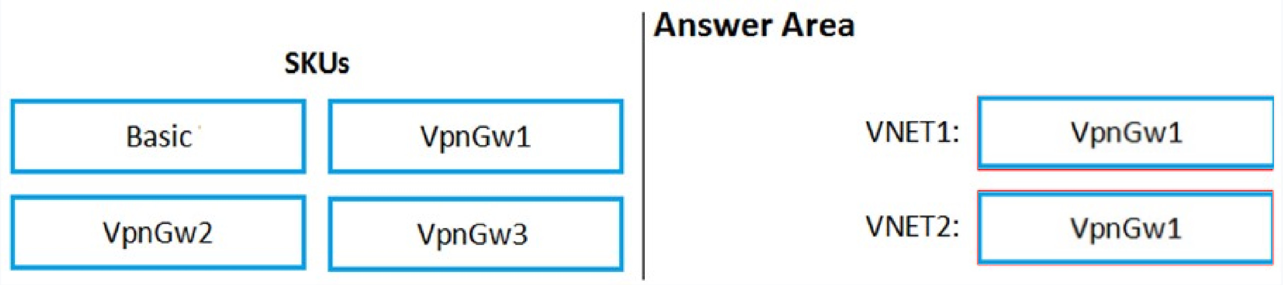
Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



VNET1: VpnGw1

VNET2: VpnGw1

References:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

⊟ **Fred64** Highly Voted 4 years, 2 months ago

in real life, do you kno someone learning things like that for every sazure service?

upvoted 82 times

⊟ **rawrkadia** 3 years, 10 months ago

Thats every certification test I've ever taken. Its a little irritating for Azure where there's a million SKUs and what is supported where is constantly changing but its also not *that* hard to remember basic guidelines like "no BGP on basic sku vpn gateway".

Don't bother retaining it past the test, just cram it in move on.

upvoted 22 times

⊟ **tshamilton** 2 years, 11 months ago

To look at it another way, they're testing your ability to use what you've crammed in a situation where the knowledge can be applied, not just reduce the question to "Hey, do you remember the thing you crammed?"

upvoted 4 times

⊟ **xRiot007** 11 months ago

No, it would be ridiculous to know this stuff by heart when you can google it in 2 minutes.

upvoted 3 times

⊟ **kimalto452** 4 years ago

yes, you for example :D

upvoted 8 times

⊟ **whysohardwhy** 3 years, 12 months ago

"remember they are just exams, don't argue with them"

upvoted 20 times

EM1234 2 years, 7 months ago

I wrote that down so I will remember it.

upvoted 3 times

nihao381 Highly Voted 4 years, 3 months ago

Correct, as BGP is not supported in the Basic SKU.

upvoted 21 times

souvik123 4 years, 2 months ago

Any reference for BGP not supported in Basic SKU?

upvoted 2 times

nicksu 4 years, 1 month ago

Same as below

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Generation1 Basic Max. 10 Max. 128 Not Supported 100 Mbps ->Not Supported<- No

upvoted 3 times

SandroAndrade 4 years, 1 month ago

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

upvoted 2 times

khamrumunnu Most Recent 1 month ago

Final Answer is vpngW1 and vpngw1

https://azure.microsoft.com/en-us/pricing/details/vpn-gateway/

VpnGw1 $138.70/month 650 Mbps Max 30

1-10: Included

11-30: $0.015/hour per tunnel Max 250

1-128: Included

129-250: $0.01/hour per connection

upvoted 1 times

khamrumunnu 1 month ago

Final Answer:

VNET1 → VpnGw1

VNET2 → VpnGw2

SKU Max S2S Connections BGP Support Cost (Relative)

Basic 0 No Cheapest

VpnGw1 10 Yes Low

VpnGw2 30 Yes Medium

VpnGw3 30 Yes High

upvoted 1 times

pentium75 11 months ago

How is that related to security?

upvoted 2 times

datz 1 year ago

this should be under AZ700, not 500zzz

upvoted 2 times

flafernan 1 year, 7 months ago

When you use BGP (Border Gateway Protocol) over a VPN connection in Azure, you gain benefits such as support for custom routing policies, making network configuration and management more efficient and flexible. BGP enables the dynamic exchange of routing information between your on-premises network and the Azure virtual network. Instead of having to manually configure static routes, BGP automates updating routing tables.

VPN gateway SKUs take into account the number of connections and throughput. Below are some examples of the dozens of G. VPN SKU possibilities.

a) Basic SKU – Max 10 S2S tunnels – 100 Mbps – single without any BGP support.

b) SKU VpnGw1 – Max 30 S2S tunnels – 650 Mbps – with BGP support.

c) SKU VpnGw2 – Max 30 S2S tunnels – 1 Gbps – with BGP support.

d) SKU VpnGw3 – Max 30 S2S tunnels – 1.25 Gbps – with BGP support

upvoted 6 times

ESAJRR 1 year, 9 months ago

1. VpnGw1

1. VpnGw1

upvoted 1 times

zellck 2 years, 1 month ago

1. VpnGw1

1. VpnGw1

https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#benchmark

SKU - VpnGw1

S2S/VNet-to-VNet Tunnels - Max. 30

upvoted 3 times

zellck 2 years, 1 month ago

Typo.

1. VpnGw1
2. VpnGw1

upvoted 2 times

majstor86 2 years, 3 months ago

VNET1: VpnGw1

VNET2: VpnGw1

upvoted 2 times

ltjones12 2 years, 6 months ago

Memorizing SKUs that constantly change every few months. Makes perfect sense to include this on a test :)

upvoted 3 times

baloum 3 years ago

Correct, as BGP is not supported in the Basic SKU.

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

upvoted 2 times

Eltooth 3 years, 3 months ago

Correct - VpnGw1 is minimum SKU that allows upto 10 S2S VPNs.

upvoted 2 times

mahi83 3 years, 6 months ago

Correct:

VpnGw1 $0.19/hour 650 Mbps Max 30

1-10: Included

11-30: $0.015/hour per tunnel Max 250

1-128: Included

129-250: $0.01/hour per connection

upvoted 5 times

GQ 3 years, 9 months ago

If this really come up for my exam, i will rage -.-

upvoted 6 times

cosine 3 years, 9 months ago

Not only VpnGw1.

VpnGw2 and VpnGw3 can be the correct answer as well.

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

upvoted 1 times

hazard74 3 years, 9 months ago

"cost must be minimize"

upvoted 12 times

⊟ **Cyberbug2021** 4 years, 2 months ago

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

upvoted 1 times

Question #52 *Topic 3*

You are securing access to the resources in an Azure subscription.
A new company policy states that all the Azure virtual machines in the subscription must use managed disks.
You need to prevent users from creating virtual machines that use unmanaged disks.
What should you use?

A. Azure Monitor

B. Azure Policy

C. Azure Security Center

D. Azure Service Health

Suggested Answer: *B*

Community vote distribution

B (100%)

JohnYinToronto Highly Voted 👍 3 years, 3 months ago

answer correct

upvoted 34 times

alfaAzure Highly Voted 👍 10 months ago

Selected Answer: B

B. Azure Policy

To prevent users from creating virtual machines that use unmanaged disks in an Azure subscription, you should use Azure Policy. Azure Policy allows you to define and enforce rules for resource properties during resource creation and updates. In this case, you can create a custom policy that enforces the use of managed disks for virtual machines and assign it to your subscription. This way, any attempt to create a virtual machine with unmanaged disks would be denied based on the policy.

upvoted 6 times

ESAJRR Most Recent 9 months ago

Selected Answer: B

B. Azure Policy

upvoted 2 times

zellck 1 year, 1 month ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
zure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 2 times

majstor86 1 year, 3 months ago

Selected Answer: B

B. Azure Policy

upvoted 2 times

F117A_Stealth 1 year, 7 months ago

Selected Answer: B

B. Azure Policy

upvoted 1 times

Amit3 1 year, 11 months ago

B. Azure Policy.

upvoted 2 times

Alessandro365 2 years ago

Selected Answer: B

B is correct answer.

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 3 times

WhalerTom 2 years, 6 months ago

In exam Dec 21. 40 questions, 1 case study, no labs.

upvoted 2 times

Sandomj55 2 years, 10 months ago

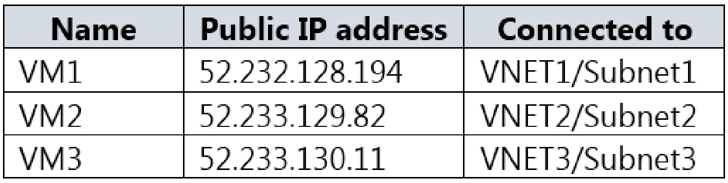
In Exam 8/4/2021

upvoted 4 times

Question #53 *Topic 3*

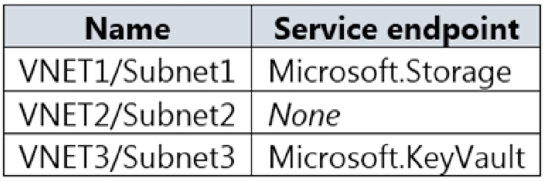
HOTSPOT -

You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.



Name	Public IP address	Connected to
VM1	52.232.128.194	VNET1/Subnet1
VM2	52.233.129.82	VNET2/Subnet2
VM3	52.233.130.11	VNET3/Subnet3

The virtual network subnets have service endpoints defined as shown in the following table.



Name	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET2/Subnet2	*None*
VNET3/Subnet3	Microsoft.KeyVault

You configure the following Firewall and virtual networks settings for storage1:

✑ Allow access from: Selected networks

✑ Virtual networks: VNET3\Subnet3

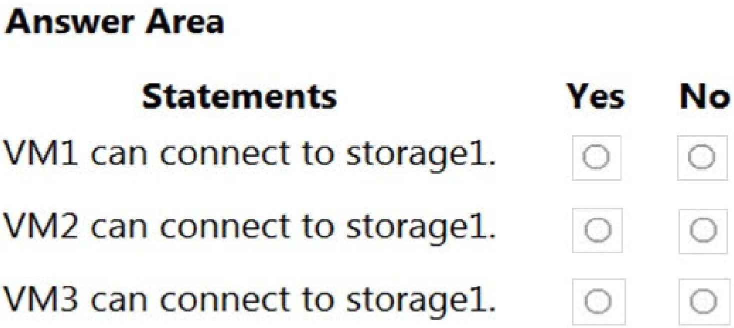
Firewall `" Address range: 52.233.129.0/24

▪

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

NOTE: Each correct selection is worth one point.

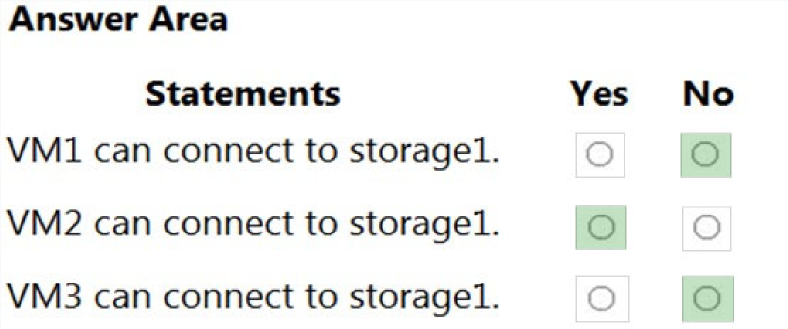
Hot Area:



Answer Area

Statements	Yes	No
VM1 can connect to storage1.	○	○
VM2 can connect to storage1.	○	○
VM3 can connect to storage1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
VM1 can connect to storage1.	○	[✓ ○]
VM2 can connect to storage1.	[✓ ○]	○
VM3 can connect to storage1.	○	[✓ ○]

Box 1: No -

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Box 2: Yes -

VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.

Box 3: No -

Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

Elazari Highly Voted 3 years, 9 months ago

No, Yes, Yes (TESTED)
VM 1 cannot connect to the storage account, service point to the storage it's not enough - should be in the selected networks too.
VM2 can connect to the storage - no service endpoint = using his public IP, his public IP in the firewall allowed network.
VM3 can connect to the storage - at the moment you register the subnet to the storage selected network, you have also to enable a service end point to the storage.
upvoted 51 times

palanto 3 years, 6 months ago
Hi Elazari, Thanks for testing the scenario at lab.
Need clarification in your 3rd point, ("you have also to enable a service end point to the storage."), Looks you have enabled Service endpoint Vnet3/subnet3 to storage, However this is not the given requirement. Should we consider the answer as 'NO' for 3rd question (VM3 can connect to Storage1?)
upvoted 7 times

somenick 2 years, 8 months ago
No, Yes, No (Really tested)
Here is how I tested:
Step 1) Storage1 without any network exceptions - all blocked. Result: VM3 can't access storage
Step 2) I added subnet3 to the whitelist on Storage1. Storage service endpoint is added to the subnet3 automatically. Result: VM3 can access Storage1.
Step 3) I removed Storage endpoint from subnet3 and added KeyVault endpoint instead as described in the question. Result: VM3 can't access Storage1
upvoted 14 times

j410aksl 3 years, 9 months ago
Weird that Azure would go against its own documentation:
"IP network rules can't be used in the following cases:

To restrict access to clients in same Azure region as the storage account.

IP network rules have no effect on requests originating from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests.

To restrict access to clients in a paired region which are in a VNet that has a service endpoint.

To restrict access to Azure services deployed in the same region as the storage account.

Services deployed in the same region as the storage account use private Azure IP addresses for communication. Thus, you can't restrict access to specific Azure services based on their public outbound IP address range."
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal
upvoted 3 times

BP_lobster 3 years, 2 months ago
The test was likely run with VM2 outside the Azure Region that our storage account sat within. Will try to remember to verify this after the exam/post my results below.
upvoted 1 times

mung 2 years, 7 months ago
Guys don't fall for this answer.
I'm pretty sure that this guy set the lab with incorrect setting.

It looks like he configured the Service EP with Storage not with keyvault.

It have to be N,Y,N.
Without Service EP set to Storage, you can't connect to the storage
upvoted 25 times

mung 2 years, 7 months ago
IP is not even in range lol.
upvoted 1 times

pentium75 11 months ago

Well, yeah. You could connect with Service EP if the subnet was listed (it is but the EP is missing), OR you could connect without Service EP (to the public endpoint but that doesn't work because the IP is not listed).

upvoted 1 times

gc12345 3 years, 4 months ago

VM3 can connect to the storage - at the moment you register the subnet to the storage selected network, ---Correct . service EP configured for key vault at VNET3 .so its not affect storage access.

upvoted 4 times

gcpbrig01 Highly Voted 4 years, 3 months ago

Answers are correct. Virtual network service end point configuration should always be done with network access configuration for the same virtual network from the service end-here storage. Either that or allow the public IP address of the VM that wants to connect to the storage account in the firewall section of the storage account.

upvoted 28 times

rgullini 4 years, 2 months ago

Agree with you. Answers are correct

upvoted 2 times

intimidator 3 years, 10 months ago

Isn't a new Service endpoint created automatically once you whitelist a subnet on the Storage account firewall?

upvoted 3 times

hmghmg 4 years, 2 months ago

Yes, but not on the same Azure region.

The answer is: NO,NO,NO

upvoted 4 times

[Removed] 3 years, 11 months ago

It's stated on the HOTSPOT :

The storage account and virtual machines are in the same Azure region.

upvoted 4 times

rgullini 4 years, 2 months ago

To access from a VNET to a storage account without using the public IP space, you need both: a rule and a service endpoint

Point 1: There is a SERVICE endpoint configured for VNET1. However, the rule does not allow the internal nor the Public IP

Point 2: No endpoint so public IP is used which is allowed by the rule

Point 3: Rule allows the VNET3 but there is no Service Endpoint. The public IP is not allowed

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

Section: Grant access from a virtual network

upvoted 21 times

flafernan Most Recent 1 year, 7 months ago

NO, YES, NO

a) After configuring a "service endpoint" in a VNET, directing to Azure Storage for example, access will still not be possible, as it will be necessary to configure Azure Storage, allowing access from the VNET, that is, there must be permissions on both sides.

b) In a second example in which a permission is created in Storage that allows access to an IP range 10.20.30.0/24, and a VNET that is in that same range (10.20.30.52), even if the VNET does not have service configured endpoint, access will be possible, as its IP is already on a Storage whitelist.

c) In a third example where the storage already allows a VNET, but the service endpoint is not configured, access will not be possible. Access must be configured at two ends. The exception is what was mentioned in letter "b)", as the storage allows the IP range in which the VNET belongs.

upvoted 7 times

[Removed] 1 year, 7 months ago

No Yes Yes, as soon as you add a VNET you get the following message

The following networks don't have service endpoints enabled for 'Microsoft.Storage'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait.

So there is no way you can add a VNET in the firewall list and not have a service endpoint enabled the question itself is wrong if they are not showing the service end point this has been tested in lab.

upvoted 3 times

[Removed] 1 year, 6 months ago

Correcting answer its NO YES NO, if I delete the service end point after adding the VNET the access will go away

upvoted 1 times

⊟ **wardy1983** 1 year, 8 months ago

Box 1: No -

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Box 2: Yes -

VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.

Box 3: yes

VM3 can connect to the storage - at the moment you register the subnet to the storage selected network, you have also to enable a service end point to the storage.

upvoted 2 times

⊟ **foobar1985** 1 year, 9 months ago

Formula: ($is_Service_enpoint_in_VNET && $is_VNET_in_Selcted_network) || $is_PIP_in_Firewall_range

BOX1: NO. (TRUE && FALSE) || FALSE -> FALSE

BOX2: YES. (FALSE && FALSE) || TURE -> TURE

BOX3: NO. (TURE && FALSE) || FALSE

upvoted 3 times

⊟ **heatfan900** 1 year, 10 months ago

n, n, y

VM1 is not in the ALLOWED VNET list and their PUBLIC IP is not allowed either

VM2 is not in the ALLOWED VNET list but their PUBLIC IP falls within the range of allowed

VM3 is in the ALLOWED VNET and its PUBLIC IP is not required to connect to the SA. The explanation here is wrong. The SERVICE ENDPOINT is configured from the NETWORK SETTINGS on the SA. If the SA can see the VNET/SUBNET and is allowing it then the VNET/SUBNET then it can obviously connect to it.

upvoted 2 times

⊟ **heatfan900** 1 year, 10 months ago

I meant n, y, y

upvoted 1 times

⊟ **_fvt** 1 year, 11 months ago

N-N-N.

Explanation is correct: Box 1: No -

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Incorrect: Box 2: No, you cannot filter access with public IP of Azure services deployed in the same region as the storage account.
(https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range)

Explanation is correct: Box 3: No -

Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

upvoted 2 times

⊟ **_fvt** 1 year, 10 months ago

N-N-Y. Managed to test it in LAB.

The change concerns the Box 3: answer is Yes.

When you select VNET3\Subnet3, "(Service endpoint required)" will be added after the name of the selected Subnet, and show a disclaimer about the time required to enable the service endpoint..

So the service Endpoint is automatically created when you select subnet which needs it.

upvoted 2 times

⊟ **_fvt** 1 year, 11 months ago

("Services deployed in the same region as the storage account use private Azure IP addresses for communication. So, you can't restrict access to specific Azure services based on their public outbound IP address range.")

upvoted 1 times

⊟ **_fvt** 1 year, 11 months ago

For the box 3 I am unsure as https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range says:

"IP network rules have no effect on requests that originate from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests."

So maybe that will works...
upvoted 1 times

⊟ **zellck** 2 years, 1 month ago
NNY is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range
You can't use IP network rules in the following cases:
- To restrict access to Azure services deployed in the same region as the storage account.
Services deployed in the same region as the storage account use private Azure IP addresses for communication. So, you can't restrict access to specific Azure services based on their public outbound IP address range.
upvoted 3 times

⊟ **ITTesters** 2 years, 1 month ago
NNY;
first; subnet is not added to allowed virtual networks

second; Public ip range is on the allowed list, but is blocked due being in the same region (https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range)

third; the case starts with only a keyvault endpoint, but when adding Subnet3 to the allowed virtual networks, an service endpoint needs to be added to the subnet, after you click "enable" you can continue to add the subnet to the allow list.
upvoted 3 times

⊟ **mssii** 2 years, 3 months ago
Service endpoints are not mandatory to route traffic
You can configure storage accounts to allow access only from specific subnets. The allowed subnets may belong to a VNet in the same subscription, or those in a different subscription, including subscriptions belonging to a different Azure Active Directory tenant.

You can enable a Service endpoint for Azure Storage within the VNet. The service endpoint routes traffic from the VNet through an optimal path to the Azure Storage service.
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal
upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago
NO
YES
NO
upvoted 3 times

⊟ **samimshaikh** 2 years, 5 months ago
Tested in LAB:

The following networks don’t have service endpoints enabled for 'Microsoft. Storage'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait. NYY
upvoted 2 times

⊟ **Muaamar_Alsayyad** 2 years, 8 months ago
N - service endpoint configured but Subnet1 is not added to selected network
Y - through public IP
N - subnet3 added to slected networks but servide endpoint is not configured
upvoted 3 times

⊟ **arseyam** 2 years, 8 months ago
Service endpoints are used to create a shorter route to direct traffic through Microsoft network not through the internet.
You still need to whitelist the IP address of the source machine to access the storage account so the real reason 1 & 3 are No is because of the

non IP whitelisting in the storage account firewall.

upvoted 1 times

⊟ **bugimachi** 2 years, 7 months ago

No, this is wrong. When enable service endpoints, you will still need to allow the originating VNet to access the storage account, but whitelisting the IP is definitely not required.

upvoted 1 times

⊟ **Pasmo** 2 years, 10 months ago

Correct Answer: No Yes No

upvoted 2 times

⊟ **randomaccount123** 2 years, 11 months ago

I originally thought it was NYN. However I've just realized it says the storage account and VM are in the same region, therefore the firewall don't actually take affect. So its actually NNN.

upvoted 3 times

⊟ **Amit3** 2 years, 11 months ago

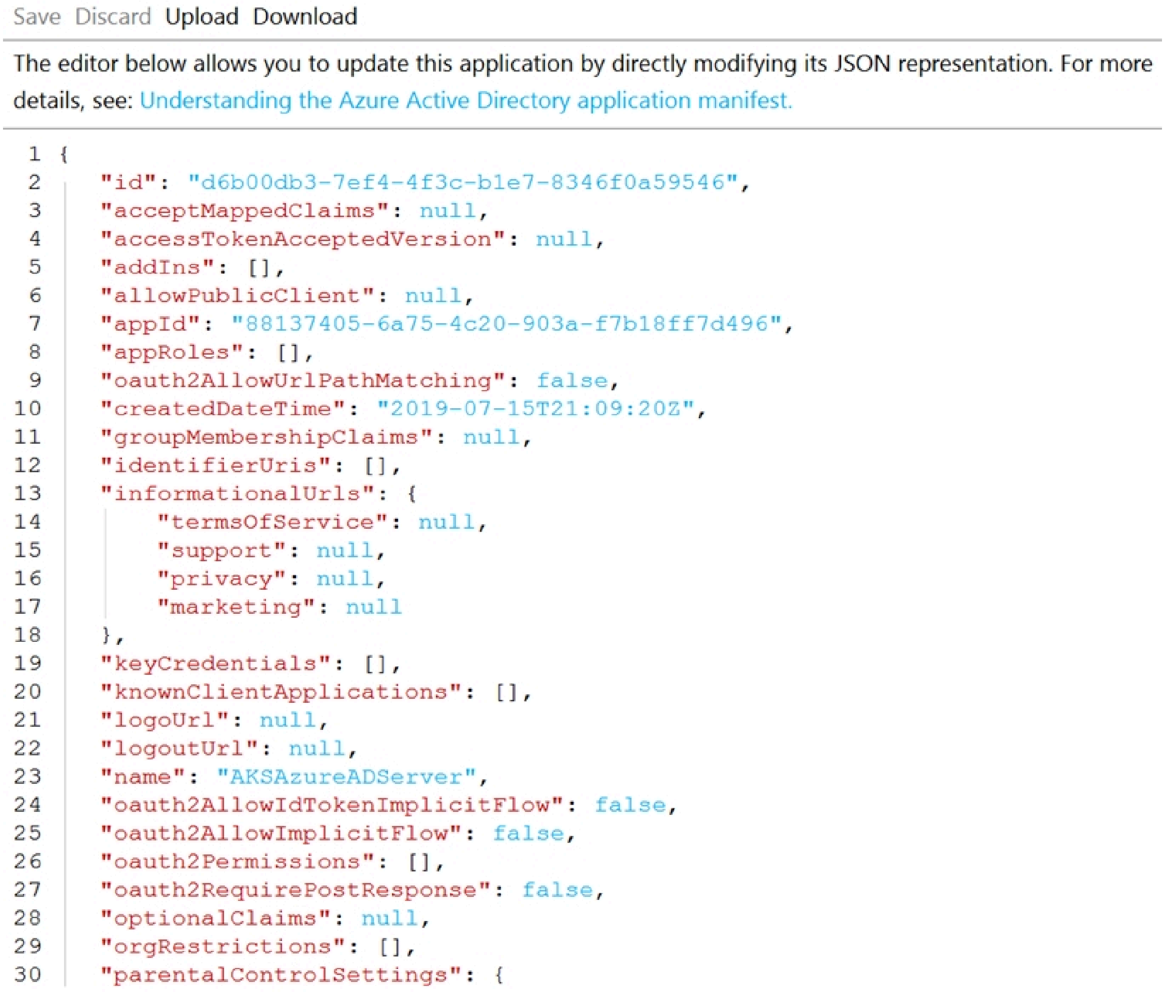
Answer should N,Y,N because for VNet3 there is no service end-point configured. We need to answer based on information given in questions, without making any assumptions.

upvoted 1 times

Question #54 Topic 3

You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription.

The manifest of the registered server application is shown in the following exhibit.



The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

```
{
    "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-07-15T21:09:20Z",
    "groupMembershipClaims": null,
    "identifierUris": [],
    "informationalUrls": {
        "termsOfService": null,
        "support": null,
        "privacy": null,
        "marketing": null
    },
    "keyCredentials": [],
    "knownClientApplications": [],
    "logoUrl": null,
    "logoutUrl": null,
    "name": "AKSAzureADServer",
    "oauth2AllowIdTokenImplicitFlow": false,
    "oauth2AllowImplicitFlow": false,
    "oauth2Permissions": [],
    "oauth2RequirePostResponse": false,
    "optionalClaims": null,
    "orgRestrictions": [],
    "parentalControlSettings": {
```

You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated.

Which property should you modify in the manifest?

A. accessTokenAcceptedVersion

B. keyCredentials

C. groupMembershipClaims

D. acceptMappedClaims

Suggested Answer: *C*

Reference:

https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications

Community vote distribution

C (100%)

dadageer Highly Voted 3 years, 3 months ago

# Create the Azure AD application

serverApplicationId=$(az ad app create \

--display-name "${aksname}Server" \

--identifier-uris "https://${aksname}Server" \

--query appId -o tsv)

# Update the application group membership claims

az ad app update --id $serverApplicationId --set groupMembershipClaims=All

upvoted 21 times

Deepmindx Highly Voted 👍 3 years ago

### IN EXAM ### 29/6/2021

upvoted 18 times

ESAJRR Most Recent 9 months ago

Selected Answer: C

C. groupMembershipClaims

upvoted 1 times

zellck 1 year, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/aks/azure-ad-integration-cli#create-azure-ad-server-component
To integrate with AKS, you create and use an Azure AD application that acts as an endpoint for the identity requests. The first Azure AD application you need gets Azure AD group membership for a user.

Create the server application component using the az ad app create command, then update the group membership claims using the az ad app update command.
# Update the application group membership claims
az ad app update --id $serverApplicationId --set groupMembershipClaims=All

upvoted 4 times

majstor86 1 year, 3 months ago

Selected Answer: C

C. groupMembershipClaims
outdated

upvoted 1 times

OrangeSG 1 year, 5 months ago

Selected Answer: C

The question is outdated.

Reference
Integrate Azure Active Directory with Azure Kubernetes Service using the Azure CLI (legacy)
https://learn.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

**The feature described in this document, Azure AD Integration (legacy), will be deprecated on June 1st, 2023.

AKS has a new improved AKS-managed Azure AD experience that doesn't require you to manage server or client application

upvoted 7 times

F117A_Stealth 1 year, 7 months ago

Selected Answer: C

Select Manifest, and then edit the groupMembershipClaims: value as "All". When you're finished with the updates, select Save.

upvoted 2 times

JohnYinToronto 3 years, 3 months ago

answer correct

upvoted 4 times

gcpbrig01 3 years, 3 months ago

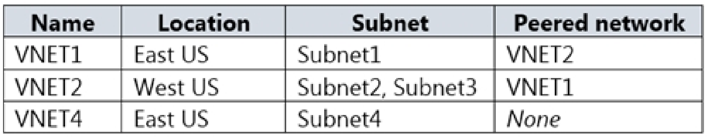
groupMembershipClaims should be set to "All"

upvoted 9 times

Question #55 *Topic 3*

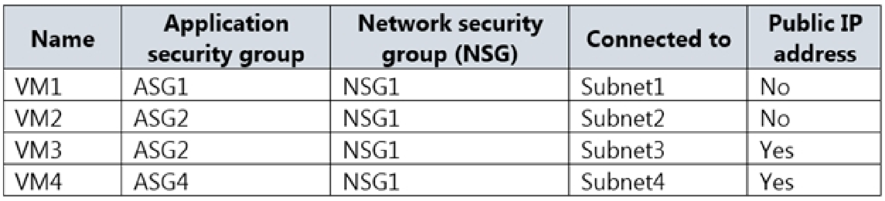
HOTSPOT -

You have the Azure virtual networks shown in the following table.



Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet2, Subnet3	VNET1
VNET4	East US	Subnet4	*None*

You have the Azure virtual machines shown in the following table.

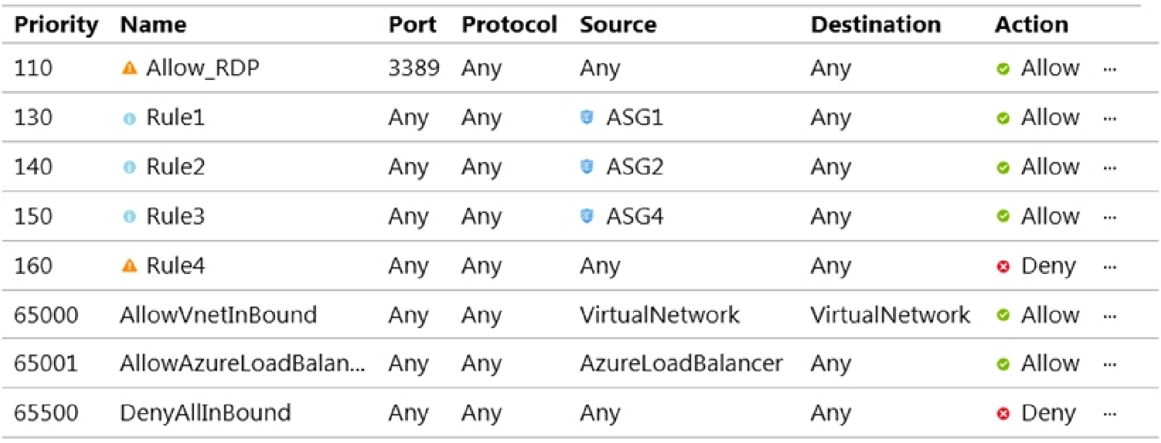


Name	Application security group	Network security group (NSG)	Connected to	Public IP address
VM1	ASG1	NSG1	Subnet1	No
VM2	ASG2	NSG1	Subnet2	No
VM3	ASG2	NSG1	Subnet3	Yes
VM4	ASG4	NSG1	Subnet4	Yes

The firewalls on all the virtual machines allow ping traffic.

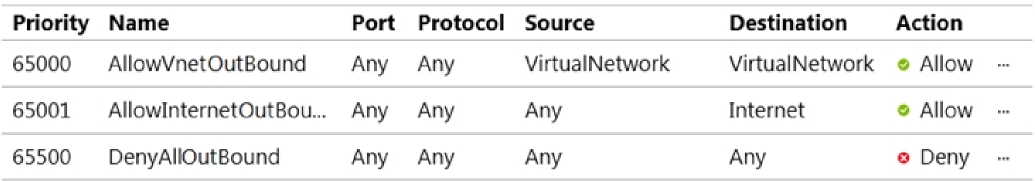
NSG1 is configured as shown in the following exhibit.

Inbound security rules -



Priority	Name	Port	Protocol	Source	Destination	Action	
110	⚠ Allow_RDP	3389	Any	Any	Any	✓ Allow	...
130	Rule1	Any	Any	ASG1	Any	✓ Allow	...
140	Rule2	Any	Any	ASG2	Any	✓ Allow	...
150	Rule3	Any	Any	ASG4	Any	✓ Allow	...
160	⚠ Rule4	Any	Any	Any	Any	✖ Deny	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	✖ Deny	...

Outbound security rules -

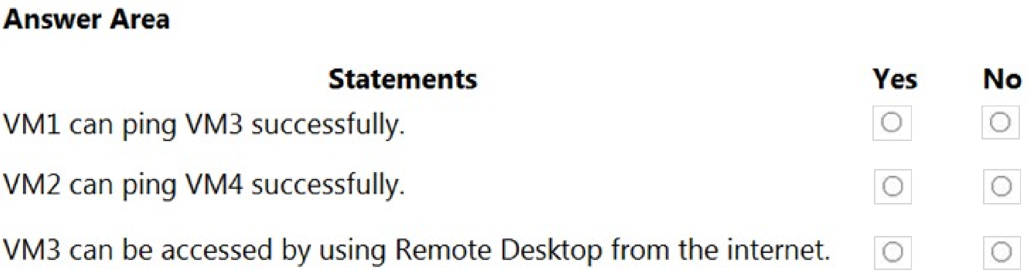


Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowInternetOutBou...	Any	Any	Any	Internet	✓ Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	✖ Deny	...

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

NOTE: Each correct selection is worth one point.

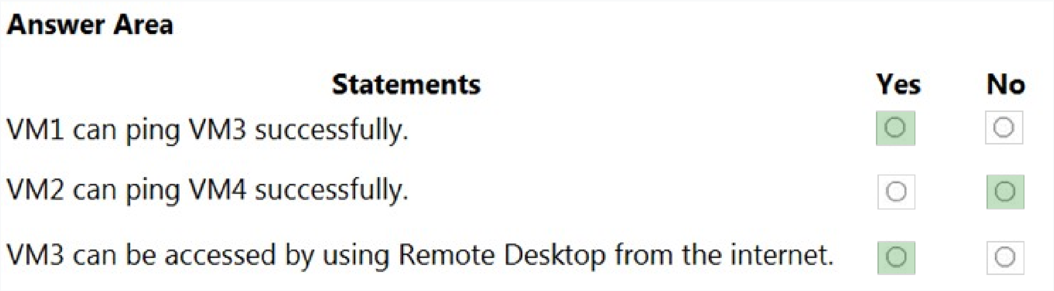
Hot Area:



Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	●	○
VM2 can ping VM4 successfully.	○	●
VM3 can be accessed by using Remote Desktop from the internet.	●	○

Box 1: Yes -

VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow 'any' traffic on 'any' protocol so pings are allowed between VM1 and VM3.

Box 2: No -

VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don't go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.

Box 3: Yes -

VM3 has a public IP address and the firewall allows traffic on port 3389.

gcpbrig01 Highly Voted 4 years, 3 months ago

Suggested answers are correct. VMs if not in peered network, need public ip address to communicate with each other backed up firewall rules that allow access.

upvoted 40 times

rgullini 4 years, 2 months ago

Agree with your comments and the answers.

upvoted 2 times

Cyberbug2021 4 years, 1 month ago

Peered yes but what about rule 160 - any any deny

upvoted 1 times

BalderkVeit 4 years, 1 month ago

Nothing.
box 1 - peering available, rule 130 will allow, so it's yes
box 2 - no peering between vnets, so it's no
box 3 - RDP is allowed, and it has Public IP, so it's yes.

upvoted 29 times

makimaki 2 years, 9 months ago

I think the box 2 should be yes.
VM4 needs not to send packets as a source.
Just replying to packets from VM2 will do.
In this case, VM4 can reply without the VM2 public IP address.

upvoted 2 times

pentium75 11 months ago

The VNets are not peered and we don't know if the machines have public IPs at all.

upvoted 1 times

AMMANANA Highly Voted 4 years, 1 month ago

Answer is YES, YES,YES
1) Since Rule1 allows all traffic from the source of ASG1 and demovm1 is part of ASG1, ICMP traffic would be allowed.
2) Since Rule3 allows all traffic from the source of ASG4 and demovm4 is part of ASG4, ICMP traffic would be allowed.
3) Since demovm3 has a public IP address and the Allow_RDP rule is in place, you can go ahead and connect to the machine from the Internet via Remote Desktop.

upvoted 12 times

CJ32 3 years, 5 months ago

VM2 and VM4 are not peered therefore the traffic would have to go over the internet. VM2 doesnt have a public IP so the traffic ends there

upvoted 8 times

nicksu 4 years, 1 month ago

There is no peering between VNET2 & VNET4. The VM4 does have the PIP, but the ICMP from Internet is not allowed

upvoted 8 times

[Removed] Most Recent 11 months ago

Is this question valid?

1. Can we associate NSG with multiple VMs from different regions?

2. Can we even associate single NSG with multiple VMs from separate VNETs?

upvoted 2 times

bxlin 1 year, 1 month ago

First of above, VM1 and VM4 are in East US, VM2 and VM3 are in West US. It is not possible to attach NSG1 to all the VMs at the same time. VM and NSG must be in the same region.

upvoted 2 times

bxlin 1 year, 1 month ago

therefore, this question makes no sense.

upvoted 2 times

flafernan 1 year, 7 months ago

In Azure, pings go out through the default gateway, I just tested it. So the answer is:

Y-Y-Y

upvoted 1 times

cris_exam 1 year, 5 months ago

What are you talking about man? a link to sustain what you said that would be nice.

Until then, my Az Network experience and tests show that, pings are just the same as any other network traffic/commands that flows, that is: if allowed OR if there is a network route path to be able to flow.

The default gateway if perhaps is what you are trying to say here, could be referring to the External SDN Load Balancers that are set up for outbound/inbound Internet communication with any given VM and other resource, but it would not be called default gateway, OR perhaps it could be a NAT GW configured instead of LB. Here's a link for reading if anyone is interested, on the left side there are several other concepts explained about how internet inbound/outbound work when having and not having a public IP attached, it's a nice read.
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/default-outbound-access

BTW, the given answers are correct: Y N Y

upvoted 2 times

foobar1985 1 year, 9 months ago

in exam 11/09/2023

upvoted 4 times

majstor86 2 years, 3 months ago

YES
NO
YES

upvoted 4 times

mung 2 years, 7 months ago

I though ASG is for only web app not the regular network traffic.

I think when you send an ICMP, it shouldn't have any business with ASG.. So N N Y?

upvoted 1 times

mung 2 years, 7 months ago

Nevermind i was wrong

upvoted 1 times

mung 2 years, 7 months ago

*thought

upvoted 1 times

⊟ **CK9797** 2 years, 7 months ago

Passed exam 04/11/22

40 Questions
1 Case Study = 6 Questions
1 Lab = 10 Tasks - You need to be comfortable navigating in Azure
Total 56 Questions
Some new questions, most are from this site. Big thank you to Exam Topics and everyone for their comments. Rule of thumb, go with the most votes.

upvoted 4 times

⊟ **acexyz** 2 years, 12 months ago

# IN EXAM - 30/6/2022

upvoted 5 times

⊟ **WMG** 3 years, 2 months ago

You cannot ping outside of Azure without a public IP address. ICMP works on layer 3. When you don't associate a Public IP address to a VM, when it initiates an outbound connection to Internet, it does a SNAT with a Psudorandom VIP. Since ICMP doesn't have a port, it gets dropped by the platform.

upvoted 3 times

⊟ **Eltooth** 3 years, 3 months ago

Yes, No, Yes

upvoted 6 times

⊟ **azcourse** 3 years, 8 months ago

answer is .y.y.y
Since Rule3 allows all traffic from the source of ASG4 and demovm4 is part of ASG4, ICMP traffic would be allowed

upvoted 2 times

⊟ **SecurityAnalyst** 3 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 5 times

⊟ **rsharma007** 3 years, 10 months ago

1. First check whether the Layer 3 or routing exists between source and destination.
2. Check whether NSG policy allows the flow.

As per NSG, RDP from any source is allowed inbound and everything else is denied(other allows are from ASGs which are private). VNET to VNET is allowed.

VM1 and VM3 are peered VNETs. Routing exist and hence will use their private IPs which are allowed.
VM2 and VM4 are not peered and hence will be denied.

upvoted 3 times

⊟ **Sandomj55** 3 years, 10 months ago

In Exam 8/4/2021

upvoted 2 times

⊟ **hydrillo** 4 years ago

Tricky question. It say that all vms allow ping traffic. Nothing is mentioned about rdp. So one should assume that rdp is blocked.

upvoted 2 times

⊟ **j410aksl** 3 years, 9 months ago

Port 3389 is the RDP port.

upvoted 2 times

⊟ **ITTesters** 2 years, 1 month ago

On the NSG it is, but the case mentions that ICMP is open on the VM firewall, but does not mention 3389/RDP is open/enabled on the VMs.

upvoted 1 times

Question #56 *Topic 3*

You have multiple development teams that will create apps in Azure.
You plan to create a standard development environment that will be deployed for each team.
You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.
What should you include in the recommendation?

A. an Azure policy

B. an Azure Resource Manager template

C. a management group

D. an Azure blueprint

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

Community vote distribution
D (69%) A (23%) 8%

⊟ **sadako** Highly Voted 3 years, 7 months ago
D: Azure Blueprint

Reference: "How blueprint locks work"
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking
upvoted 29 times

⊟ **cfsxtuv33** 3 years, 6 months ago
Thank you for the link. It seems the answer is correct once I looked at the link, originally I thought it was Policy as it makes sense. "The creation of consistent environments at scale is only truly valuable if there's a mechanism to maintain that consistency. This article explains how resource locking works in Azure Blueprints."
upvoted 3 times

⊟ **cfsxtuv33** 3 years, 6 months ago
Sorry, the link from "sadako" explains this.
upvoted 1 times

⊟ **mrfallacy** Highly Voted 3 years, 8 months ago
Sounds like an Azure Resource Manager (ARM) Template makes the most sense in this case. It allows for the consistency needed for the locks without manually creating locks each time for each of the standard development environments. Also, since they're all standard development environments, they will most likely be the same for each team.
upvoted 7 times

⊟ **khamrumunnu** Most Recent 1 month ago
Selected Answer: D
The correct answer is: D. an Azure blueprint

Azure Blueprints are designed specifically to help you orchestrate the deployment of various Azure resources and configurations in a repeatable, consistent, and governed manner. This includes:

Resource locks (e.g., CanNotDelete, ReadOnly)
Role assignments
Policy assignments
ARM templates

Why the others are not ideal for this scenario:
A. Azure policy
Azure Policy is excellent for enforcing rules (like tagging, allowed SKUs, regions) but does not create or enforce resource locks directly.

B. Azure Resource Manager template

ARM templates can deploy resources and locks, but do not enforce governance or standardization across multiple environments the way Blueprints do.

C. Management group

A management group helps organize and apply policies at scale, but does not create or enforce resource locks directly.

upvoted 1 times

golitech 4 months, 4 weeks ago

Selected Answer: D

Azure Blueprints are designed to help you set up and enforce a repeatable set of resources and policies that are applied consistently across multiple environments. Blueprints can include Azure Policy, Resource Manager templates, Role-Based Access Control (RBAC) assignments, and resource locks.

In this case, the requirement is to enforce resource locks consistently across development environments. Azure Blueprints can include the configuration of resource locks, ensuring that the locks are consistently applied every time a new environment is deployed for each team.

upvoted 1 times

153a793 8 months, 1 week ago

i would go with "A".

ARM and blue print provides the options, but when it comes to enforcement it is "policy". Policy with ARM or blue print. Consider if someone created resources without using available ARM or bluprint option.

upvoted 1 times

gen33 1 year, 6 months ago

Today Azure Resource Manager (ARM) Template is the best choice to achieve this

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json

upvoted 3 times

elster 1 year, 2 months ago

Correct, Blueprints will be even deprecated as stated in this link https://learn.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking#how-blueprint-locks-work

upvoted 2 times

flafernan 1 year, 7 months ago

Selected Answer: D

112. Azure Blueprint has the ability to create a standard and replicable ENVIRONMENT, including resources, policies, Locks, role assignments, and other configurations. The doubt that may arise is regarding the use of Azure Police, which in theory would have the same properties. To help you decide which one to use, just remember that Azure Police works at the subscription level, resource group, or individual resources, more globally. Azure Blueprint is aimed at a specific environment, such as a DEV environment, which can be replicated to another DEV team. So when the issue involves standardizing consistent environments, the ideal is to choose the use of Azure Blueprint.

upvoted 5 times

ESAJRR 1 year, 9 months ago

Selected Answer: D

D. an Azure blueprint Most Voted

upvoted 1 times

_fvt 1 year, 10 months ago

I would go for D (blueprints).

"You plan to create a standard development environment that will be deployed for each team." so you will probably use blueprint.

Using blueprints resource locks in that case is great because "you can protect newly deployed resources from being tampered with, even by an account with the Owner role".

https://learn.microsoft.com/en-us/azure/governance/blueprints/tutorials/protect-new-resources

But if you use another deployment method for environment, or if developers have to create resources which will need to have enforced resources locks, then you will need to use azure policies, as blueprint resource locks only applies on New resources deployed by the blueprint

https://learn.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking.

upvoted 1 times

Ario 1 year, 12 months ago

Selected Answer: D

Correct Answer: D

upvoted 1 times

⊟ **zellck** 2 years, 1 month ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

The creation of consistent environments at scale is only truly valuable if there's a mechanism to maintain that consistency. This article explains how resource locking works in Azure Blueprints.

upvoted 2 times

⊟ **zellck** 2 years, 1 month ago

D is the answer.

https://learn.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

The creation of consistent environments at scale is only truly valuable if there's a mechanism to maintain that consistency. This article explains how resource locking works in Azure Blueprints.

upvoted 2 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: D

D. an Azure blueprint

upvoted 4 times

⊟ **Fal991l** 2 years, 4 months ago

Selected Answer: A

AI: To enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner, I would recommend using an Azure Policy.

Azure Policy allows you to enforce organizational standards and ensure compliance with corporate governance policies. You can use Azure Policy to define and enforce resource locks for all resources within a specified scope. Resource locks can help prevent accidental deletion or modification of critical resources.

Using Azure Policy, you can define a policy that enforces resource locks for all resources within a subscription, resource group, or individual resource. The policy can be assigned to a management group, which will ensure that it is applied consistently across all development environments.

upvoted 2 times

⊟ **mung** 2 years, 7 months ago

Both ARM template and blueprint can deploy locks on the resouces.
However, when they do not enforces the "lock", they just deploys it..

So i guess A..?

upvoted 1 times

⊟ **ylfr** 2 years, 8 months ago

Selected Answer: D

I agree with sadako : Blueprint

upvoted 2 times

⊟ **Kelly8023** 2 years, 8 months ago

Vote for B - Azure Resource Manager.
Reference: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?source=recommendations&tabs=json
I think the 'consistent manner' is the key here. ARM has lock inheritance function: When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the same parent lock. The most restrictive lock in the inheritance takes precedence.

upvoted 1 times

Question #57 *Topic 3*

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use the automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.
What should you create?

A. a secret in Azure Key Vault

B. a role assignment

C. an Azure Active Directory (Azure AD) user

D. an Azure Active Directory (Azure AD) group

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

Community vote distribution

B (100%)

Sergi0 Highly Voted 3 years, 5 months ago

The answer is correct

upvoted 26 times

deegadaze1 Highly Voted 2 years, 10 months ago

In Exam

upvoted 13 times

zellck Most Recent 7 months, 3 weeks ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/aks/cluster-container-registry-integration
The AKS to ACR integration assigns the AcrPull role to the Azure Active Directory (Azure AD) managed identity associated with the agent pool in your AKS cluster.

upvoted 5 times

majstor86 9 months, 4 weeks ago

Selected Answer: B

B. a role assignment
Outdated. System Managed Identity-currently

upvoted 5 times

Ajdlfasudfo0 11 months, 2 weeks ago

outdated questions, nowadays you get a System Managed Identity

upvoted 2 times

OrangeSG 11 months ago

You are correct.

An Azure Kubernetes Service (AKS) cluster requires an identity to access Azure resources like load balancers and managed disks. This identity can be either a managed identity or a service principal. By default, when you create an AKS cluster a system-assigned managed identity is automatically created.

To use a service principal, you have to create one, as AKS does not create one automatically.

https://learn.microsoft.com/en-us/azure/aks/use-managed-identity

upvoted 3 times

Eltooth 1 year, 9 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

⊟ **adamsca** 2 years ago

Correct

This is a duplicate Question of Q21 topic3. Slightly different wording but same.

upvoted 2 times

⊟ **SecurityAnalyst** 2 years, 4 months ago

# IN EXAM - 31/8/2021

upvoted 3 times

⊟ **Sandomj55** 2 years, 4 months ago

In Exam 8/4/2021

upvoted 2 times

⊟ **Corpsy** 2 years, 5 months ago

In exam 06/07/21

upvoted 3 times

⊟ **sureshatt** 2 years, 9 months ago

I could accept the answer, but who needs RBAC for authentication? RBAC is for authorisation. Again, trying to confuse.

upvoted 1 times

⊟ **Startkabels** 2 years, 8 months ago

No that is just you being autistic :D In order to successfully authenticate you need authorization no?

upvoted 1 times

⊟ **cfsxtuv33** 2 years ago

First, you need to "authenticate" to the network. Once you're authenticated you will then be "authorized" to access resources on that network.

upvoted 2 times

⊟ **babusartop17** 2 years, 6 months ago

It's actually the other way around -- first authenticate and then authorize see, this is why you don't get personal...

upvoted 19 times

⊟ **wooyourdaddy** 2 years ago

Preach the good word / way !!

upvoted 2 times

⊟ **macco455** 2 years, 9 months ago

Correct...

https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal#delegate-access-to-other-azure-resources

upvoted 5 times

⊟ **mayenite** 2 years, 11 months ago

Correct

upvoted 2 times

⊟ **tuta** 3 years ago

repeated on same page

upvoted 1 times

Question #58 *Topic 3*

You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019.

You are implementing Update Management in Azure Automation.

You plan to create a new update deployment named Update1.

You need to ensure that Update1 meets the following requirements:

✑ Automatically applies updates to VM1 and VM2.

✑ Automatically adds any new Windows Server 2019 virtual machines to Update1.

What should you include in Update1?

A. a security group that has a Membership type of Assigned

B. a security group that has a Membership type of Dynamic Device

C. a dynamic group query

D. a Kusto query language query

Suggested Answer: *C*

Reference:

https://docs.microsoft.com/en-us/azure/automation/update-management/configure-groups

Community vote distribution

C (87%) 10%

milind8451 Highly Voted 👍 4 years, 4 months ago

Right ans. Update Management allows you to target a dynamic group of Azure or non-Azure VMs for update deployments. A dynamic group is defined by a query that Azure Automation evaluates at deployment time.

upvoted 37 times

sieira Highly Voted 👍 3 years, 5 months ago

Selected Answer: C

C is the right answer, sure. I use in my work

upvoted 15 times

khamrumunnu Most Recent 1 month ago

Selected Answer: C

C

Why not the others?

A. A security group with Assigned membership:

This is static and does not dynamically add VMs.

B. A security group with Dynamic Device membership:

This applies to Azure AD groups, but Update Management doesn't target Azure AD groups directly — it works with dynamic queries based on Azure VM metadata.

D. A Kusto query language query:

KQL is used with Log Analytics, not for defining update deployment groups in Update Management.

upvoted 1 times

golitech 4 months, 4 weeks ago

Selected Answer: C

To meet the requirements, you need to use a dynamic group query. This is because:

Automatically applies updates to VM1 and VM2: When configuring Update Management in Azure Automation, you can target virtual machines for update deployments. The dynamic group query allows you to automatically include VMs, and as new Windows Server 2019 VMs are added, they will be automatically included in the update deployment without requiring manual intervention.

Automatically adds any new Windows Server 2019 virtual machines to Update1: By using a dynamic group query, new virtual machines that meet the criteria of being Windows Server 2019 will automatically be added to the group, which will then be included in the update deployment. A dynamic group query can automatically group VMs based on specific criteria such as operating system or other properties.

upvoted 1 times

Feraso 1 year, 7 months ago

Selected Answer: C

Answer C.

Update Management allows you to target a dynamic group of Azure or non-Azure VMs for update deployments. Using a dynamic group keeps you from having to edit your deployment to update machines.

A dynamic group is defined by a query that Azure Automation evaluates at deployment time.

https://learn.microsoft.com/en-us/azure/automation/update-management/configure-groups

upvoted 2 times

ESAJRR 1 year, 9 months ago

Selected Answer: C

C. a dynamic group query

upvoted 1 times

BigShot0 1 year, 9 months ago

Selected Answer: C

The answer is C. While a dynamic security group would be applicable in many cases in this case Update Management has it own Dynamic Group capabilities. See the article:
https://learn.microsoft.com/en-us/azure/automation/update-management/configure-groups

upvoted 2 times

heatfan900 1 year, 10 months ago

C

Define dynamic groups for Azure machines
When defining a dynamic group query for Azure machines, you can use the following items to populate the dynamic group:

Subscription
Resource groups
Locations
Tags

upvoted 1 times

alfaAzure 1 year, 10 months ago

Selected Answer: B

B. a security group that has a Membership type of Dynamic Device

To ensure that Update1 automatically applies updates to VM1 and VM2 and also automatically includes any new Windows Server 2019 virtual machines, you should use a dynamic group with a Membership type of Dynamic Device.

A dynamic group is a feature of Azure Automation Update Management that allows you to create groups of devices based on dynamic queries. By using a dynamic query, you can automatically include devices that match specific criteria. In this case, you would set up a dynamic query that selects Windows Server 2019 virtual machines, and any new virtual machines that meet this criterion would be automatically added to the group.

upvoted 1 times

> **pentium75** 11 months ago
>
> Thought that too, but per documentation you define the query in Update Management. The syntax is misleading, you assign updates to a "dynamic group" but this does NOT refer to a security group with dynamic membership type.
>
> upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/automation/update-management/configure-groups

Update Management allows you to target a dynamic group of Azure or non-Azure VMs for update deployments. Using a dynamic group keeps you from having to edit your deployment to update machines.

upvoted 2 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: C

C. a dynamic group query

upvoted 3 times

⊟ **obatunde** 2 years, 6 months ago

Selected Answer: C

C seems the right answer according to the link posted; "When defining a dynamic group query for Azure machines, you can use the following items to populate the dynamic group:

Subscription, Resource groups, Locations, Tags."

upvoted 1 times

⊟ **Jhill777** 2 years, 7 months ago

Selected Answer: C

There has to be more to the question as we have to make sure all future Server 2019 vms are included. The only attributes we can query against include:

Subscription

Resource Groups

Locations

Tags

upvoted 1 times

⊟ **xingu** 3 years ago

Correta Letra C - CONSulta. A letra B esta incorreta Porque se tiver um grupo de seguranca dinamico de dispositivo e usar a tag devicetypeOS ele retonar apenas se WINDOWS idependete se a maquina e windows server 2016, 2019 e no anunciado ele que WINDOWS SEVER 2019.

upvoted 1 times

⊟ **salmantarik** 3 years ago

Clearly Dynamic group is the answer.

upvoted 1 times

⊟ **alou333** 3 years ago

# IN EXAM - 3/6/2022 (online).

Lot of new questions. Good luck !

upvoted 2 times

⊟ **licna** 3 years, 5 months ago

Selected Answer: D

I am really not sure whether the suggested C is correct. It appears to me you can't define computer groups based on OS.

"When defining a dynamic group query for Azure machines, you can use the following items to populate the dynamic group:

Subscription / Resource groups / Locations / Tags "

Instead check the prereqs to enable Update management. You will need:

1. Automation account

2. Log Analytics Workspace

And in your LAW there you should define the targeting to what VMs the updated shall be applied. See:

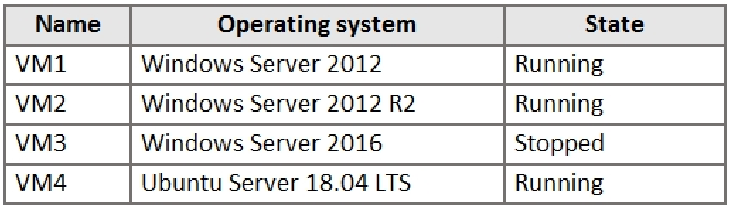
https://docs.microsoft.com/en-us/azure/automation/update-management/scope-configuration

Thus I am tempted to choose D (i.e. Kusto).

upvoted 3 times

Question #59 *Topic 3*

You have the Azure virtual machines shown in the following table.



Name	Operating system	State
VM1	Windows Server 2012	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machines can you enable Update Management?

A. VM2 and VM3 only

B. VM2, VM3, and VM4 only

C. VM1, VM2, and VM4 only

D. VM1, VM2, VM3, and VM4

E. VM1, VM2, and VM3 only

Suggested Answer: *C*

References:

https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json

Community vote distribution

C (72%) D (28%)

⊟ **Khumnan** Highly Voted 4 years, 3 months ago

"enable Update Management" is to install agent on the machine. You can install the agent only when the machine is on.

upvoted 69 times

⊟ **sureshatt** Highly Voted 4 years, 3 months ago

Could not find it in the documentation. But if tried it by creating a vm and shutting it down, and then trying to add that VM to update management, the UI says "Cannot enable" for that VM. So the answer is correct.

upvoted 24 times

⊟ **golitech** Most Recent 4 months, 4 weeks ago

Selected Answer: C

Update Management in Azure Automation cannot be enabled on a stopped virtual machine.

For Update Management to function, the virtual machine (VM) needs to be running so that it can communicate with Azure Automation and report its status, as well as receive updates.

Here's why:

Update Management depends on the ability of the VM to connect to Azure Automation to receive update information, apply updates, and report back on compliance.
If the VM is stopped (especially if it's stopped deallocated), it won't be able to send or receive any data, including updates.

upvoted 1 times

⊟ **ITFranz** 5 months, 3 weeks ago

Selected Answer: C

Update Management can be enabled on a VM that is not currently running, but there are some important considerations:

1. For Azure VMs, the VM must be in a started state to complete the initial onboarding process[3]. Once enabled, updates can be assessed and applied even when the VM is stopped.

2. For non-Azure VMs (on-premises or other cloud providers), the machine must be running and connected to Azure Arc to enable Update Management[3][6].

3. If you're using the newer Azure Update Manager (which replaced the classic Update Management solution), there are pre-made scripts available to automatically start and stop VMs for updates[7]. This is particularly useful for VMs that are normally kept in a deallocated state.

4. To use Update Management on non-Azure VMs, you need to:
- Install the Log Analytics agent on the VM[5]

upvoted 1 times

JaridB 1 year, 2 months ago

Selected Answer: D

Azure Update Management can be enabled for virtual machines regardless of their operating system, as long as they are supported by Azure and meet the requirements for the Update Management service. This service supports various operating systems including Windows Server and Linux distributions.

Based on the operating systems listed:

VM1: Windows Server 2012
VM2: Windows Server 2012 R2
VM3: Windows Server 2016
VM4: Ubuntu Server 18.04 LTS
All of these operating systems are supported by Azure Update Management. Moreover, the state of the virtual machine (running or stopped) does not affect whether Update Management can be enabled; it only affects whether updates can be applied directly. Update Management can be enabled on a stopped VM, but updates can only be applied when it is running.

Therefore, the correct answer is:
D. VM1, VM2, VM3, and VM4

All these VMs can have Update Management enabled to manage and apply updates across the different operating systems.

upvoted 3 times

Hot_156 3 months, 4 weeks ago

This is tricky because if the question is asking about RIGHT NOW! VM3 cannot have this enabled.

upvoted 1 times

epomatti 1 year, 6 months ago

Selected Answer: C

C, the VM must be running.

"The solution cannot be enabled on this virtual machine because the virtual machine is not running. Start the virtual machine first and then enable the solution."

upvoted 3 times

ESAJRR 1 year, 9 months ago

Selected Answer: C

C. VM1, VM2, and VM4 only

upvoted 1 times

zellck 2 years, 1 month ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/automation/update-management/operating-system-requirements?tabs=os-win%2Csr-win#supported-operating-systems

upvoted 2 times

majstor86 2 years, 3 months ago

Selected Answer: C

C. VM1, VM2, and VM4 only
Because the VM3 is stopped. If the VM3 is on, it will be VM1, VM2, VM3 and VM4

upvoted 5 times

ligu 2 years, 4 months ago

Answer is correct

upvoted 1 times

⊟ **Pasapugazh** 2 years, 9 months ago

Tested in Lab. If the VM is stopped then that can't be selected for update management.

upvoted 6 times

⊟ **dakasa** 2 years, 9 months ago

Selected Answer: D

Now Update management supports Linux and Windows Servers. So Answer is D

https://learn.microsoft.com/en-us/azure/automation/update-management/operating-system-requirements?tabs=os-win%2Csr-linux

upvoted 4 times

⊟ **epomatti** 1 year, 6 months ago

You still can't enable it on a VM that is stopped.

The correct answer is C.

upvoted 2 times

⊟ **Sweet_co** 2 years, 11 months ago

In exam on: 20-7-2022

upvoted 2 times

⊟ **Amit3** 2 years, 11 months ago

With agent install C is correct answer.

upvoted 1 times

⊟ **Alessandro365** 3 years ago

Selected Answer: C

C is correct answer.

upvoted 2 times

⊟ **salmantarik** 3 years ago

Correct answer. You cant deploy update management on the offline machines.

upvoted 2 times

⊟ **alou333** 3 years ago

# IN EXAM - 3june2022 (online).

Lot of new questions. Good luck !

upvoted 4 times

⊟ **NadirM_18** 3 years ago

Any estimation of the percentage of questions came from here?

upvoted 2 times

Question #60 *Topic 3*

DRAG DROP -

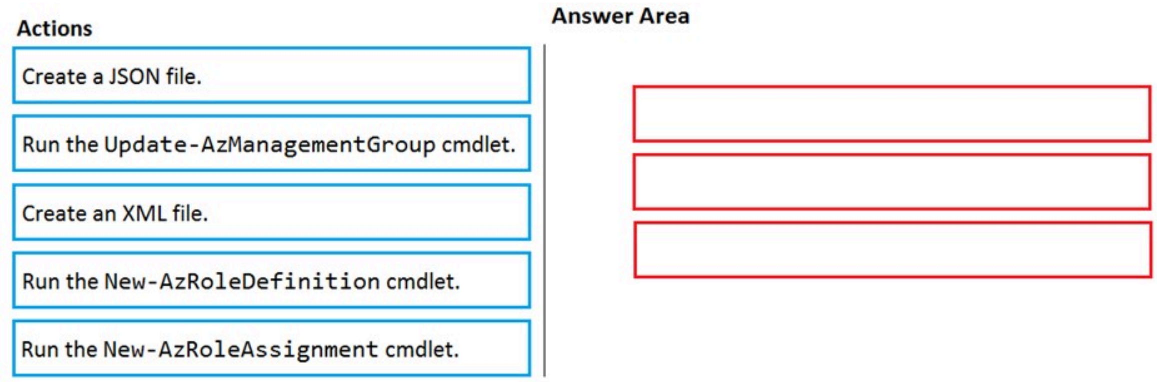
You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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

Select and Place:



Actions

Create a JSON file.

Run the Update-AzManagementGroup cmdlet.

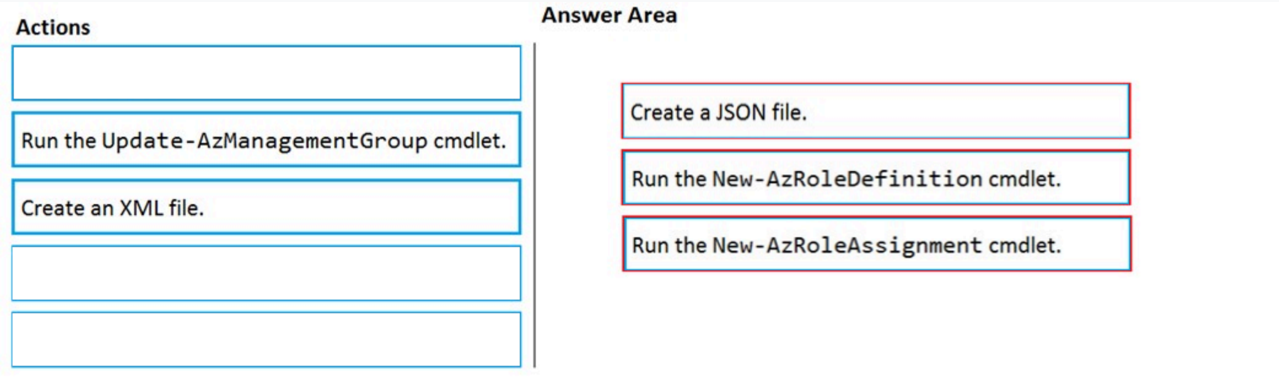
Create an XML file.

Run the New-AzRoleDefinition cmdlet.

Run the New-AzRoleAssignment cmdlet.

Answer Area

Suggested Answer:



Actions

Run the Update-AzManagementGroup cmdlet.

Create an XML file.

Answer Area

Create a JSON file.

Run the New-AzRoleDefinition cmdlet.

Run the New-AzRoleAssignment cmdlet.

References:

https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure

teehex Highly Voted 2 years, 7 months ago

Three steps you need:

- Create a json file that contains role definition (https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added#what-are-service-principals-and-where-do-they-come-from).

- Create a new role definitoon by running New-AzRoleDefinition -InputFile "C:\CustomRoles\customrole1.json" (https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-powershell#create-a-custom-role-with-json-template)

- Assigning a new role definition to the Group1 in subscription scope by running New-AzRoleAssignment https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-powershell#step-4-assign-role

upvoted 47 times

LHU 1 week, 4 days ago

Why is the answer correct?

1) We need a new role because of the "least privileged" requirement. And to create a role, you need a JSON file outlining what it is about. This is why the JSON file comes first.

2) New-AzRoleDefinition uses the -InputFile (the JSON we just made) to get the role created.

3) And then we assign it.

upvoted 1 times

LJack Highly Voted 2 years, 9 months ago

Correct answer

upvoted 19 times

majstor86 Most Recent 9 months, 4 weeks ago

1. Create a json file that contains role definition

2. Run the New-AzRoleDefinition cmdlet.

3, Run the New-AzRoleAssignment cmdlet.

upvoted 6 times

ligu 10 months, 1 week ago

Answers are correct

upvoted 1 times

sofieejo 11 months ago

In exam 29/01/2023 + many questions about Microsoft Sentinel

upvoted 4 times

Sweet_co 1 year, 5 months ago

In exam: 20-7-2022

upvoted 4 times

acexyz 1 year, 6 months ago

# IN EXAM - 30/6/2022

upvoted 3 times

alou333 1 year, 6 months ago

# IN EXAM - 3rd june 2022 (online).

Lot of new questions. Good luck !

upvoted 4 times

[Removed] 2 years, 2 months ago

Kinda logic

upvoted 1 times

orallony 2 years, 3 months ago

# IN EXAM - 29/9/2021 - Pass!

upvoted 4 times

Sandomj55 2 years, 4 months ago

In Exam 8/4/2021

upvoted 3 times

kumax 2 years, 6 months ago

On exam, May 2021.

upvoted 6 times

Fred64 2 years, 7 months ago

correct answer

we must create a custom role

upvoted 3 times

Question #61 *Topic 3*

DRAG DROP -

You have an Azure subscription that contains the following resources:

A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.

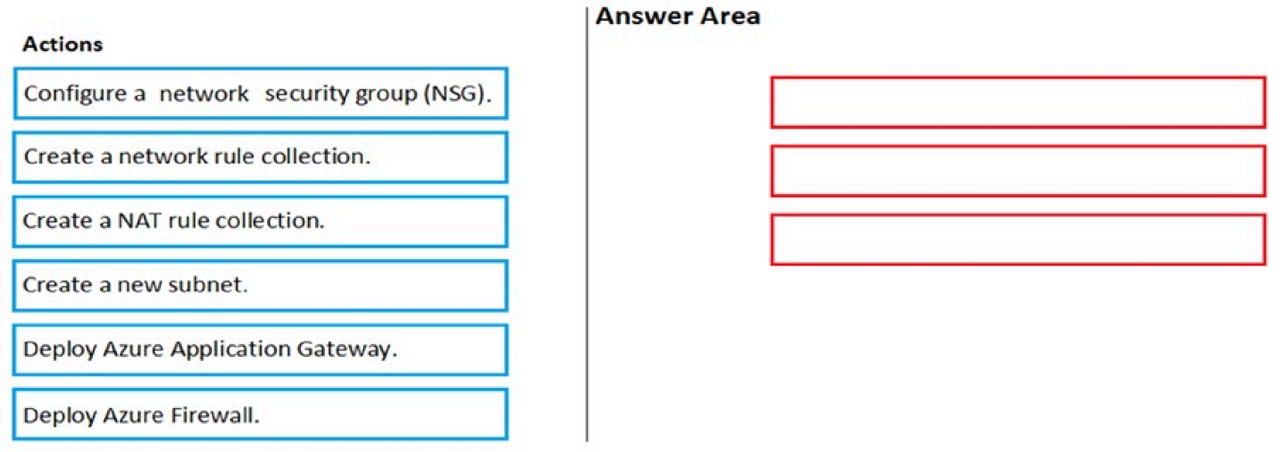
.

✑ A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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 then in the correct order.

Select and Place:



Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

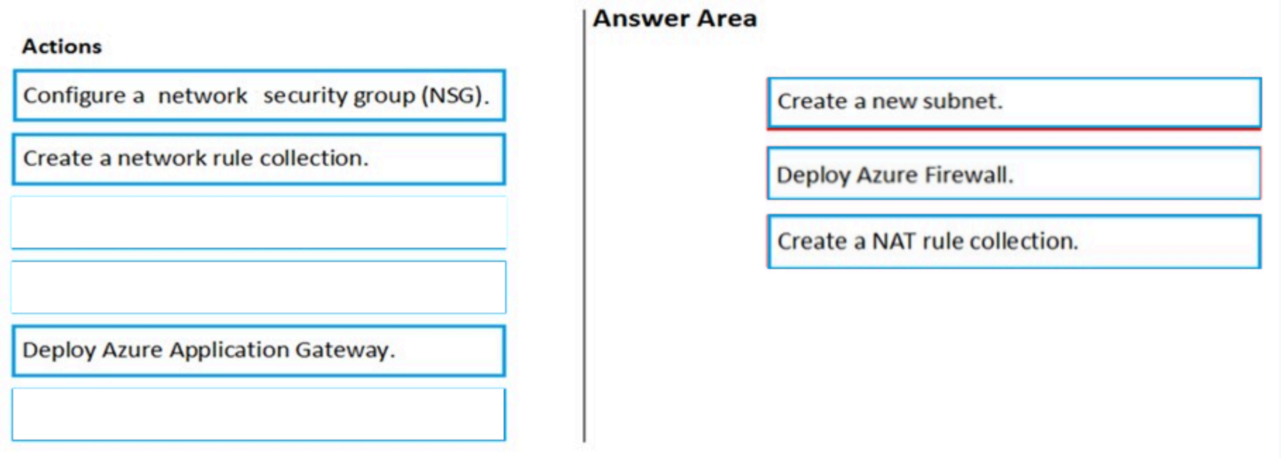
Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Suggested Answer:



Actions

Configure a network security group (NSG).

Create a network rule collection.

Deploy Azure Application Gateway.

Answer Area

Create a new subnet.

Deploy Azure Firewall.

Create a NAT rule collection.

⊟ **Johnvic** Highly Voted 2 years, 2 months ago

Exam.6 case studies. 3 true/false questions. 47 multiple questions and no simulations. Alot of new questions thats not up here

upvoted 13 times

⊟ **liorh** 2 years, 1 month ago

where can i find case studies?! i did not see it here in exam topics for az500...

upvoted 1 times

⊟ **obaali1990** 2 years, 2 months ago

Did you pass? What was your experience at the exams center?

upvoted 1 times

⊟ **foobar1985** Highly Voted 1 year, 9 months ago

in the exam on 11/9/2023

upvoted 7 times

⊟ **shanrajesh** Most Recent 5 months ago

Why we need to create an new subnet, Subnet2 is not associated to any resource. Subnet1 is associtated with Vm1, anyone clarifiy on this

upvoted 1 times

hellboysecret 3 months, 2 weeks ago

We need to create a subnet for firewall.

upvoted 1 times

Hot_156 3 months, 4 weeks ago

1. Deploy Azure Firewall. Subnet2
2. Create a NAT rule collection.
3. Configure a network security group (NSG).

upvoted 1 times

Hot_156 3 months, 2 weeks ago

I was wrong. There must be a new subnet called "AzureFirewallSubnet"

1. Create a new subnet
2. Deploye the FW
3. Create a NAT rule collection

upvoted 1 times

cerifyme85 8 months, 1 week ago

what about subnet 2.. we can use that as firewall

upvoted 1 times

91743b3 10 months, 3 weeks ago

On exam Aug 6 2024

upvoted 4 times

JunetGoyal 1 year, 8 months ago

Given ans is correct

You need separate Firewall subnet to deploy FW> then create Firewall> then Do NAT rule

AS VM does not have public IP, you either need Dnat or/ you can use Bastion service too /or Configure another VM from Same subnet and do RDP from new VM to this one.

upvoted 5 times

heatfan900 1 year, 10 months ago

giving the VM a public IP and configuring a rule on the NSG would be a lot easier but if that is not there then this is the alternative

upvoted 4 times

Ario 1 year, 12 months ago

this question doesn't make any sense regardless creating a new subnet is useless , Configure an Azure public IP address:

Create a new Azure public IP address resource.

Associate the public IP address with the virtual machine (VM1).

Create an Azure network security group (NSG) rule:

Create an inbound rule in the NSG associated with the network interface of VM1.

Allow incoming traffic on the Remote Desktop Protocol (RDP) port (TCP port 3389) from any source IP address (0.0.0.0/0) or a specific IP address range if necessary.

Configure the network security group (NSG) on Subnet1:

Associate the NSG created in step 2 with Subnet1 of VNET1.

Ensure that the NSG allows outgoing traffic from Subnet1 to the internet.

upvoted 2 times

flafernan 1 year, 7 months ago

totally agree

upvoted 1 times

Mnguyen0503 1 year, 6 months ago

Incorrect. Creating new subnet is required for Azure Firewall. Since the question already said the VM does not have a public IP, an Azure Firewall is required to enforce NAT rule and allow RDP traffic in. Having a public IP on a VM is not ideal if you want to scale.

upvoted 1 times

zellck 2 years, 1 month ago

1. Create a new subnet
2. Deploy Azure Firewall

3. Create a NAT rule collection

https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal-policy
- The size of the AzureFirewallSubnet subnet is /26.
- The firewall will be in this subnet, and the subnet name must be AzureFirewallSubnet.

Deploy the firewall and policy
https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal-policy#deploy-the-firewall-and-policy

Configure a DNAT rule
https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal-policy#configure-a-dnat-rule
upvoted 6 times

majstor86 2 years, 3 months ago
1. Create a new subnet.
2. Deploy Azure Firewall.
3. Create a NAT rule collection.
upvoted 2 times

ligu 2 years, 4 months ago
Answers are correct
upvoted 1 times

F117A_Stealth 2 years, 7 months ago
Answer is correct.

You can configure Azure Firewall Destination Network Address Translation (DNAT) to translate and filter inbound Internet traffic to your subnets.
upvoted 3 times

AzureJobsTillRetire 2 years, 5 months ago
That's correct. VM1 has only a private IP address. For the NSG to work, VM1 needs to have a public IP address.
upvoted 1 times

somenick 2 years, 8 months ago
Correct. https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat
upvoted 1 times

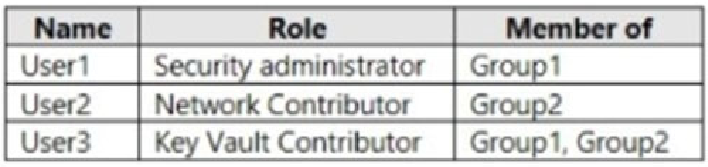
geuser 2 years, 8 months ago
question and answer does not make sense. The Q looks incomplete.
upvoted 4 times

Lozo2020 3 years, 2 months ago
Correct
upvoted 3 times

Question #62 Topic 3

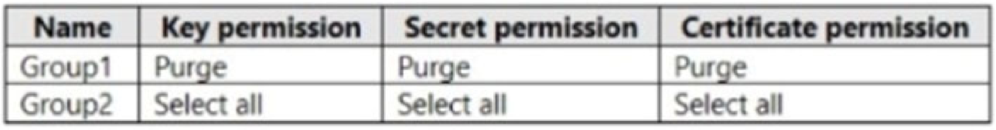
HOTSPOT -

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.



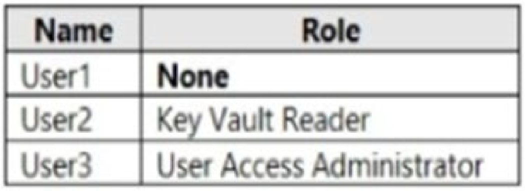
Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disable. Vault1 contains the access policies shown in the following table.



Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

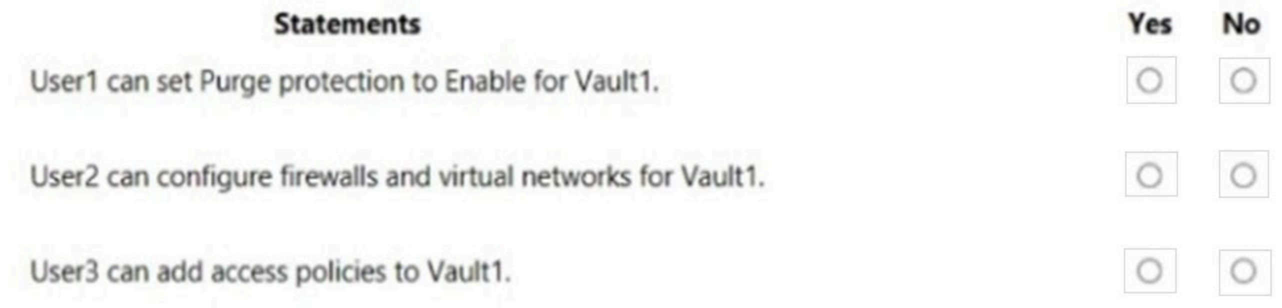


Name	Role
User1	**None**
User2	Key Vault Reader
User3	User Access Administrator

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

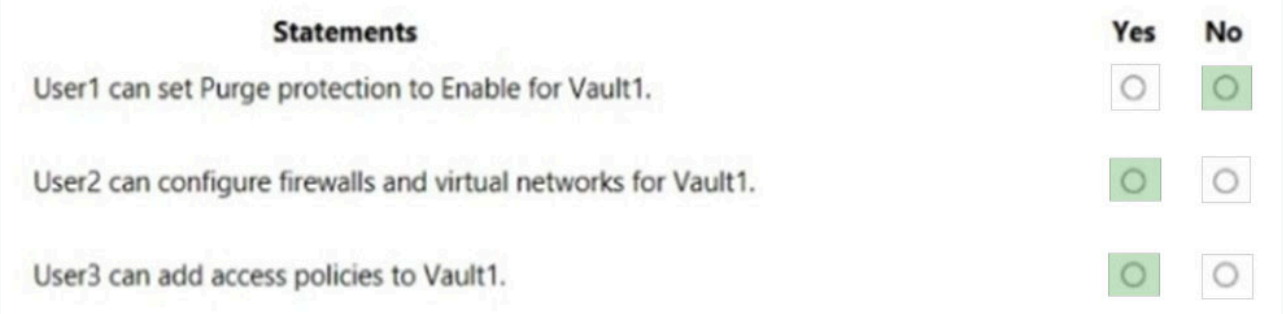
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	○
User2 can configure firewalls and virtual networks for Vault1.	○	○
User3 can add access policies to Vault1.	○	○

Suggested Answer:



Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	[✓ ○]
User2 can configure firewalls and virtual networks for Vault1.	[✓ ○]	○
User3 can add access policies to Vault1.	[✓ ○]	○

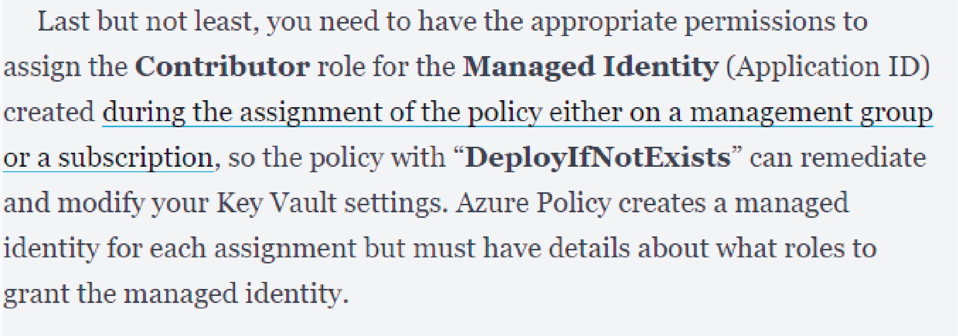
Box 1: No -

Resource Policy Contributor or Security Administrator is required.

User1 is Security Administrator only with the no specific permission granted to Vault1.

The Security Admin can 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.

However:



Last but not least, you need to have the appropriate permissions to assign the **Contributor** role for the **Managed Identity** (Application ID) created during the assignment of the policy either on a management group or a subscription, so the policy with "**DeployIfNotExists**" can remediate and modify your Key Vault settings. Azure Policy creates a managed identity for each assignment but must have details about what roles to grant the managed identity.

Box 2: Yes -
User2 is a Network Contributor, with Select All Key, Secret & Certificate permissions, and Key Vault Reader.
The Network Contributor role lets you manage networks, but not access to them.

Box 3: Yes -
User3 is a Key Vault Contributor and a User Access Administrator for Vault.
The Key Vault Contributor role allows you to manage key vaults, but does not allow you to assign roles in Azure RBAC, and does not allow you to access secrets, keys, or certificates.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor https://charbelnemnom.com/enable-purge-protection-key-vault-azure-policy/

juandmi Highly Voted 2 years, 5 months ago
Tested with following results:
A: No
Security Admin cannot manage key vault properties
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-admin
B: No
Network Contributor or Key Vault Reader cannot change the key vault firewall
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor
C: YES
Key vault contributor can do that
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-contributor
Note: "does not allow you to assign roles" - but here the question is to add access policies which works.
upvoted 33 times

sigvast 1 year, 11 months ago
Agree, but for A the user role doesn't matter anyway because purge protection cannot be changed after the vault creation.
upvoted 4 times

KvE90093 Most Recent 1 year ago
A: NO, even the user is in group1, the inherited permission cannot enable purge protection. The purge permission allows purge/delete soft-delete items, but not for configuration settings such as purge protection.
upvoted 1 times

JaridB 1 year, 2 months ago
B: NO - These roles allow the configuration of Key Vault firewall rules, including setting up network rules that restrict access to the vault based on IP addresses or virtual network settings. The Key Vault Contributor role enables a user to manage various Key Vault properties, including its networking and firewall configurations, which are essential for defining who can access the vault.
The Azure Network Contributor role does not have the permissions necessary to configure firewall and virtual network settings for an Azure Key Vault. This role primarily allows for managing networking resources such as subnets, virtual networks, and routing tables, but does not extend to managing the security and network configuration of Key Vaults.
upvoted 1 times

wardy1983 1 year, 8 months ago
Box 1: No -
Resource Policy Contributor or Security Administrator is required.
User1 is Security Administrator only with the no specific permission granted to Vault1.
The Security Admin can 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.

However:

Box 2:no

Network Contributor or Key Vault Reader cannot change the key vault firewall

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

Box 3: Yes -

User3 is a Key Vault Contributor and a User Access Administrator for Vault.

upvoted 3 times

JunetGoyal 1 year, 8 months ago

Note: When it comes to some resources in Azure, overall RBAC does not apply to them.Ypu need to give explicit permission to these resouces.

For example Key vault in this Q.

user 1-Security Admin will work for rest of other sources but not for KV. this same applies to user 2.

So my ans N,N,Y

upvoted 2 times

Strifelife 1 year, 11 months ago

no,no,yes had to check from ChatGPT just to make sure.

upvoted 3 times

majstor86 2 years, 3 months ago

NO

NO

YES

upvoted 4 times

Diallo18 2 years, 8 months ago

In Exam 10/18/2022. One case study(6 ques), no lab.

upvoted 3 times

Kelly8023 2 years, 8 months ago

Answers are correct.

upvoted 2 times

joanjcanals 2 years, 9 months ago

2nd statement is wrong: becuase not have authorization to perform action 'Microsoft.KeyVault/vaults/write

upvoted 4 times

Amit3 2 years, 9 months ago

Its only taking about firewall and network, not writing anything to keyvault

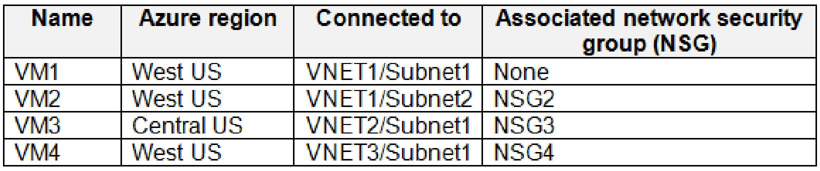
upvoted 2 times

Question #63 *Topic 3*

HOTSPOT

-

You have an Azure subscription that contains the virtual machines shown in the following table.



Name	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	None
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET3/Subnet1	NSG4

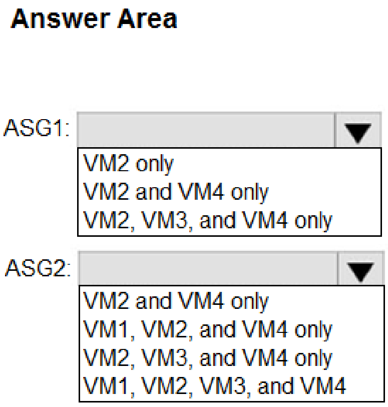
VNET1, VNET2, and VNET3 are peered with each other.

You perform the following actions:

- Create two application security groups named ASG1 and ASG2 in the West US region.
- Add the network interface of VM1 to ASG1.

The network interfaces of which virtual machines can you add to ASG1 and ASG2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

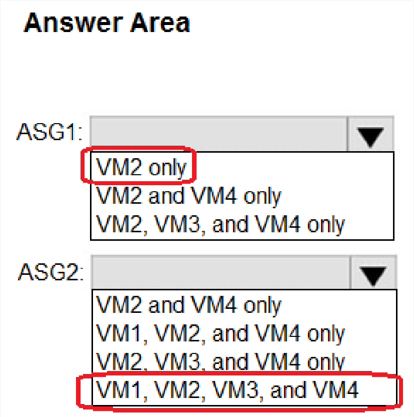
ASG1:

VM2 only
VM2 and VM4 only
VM2, VM3, and VM4 only

ASG2:

VM2 and VM4 only
VM1, VM2, and VM4 only
VM2, VM3, and VM4 only
VM1, VM2, VM3, and VM4

Suggested Answer:



Answer Area

ASG1:

[✓ VM2 only]
VM2 and VM4 only
VM2, VM3, and VM4 only

ASG2:

VM2 and VM4 only
VM1, VM2, and VM4 only
VM2, VM3, and VM4 only
[✓ VM1, VM2, VM3, and VM4]

⊟ **r_git** Highly Voted 2 years, 3 months ago

Tested in lab.

ASGs can be assigned to VMs that are in the same region the ASG is in AND the same VNET as the first VM that is assigned to it is in.

ASG1 - VM2

ASG1 is in WEST US and VM1 on VNET1 is assigned to it, so ASG1 can only be assigned to VMs that are in VNET1.

ASG2 - VM1, VM2, VM4

ASG2 is in WEST US and currently has no VMs assigned to it.

So ASG1 can be assigned to VM1 and VM2 in VNET1 OR VM4 in VNET3. But not VM1/2 AND VM4 all at the same time.

upvoted 28 times

massnonn 2 years ago

why not ASG- VM2 AND VM4 only? VM1 is just assigned

upvoted 1 times

epomatti 1 year, 6 months ago

A VM can be a member of multiple ASGs.

upvoted 3 times

epomatti 1 year, 6 months ago

Tested and confirmed.

ASG2 - VM1, VM2, VM4

Documentation does not make that explicit, but ASG and VM must be in the same region as well. After you add the first network card, then all NICs added after that must also be in the same VNET.

upvoted 1 times

Nick66 Highly Voted 👍 2 years, 5 months ago

ASG1: VM2 only

ASG2: VM1, VM2, VM4

A Virtual Machine can be attached to more than one Application Security Group. This helps in cases of multi-application servers.

There are only two requirements:

• All network interfaces used in an ASG must be within the same VNet

• If ASGs are used in the source and destination, they must be within the same VNet

upvoted 11 times

Srirupam Most Recent 🕘 7 months, 1 week ago

ASG1- VM2 & VM4

ASG2-VM1,VM2,VM4

upvoted 2 times

Goke282 1 year, 3 months ago

The answer is correct:

ASG1: VM2 Only

ASG2: VM1, VM2, VM3, VM4

Explanation according to Copilot:

Azure Virtual Machines (VMs) can be assigned to Application Security Groups (ASGs) regardless of their region. ASGs allow you to group VMs and define network security policies based on those groups. Here are some key points:

Application Security Groups (ASGs):

Enable you to configure network security as a natural extension of an application's structure.

Group VMs and define network security policies based on those groups.

Reuse security policies at scale without manual maintenance of explicit IP addresses.

Handle the complexity of explicit IP addresses and multiple rule sets.

Example:

Consider an example where NIC1 and NIC2 are members of the AsgWeb ASG, NIC3 is a member of the AsgLogic ASG, and NIC4 is a member of the AsgDb ASG.

Each NIC can be a member of multiple ASGs, up to Azure limits.

Network interfaces apply rules based on the ASGs they belong to.

upvoted 1 times

gen33 1 year, 6 months ago

region constraint does not apply so the proposed answer is correct

upvoted 2 times

[Removed] 1 year, 6 months ago

Tested in the lab the ASG was in a UK West region and I could not add the NIC which was in North Europe Region to it so all VMs in the same region as the ASG could be added only its VM1,2,4

upvoted 1 times

femzy 1 year, 7 months ago

Application Security Groups (ASGs) are used within a single network security group (NSG).

ASGs are regional resources and can only be used within the same Azure region where they are created.

ASG1: VM2 and VM4 only (because they are in the same region as ASG1)

ASG2: VM1, VM2, and VM4 only (because they are all in the West US region and can be grouped together in ASG2)

upvoted 2 times

flafernan 1 year, 7 months ago

ASG1 - VM2 Only

Because it is the only one that is in the same VNET as VM1.

ASG2 - VM2 VM3 and VM4 Only

Following the rule that you can only associate an ASG with a single VNET, and that even if Virtual Machines (VMs) are in the same Virtual Network (VNET), you can associate each VM with a different Application Security Group (ASG) . This would already exclude VM1 from ASG2 which is already associated with VNET1.

There would then only be the possibility of VM2 VM3 and VM4 Only.

upvoted 1 times

pentium75 11 months ago

VM1 could be member of multiple ASGs, you can add it to ASG2 as long as that is empty.

upvoted 1 times

wardy1983 1 year, 8 months ago

ASG1: VM2 only

ASG2: VM1, VM2, VM4

A Virtual Machine can be attached to more than one Application Security Group. This helps in cases of multiapplication servers.

There are only two requirements:

• All network interfaces used in an ASG must be within the same VNet

• If ASGs are used in the source and destination, they must be within the same VNet

upvoted 1 times

TheProfessor 1 year, 9 months ago

Can anybody please explain why ASG2: VM1 VM2 VM3 VM4

VM1 and VM2 are in one Vnet where VM4 is in another Vnet. As per my understanding, VMs need to be under same Vnet. In that case, only VM4 should in ASG2.

upvoted 2 times

pentium75 11 months ago

Yes, "VMs need to be under same Vnet", but ASG2 is currently empty. Thus you can add any VM to it. Once you added the first VM, THEN you can only add VMs from the same VNet.

upvoted 1 times

Self_Study 1 year, 10 months ago

On my exam today. The question asked where ASG1 only can be assigned.

upvoted 5 times

ITTesters 2 years, 1 month ago

Tip note from the Azure Portal when you try to add a ASG to a VM NIC:

"Showing only application security groups in the same region as the network interface. If you choose more than one application security group, they must all exist in the same virtual network."

upvoted 4 times

zellck 2 years, 2 months ago

ASG1: VM2 only

ASG2: VM1, VM2 and VM4 only

https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You can't add network interfaces from different virtual networks to the same application security group.

upvoted 5 times

⊟ **xRiot007** 11 months, 1 week ago

Your explanation and answer make no sense. VM4 is in VNET3, while WM1 is in VNET1.

upvoted 1 times

⊟ **Tecenvi** 2 years, 2 months ago

There is not limit to the region... An ASP can has more than one NIC but all must be in the same vNet.

https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

ASG1 - VM2

ASG2 - VM1, VM2, VM4

upvoted 4 times

⊟ **stepman** 2 years, 2 months ago

I chose this. On exam 4/27 along with the new user experience exam

upvoted 3 times

⊟ **zellck** 2 years, 2 months ago

what new user experience did you get?

upvoted 2 times

⊟ **another2** 2 years, 5 months ago

Correct answer is :

asg1 - VM2

asg2 - VM1, VM2, VM4

when ASG contains VM, you can only add other vm's that are in the same virtual network in this case VM2,

if ASG(asg2) has not previously added vm's , you can add them only from the same Region, in this case US West.

upvoted 6 times

⊟ **another2** 2 years, 5 months ago

P.S peering not changing anything in this case.

upvoted 5 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

Box1: VM2 only

Add the network interface of VM1 to ASG1. VM1 is in VET1, all available ASGs must be in VNET1.

Box2: VM2 and VM4

ASG2 is in the West US region, and it has not been attached to any NIC yet. It can be attached to NICs in the West US region, and both VM2 and VM4 are in the West US region.

upvoted 2 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

Azure security groups can't be moved from one region to another. You can however, use an Azure Resource Manager template to export the existing configuration and security rules of an NSG. You can then stage the resource in another region by exporting the NSG to a template, modifying the parameters to match the destination region, and then deploy the template to the new region.

https://learn.microsoft.com/en-us/azure/virtual-network/move-across-regions-nsg-portal

upvoted 1 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

Sorry I copied the wrong ref, pls, disregard this particular comment. I will upload the right ref soon

upvoted 1 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

upvoted 2 times

⊟ **AzureJobsTillRetire** 2 years, 5 months ago

Sorry my bad. I think Box2 is VM1, VM2 and VM4. The catch is that you cannot add VM1/VM2 and VM4 to ASG2 at the same time. Once you add VM1 or VM2 to ASG2, VM4 is out. Once you add VM4 to ASG2, VM1 and VM2 are out.

upvoted 3 times

Question #64 *Topic 3*

You have an Azure subscription that contains an Azure key vault.

You need to configure the maximum number of days for which new keys are valid. The solution must minimize administrative effort.

What should you use?

A. Azure Purview

B. Key Vault properties

C. Azure Blueprints

D. Azure Policy

Suggested Answer: *D*

Community vote distribution

D (100%)

OrangeSG Highly Voted 👍 11 months ago

Selected Answer: D

Azure Buil-t-in policy name: Keys should not be active for longer than the specified number of day

Description: Specify the number of days that a key should be active. Keys that are used for an extended period of time increase the probability that an attacker could compromise the key. As a good security practice, make sure that your keys have not been active longer than two years.

Reference
Azure Policy built-in definitions for Key Vault
https://learn.microsoft.com/en-us/azure/key-vault/policy-reference
upvoted 12 times

AzureJobsTillRetire Highly Voted 👍 11 months, 2 weeks ago

I've checked the key vault properties and have not found anything about the maximum number of days for which new keys are valid.
upvoted 9 times

zellck Most Recent 🕒 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/key-vault/general/azure-policy#lifecycle-of-keys
With lifecycle management built-ins you can flag or block keys that do not have an expiration date, get alerts whenever delays in key rotation may result in an outage, prevent the creation of new keys that are close to their expiration date, limit the lifetime and active status of keys to drive key rotation, and preventing keys from being active for more than a specified number of days.
upvoted 7 times

Cristoicach91 9 months, 2 weeks ago

answer is B, key vault properties
upvoted 1 times

majstor86 9 months, 4 weeks ago

Selected Answer: D

D. Azure Policy
upvoted 1 times

Ajdlfasudfo0 11 months, 2 weeks ago

https://learn.microsoft.com/en-us/azure/key-vault/general/azure-policy?tabs=certificates

You want to improve the security posture of your company by implementing requirements around minimum key sizes and maximum validity periods of certificates in your company's key vaults but you don't know which teams will be compliant and which are not.

Manage certificates that are within a specified number of days of expiration

Your service can experience an outage if a certificate that is not being adequately monitored is not rotated prior to its expiration. This policy is critical to making sure that your certificates stored in key vault are being monitored. It is recommended that you apply this policy multiple times with different expiration thresholds, for example, at 180, 90, 60, and 30-day thresholds. This policy can be used to monitor and triage certificate expiration in your organization.

upvoted 3 times

Question #65 *Topic 3*

You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1.

You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network.

You need to enable access from synapsews1 to storage1.

What should you configure?

A. peering

B. a private endpoint

C. a network security group (NSG)

D. a virtual network gateway

Suggested Answer: *B*

Community vote distribution

B (100%)

OrangeSG Highly Voted 1 year, 5 months ago

Selected Answer: B

Managed private endpoints are private endpoints created in a Managed Virtual Network associated with your Azure Synapse workspace. Managed private endpoints establish a private link to Azure resources. Azure Synapse manages these private endpoints on your behalf. You can create Managed private endpoints from your Azure Synapse workspace to access Azure services (such as Azure Storage or Azure Cosmos DB) and Azure hosted customer/partner services.

Reference

Synapse Managed private endpoints

https://learn.microsoft.com/en-us/azure/synapse-analytics/security/synapse-workspace-managed-private-endpoints

upvoted 8 times

flafernan Most Recent 7 months, 1 week ago

Selected Answer: B

To allow access to the Azure Synapse Analytics workspace (synapsews1) and Azure Data Lake Storage Gen2 account (storage1), you must configure a private endpoint. Don't confuse it with peering, as this happens even if they are in different VNETs. The private endpoint is a private connection within the virtual network, which provides an additional layer of security and isolation.

upvoted 2 times

wardy1983 7 months, 2 weeks ago

Answer: B

Explanation:

Managed private endpoints are private endpoints created in a Managed Virtual Network associated with your

Azure Synapse workspace. Managed private endpoints establish a private link to Azure resources. Azure

Synapse manages these private endpoints on your behalf. You can create Managed private endpoints from

your Azure Synapse workspace to access Azure services (such as Azure Storage or Azure Cosmos DB) and

Azure hosted customer/partner services.

Reference

Synapse Managed private endpoints

https://learn.microsoft.com/en-us/azure/synapse-analytics/security/synapse-workspace-managed-privateendpoints

upvoted 3 times

foobar1985 9 months, 3 weeks ago

in the exam 11/9/2023

upvoted 2 times

cutek 1 year ago

Selected Answer: B

B is the answer

Managed private endpoints

upvoted 1 times

⊟ **zellck** 1 year, 2 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/synapse-analytics/security/synapse-workspace-managed-private-endpoints#managed-private-endpoints
Managed private endpoints are private endpoints created in a Managed Virtual Network associated with your Azure Synapse workspace. Managed private endpoints establish a private link to Azure resources. Azure Synapse manages these private endpoints on your behalf. You can create Managed private endpoints from your Azure Synapse workspace to access Azure services (such as Azure Storage or Azure Cosmos DB) and Azure hosted customer/partner services.

upvoted 4 times

⊟ **majstor86** 1 year, 3 months ago

Selected Answer: B

B. a private endpoint

upvoted 1 times

⊟ **Ajdlfasudfo0** 1 year, 5 months ago

Selected Answer: B

private endpoint is one of the possible solutions

upvoted 1 times

Question #66 *Topic 3*

You have a Microsoft Entra tenant named Contoso.com and an Azure Kubernetes Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com.

You need to ensure AKS1 can be accessed by using accounts from Contoso.com. The solution must minimize administrative effort.

What should you do first?

A. From Azure, recreate AKS1.

B. From AKS1, upgrade the version of Kubernetes.

C. From Microsoft Entra, add a Microsoft Entra ID P2 license.

D. From Microsoft Entra, configure the User settings.

Suggested Answer: *A*

Community vote distribution

A (100%)

TROUFIS 2 weeks, 5 days ago

Selected Answer: D

correct

upvoted 1 times

mmmyo 1 month, 3 weeks ago

Selected Answer: D

✅ Configuring Microsoft Entra User settings ensures that users from Contoso.com have the correct authentication policies and permissions to access AKS. ✅ This is the least administratively complex solution, as it does not require rebuilding AKS1 or upgrading Kubernetes.

upvoted 1 times

Abdullah14 9 months, 3 weeks ago

Selected Answer: A

account accesses happens in the phase of creation of the kubernetes service

upvoted 3 times

chiquito 1 year, 2 months ago

Answer A: is correct

This was already sorted out under : Question #42Topic 3
The following limitations apply:
Azure AD can only be enabled on Kubernetes RBAC-enabled cluster.
Azure AD legacy integration can only be enabled during cluster creation.
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

upvoted 2 times

mrt007 1 year, 3 months ago

Given the options, the best first step would be:

D. From Microsoft Entra, configure the User settings.

This would involve setting up the necessary permissions for Contoso.com accounts to access the AKS1 cluster. This is a more direct solution compared to the other options and requires less administrative effort. Recreating the AKS cluster or upgrading Kubernetes wouldn't necessarily resolve an access issue, and adding a Microsoft Entra ID P2 license is not directly related to access management.

upvoted 2 times

Question #67 Topic 3

SIMULATION

-

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs1234578 Azure Storage account.

To complete this task, sign in to the Azure portal.

Suggested Answer:

You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.

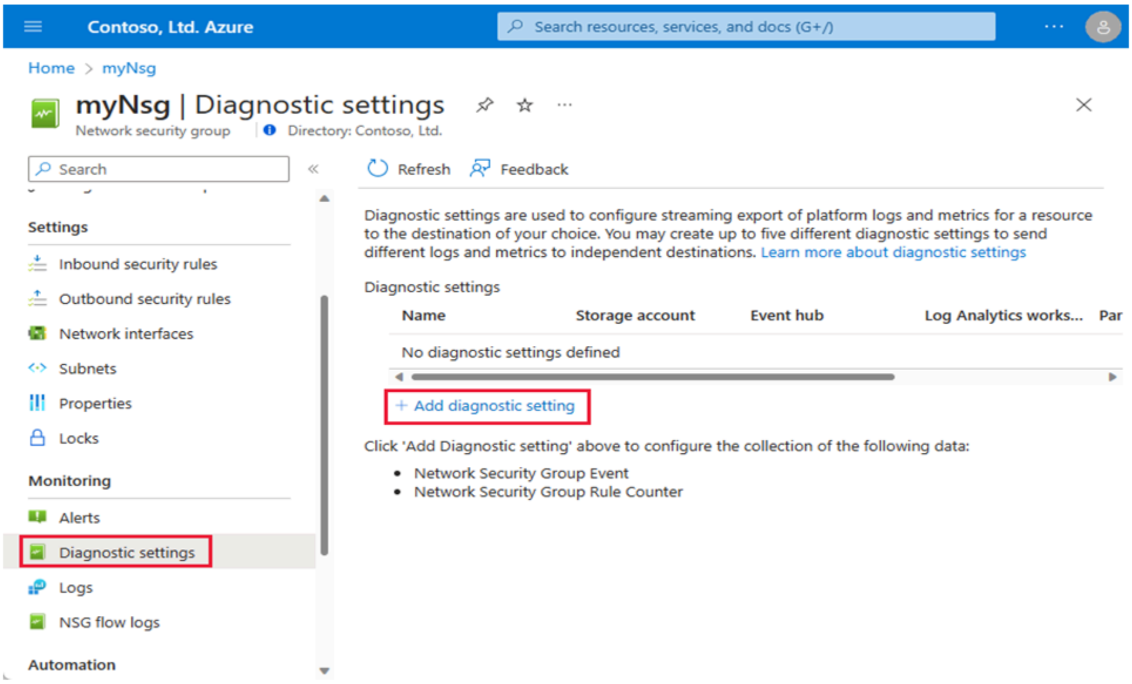
Alternative 1:
Enable logging
You can use the Azure portal, Azure PowerShell, or the Azure CLI to enable resource logging.

Azure portal
Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the Azure portal, enter network security groups. Select Network security groups in the search results.

Step 3: Select the NSG for which to enable logging. Here select: VNET01-Subnet0-NSG

Step 4: Under Monitoring, select Diagnostic settings, and then select Add diagnostic setting:



Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

Diagnostic settings

Name	Storage account	Event hub	Log Analytics works...	Par
No diagnostic settings defined				

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Network Security Group Event
- Network Security Group Rule Counter

Step 5: In Diagnostic setting, enter a name, such as myNsgDiagnostic.

Step 6: For Logs, select the **NetworkSecurityGroupRuleCounter** log .

Step 7: Under Destination details, select one or more destinations:

Send to Log Analytics workspace
*-> Archive to a storage account (Select this one!)
Stream to an event hub
Send to partner solution

Step 8: In the **Storage account** field, select the **logs1234578** storage account.

Step 9: Click the **Save** button to save the changes.

Alternative 2:

1. In the Azure portal, type **Network Security Groups** in the search box, select **Network Security Groups** from the search results then select **VNET01-Subnet0-NSG**. Alternatively, browse to Network Security Groups in the left navigation pane.
2. In the properties of the Network Security Group, click on **Diagnostic Settings.**
3. Click on the **Add diagnostic setting** link.
4. Provide a name in the **Diagnostic settings name** field. It doesn't matter what name you provide for the exam.
5. In the **Log** section, select **NetworkSecurityGroupRuleCounter**.
6. In the **Destination details** section, select **Archive to a storage account.**
7. In the **Storage account** field, select the **logs1234578** storage account.
8. Click the **Save** button to save the changes.

Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

⊟ **91743b3** 10 months, 3 weeks ago
On exam Aug 6 2024

upvoted 3 times

⊟ **mrt007** 1 year, 3 months ago

Sign in to the Azure portal.

Navigate to the Network Security Groups section.

Select the VNET01-Subnet0-NSG network security group.

In the settings pane on the left, click on Diagnostics settings.

Click on Add diagnostic setting.

In the Diagnostic settings pane, provide a name for the setting.

Check the Send to Log Analytics workspace option.

In the Log section, ensure that the NetworkSecurityGroupRuleCounter is checked.

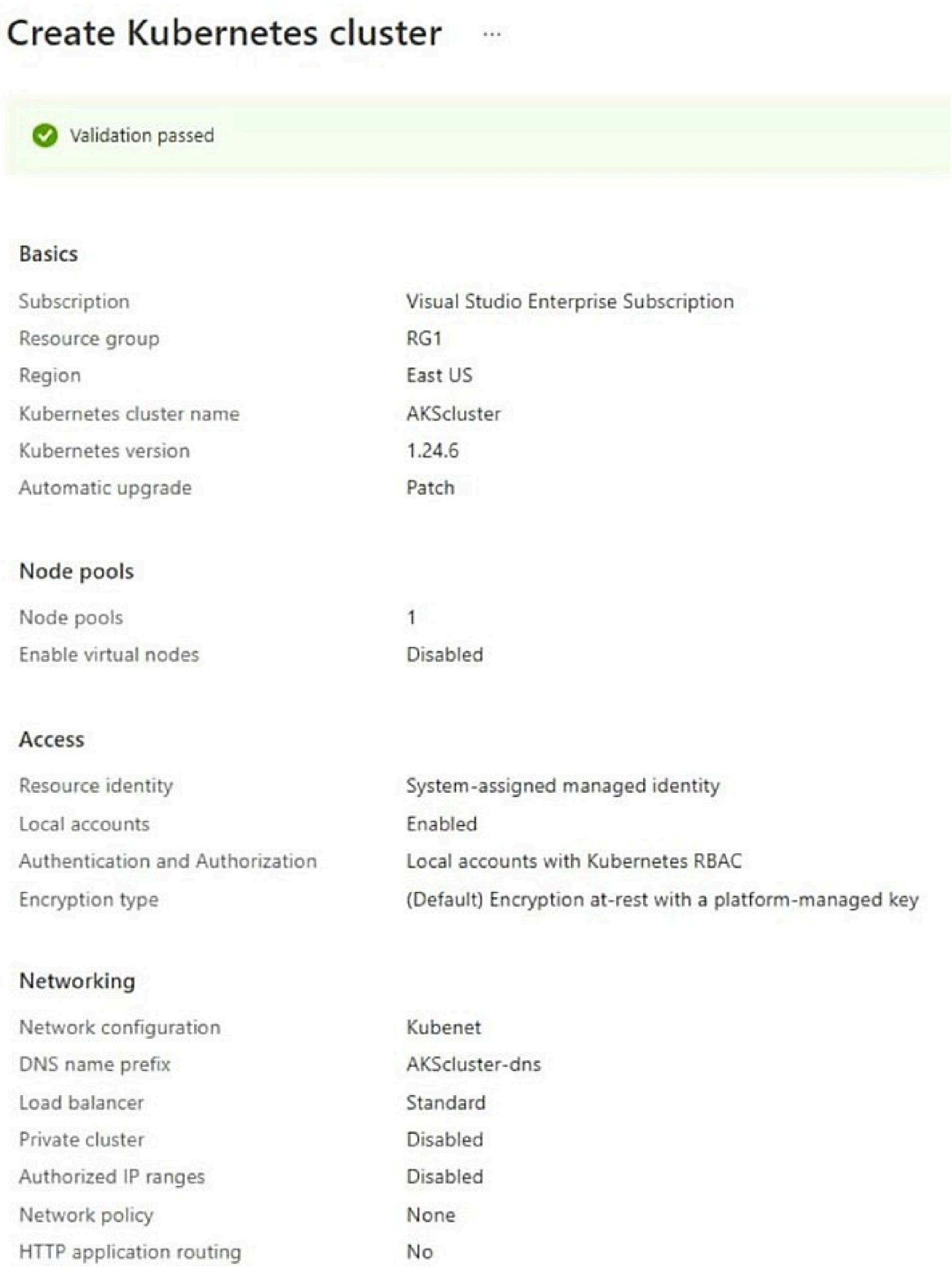
In the Destination details section, select the logs1234578 storage account.

Click on Save.

upvoted 4 times

Question #68 *Topic 3*

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)



Create Kubernetes cluster ...

✓ Validation passed

Basics

Subscription	Visual Studio Enterprise Subscription
Resource group	RG1
Region	East US
Kubernetes cluster name	AKScluster
Kubernetes version	1.24.6
Automatic upgrade	Patch

Node pools

Node pools	1
Enable virtual nodes	Disabled

Access

Resource identity	System-assigned managed identity
Local accounts	Enabled
Authentication and Authorization	Local accounts with Kubernetes RBAC
Encryption type	(Default) Encryption at-rest with a platform-managed key

Networking

Network configuration	Kubenet
DNS name prefix	AKScluster-dns
Load balancer	Standard
Private cluster	Disabled
Authorized IP ranges	Disabled
Network policy	None
HTTP application routing	No

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

A. Create an AKS Ingress controller.

B. Create an Azure Standard Load Balancer.

C. Install the container network interface (CNI) plug-in.

D. Create an Azure Basic Load Balancer.

Suggested Answer: *A*

Community vote distribution

A (100%)

HdiaOwner 9 months, 3 weeks ago

Selected Answer: A

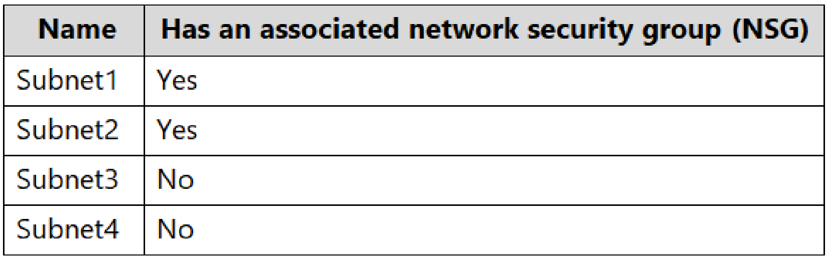
An Ingress controller is typically used to manage external access to services in a Kubernetes cluster, usually via HTTP/HTTPS, and it can provide reverse proxy and TLS termination. It enables routing traffic to services based on the URL and can handle requests coming into the cluster using a single public IP.

This option fits the requirements well as an Ingress controller supports reverse proxying and TLS termination.

upvoted 2 times

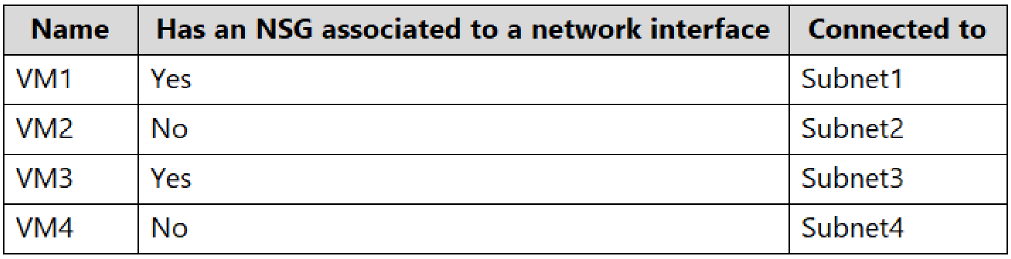
Question #69 *Topic 3*

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the subnets shown in the following table.



Name	Has an associated network security group (NSG)
Subnet1	Yes
Subnet2	Yes
Subnet3	No
Subnet4	No

You create the virtual machines shown in the following table.



Name	Has an NSG associated to a network interface	Connected to
VM1	Yes	Subnet1
VM2	No	Subnet2
VM3	Yes	Subnet3
VM4	No	Subnet4

You plan to configure just-in-time (JIT) VM access for the virtual machines. The solution must minimize administrative effort.

For which virtual machines can you configure JIT VM access?

A. VM1 only

B. VM1 and VM2 only

C. VM1 and VM3 only

D. VM1, VM2, and VM3 only

E. VM1, VM2, VM3, and VM4

Suggested Answer: *D*

Community vote distribution

D (100%)

Abdullah14 Highly Voted 9 months, 3 weeks ago

Selected Answer: D

NSG must be enabled either on VM level or Subnet

upvoted 5 times

golitech Most Recent 4 months, 4 weeks ago

Selected Answer: D

NSG with inbound is prerequisite for JIT configuration. The virtual machine must be associated with an NSG that controls inbound traffic. JIT works by modifying the NSG rules temporarily to allow access for the defined time window.

Subnet 1 and Subnet 2 have NSG assigned -> JIT can be enabled. -> VM1 and VM2 can have JIT
VM3 NIC also has NSG assigned -> JIT can be enabled.

upvoted 2 times

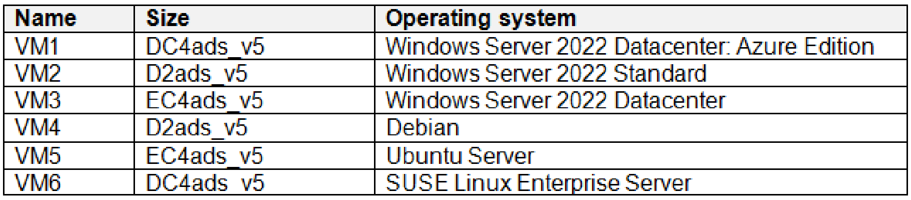
Question #70 *Topic 3*

HOTSPOT

-

You have an Azure subscription.

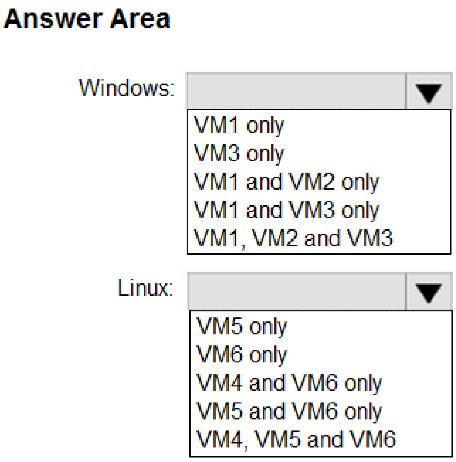
You plan to deploy the virtual machines shown in the following table.



Name	Size	Operating system
VM1	DC4ads_v5	Windows Server 2022 Datacenter: Azure Edition
VM2	D2ads_v5	Windows Server 2022 Standard
VM3	EC4ads_v5	Windows Server 2022 Datacenter
VM4	D2ads_v5	Debian
VM5	EC4ads_v5	Ubuntu Server
VM6	DC4ads_v5	SUSE Linux Enterprise Server

You need to identify the virtual machines and operating systems that can be deployed as confidential virtual machines?

Which Windows virtual machines and which Linux virtual machines should you identify?

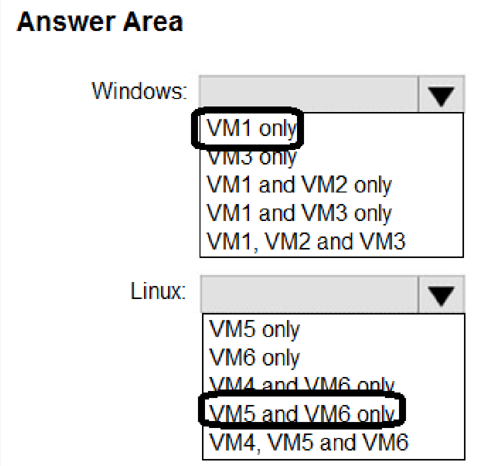


Answer Area

Windows: ▼
- VM1 only
- VM3 only
- VM1 and VM2 only
- VM1 and VM3 only
- VM1, VM2 and VM3

Linux: ▼
- VM5 only
- VM6 only
- VM4 and VM6 only
- VM5 and VM6 only
- VM4, VM5 and VM6

Suggested Answer:



Answer Area

Windows: ▼
- [✓ VM1 only]
- VM3 only
- VM1 and VM2 only
- VM1 and VM3 only
- VM1, VM2 and VM3

Linux: ▼
- VM5 only
- VM6 only
- VM4 and VM6 only
- [✓ VM5 and VM6 only]
- VM4, VM5 and VM6

⊟ **Adrianwkh** Highly Voted 8 months, 3 weeks ago

Keyword: confidential, select the Size with a C in it

1 and 3

5 and 6

upvoted 14 times

⊟ **ca7859c** 2 weeks, 5 days ago

Great shortcut!

upvoted 1 times

⊟ **HadexJ** 2 months, 2 weeks ago

I love you

upvoted 1 times

⊟ **4f13cca** Most Recent 3 months ago

Can someone explain why vm3 is supported

upvoted 1 times

⊟ **Nhadipour** 4 months, 3 weeks ago

Azure Confidential VMs support DCasv5 and ECasv5 series

Windows: VM1, VM3
Linux: VM5, VM6

upvoted 2 times

⊟ **Viggy1212** 9 months, 1 week ago

For Linux VMs,

Only Ubuntu and SUSE are supported, Debian is not supported. Hence VM5 and VM6.
Given answer is correct for Linux.

For Windows VMs,

Server 2022 Standard is not supported, so you can ignore VM2. Other supported Windows versions are,
2019 server core and datacenter
2022 server, datacenter azure edition and azure core

https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview

Per Azure VM Type naming convention, subFamily (mostly second character), if its C, then its a Confidential computing. So, For Windows VM1 and VM3.

https://learn.microsoft.com/en-us/azure/virtual-machines/sizes/overview?tabs=breakdownseries%2Cgeneralsizelist%2Ccomputesizelist%2Cmemorysizelist%2Cstoragesizelist%2Cgpusizelist%2Cfpgasizelist%2Chpcsizelist

upvoted 1 times

⊟ **BeginLearningforPP** 9 months, 1 week ago

Confidential VMs support the following VM sizes:

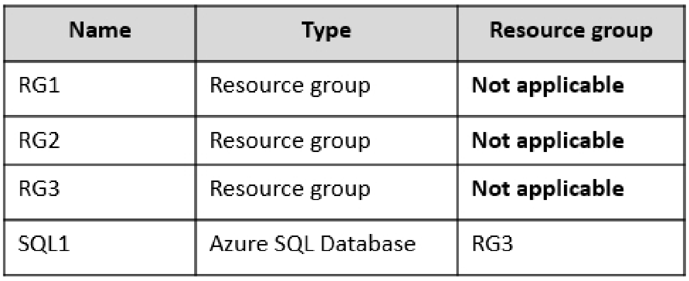
General Purpose without local disk: DCasv5-series, DCesv5-series
General Purpose with local disk: DCadsv5-series, DCedsv5-series
Memory Optimized without local disk: ECasv5-series, ECesv5-series
Memory Optimized with local disk: ECadsv5-series, ECedsv5-series
NVIDIA H100 Tensor Core GPU powered NCCadsH100v5-series

upvoted 1 times

Question #1 *Topic 4*

HOTSPOT -

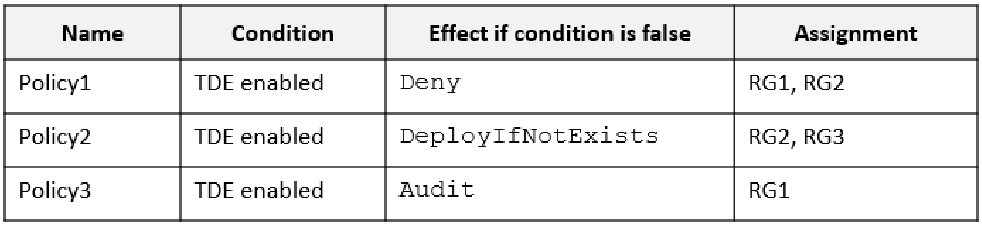
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Resource group
RG1	Resource group	**Not applicable**
RG2	Resource group	**Not applicable**
RG3	Resource group	**Not applicable**
SQL1	Azure SQL Database	RG3

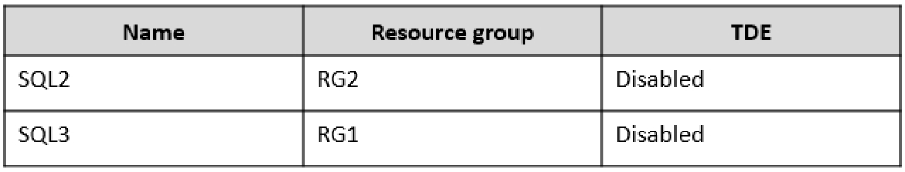
Transparent Data Encryption (TDE) is disabled on SQL1.

You assign policies to the resource groups as shown in the following table.



Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	`Deny`	RG1, RG2
Policy2	TDE enabled	`DeployIfNotExists`	RG2, RG3
Policy3	TDE enabled	`Audit`	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.

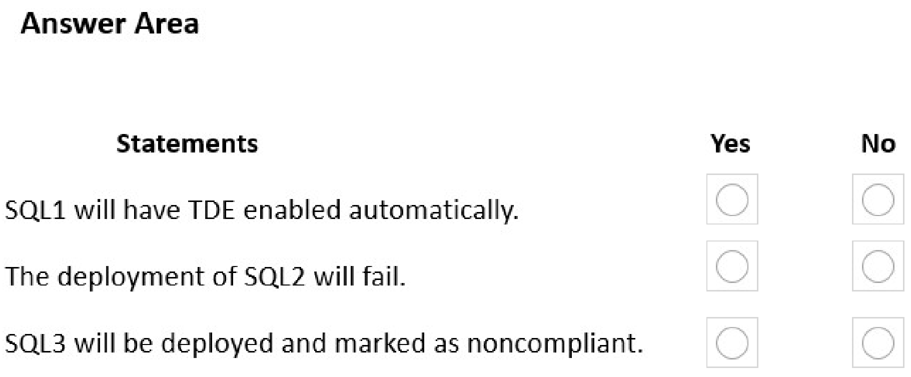


Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

NOTE: Each correct selection is worth one point.

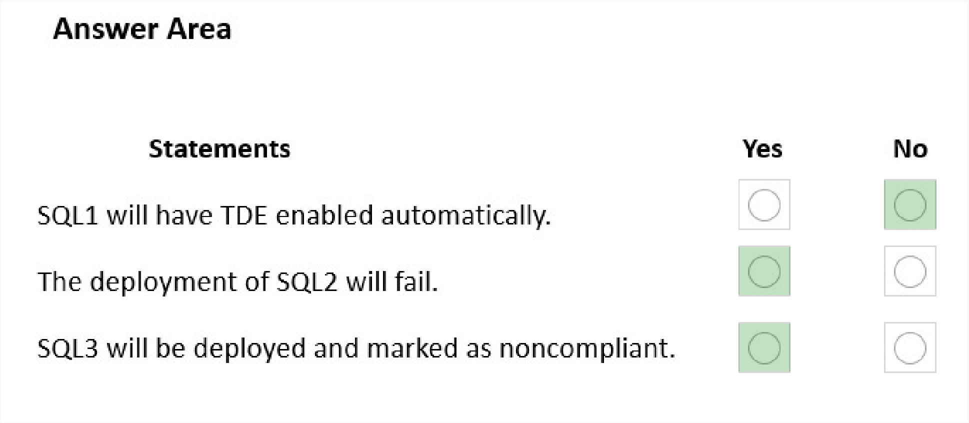
Hot Area:



Answer Area

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	○
The deployment of SQL2 will fail.	○	○
SQL3 will be deployed and marked as noncompliant.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	[✓ ○]
The deployment of SQL2 will fail.	[✓ ○]	○
SQL3 will be deployed and marked as noncompliant.	[✓ ○]	○

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

Kelly8023 Highly Voted 👍 2 years, 3 months ago

The answer should be No, Yes, No.

Reference: https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

After the Resource Provider returns a success code on a Resource Manager mode request, AuditIfNotExists and DeployIfNotExists evaluate to determine whether additional compliance logging or action is required.

So overall order of evaluation: Disabled -> Append/Modify -> Deny -> Audit -> AuditIfNotExists/DeployIfNotExists.

1st: No. DeployIfNotExists will be triggered after a configurable delay when a Resource Provider handles a create or update subscription or resource request and has returned a success code. In this scenario, because SQL1 is already deployed so it can not be enabled automatically.

2nd: Yes. Deny is processed first so can't be deployed

3rd: No. Deny is processed first

upvoted 26 times

> **somenick** 2 years, 2 months ago
>
> No - Policy2 will not enable TDE on SQL1 AUTOMATICALLY. You need to start remediation task.
>
> Yes - Deny is processed first
>
> No - Deny is processed first
>
> upvoted 11 times

dfranco76 Highly Voted 👍 2 years ago

Correcting typo in fonte explanation:

#1: SQL1 belongs in RG3, Policy #2, but DeployIfNotExists no apply (SQL1 was running before the policies were deployed.). SQL will be marked as not compliante.

#2: SQL2 is to be deployed in RG2, Policy #1 will apply, SQL2 will not be deployed.

#3: SQL3 is to be deployed in RG1, Policy #1 will apply, SQL3 will not be deployed.

FYI:

The order in which policies are applied is:

Disabled

Append and Modify

Deny

Audit

AuditIfNotExists and DeployIfNotExists

https://joefecht.com/posts/azure-policy-effects-and-paramters/

upvoted 8 times

> **fonte** 1 year, 11 months ago
>
> Thanks for the correction... It was a clear mistake on my side.
>
> upvoted 1 times

randy0077 Most Recent 🕘 3 months, 1 week ago

yny : https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-basics#policy-rule-evaluation

upvoted 1 times

> **randy0077** 3 months, 1 week ago
>
> correction: nyn : https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-basics#policy-rule-evaluation
>
> upvoted 1 times

yonie 12 months ago

Deny is processed first

No

Yes

No

upvoted 1 times

flafernan 1 year, 1 month ago

NO, YES, NO

upvoted 1 times

wardy1983 1 year, 2 months ago

After the Resource Provider returns a success code on a Resource Manager mode request, AuditIfNotExists and DeployIfNotExists evaluate to determine whether additional compliance logging or action is required.
So overall order of evaluation: Disabled -> Append/Modify -> Deny -> Audit -> AuditIfNotExists/DeployIfNotExists.
1st: No. DeployIfNotExists will be triggered after a configurable delay when a Resource Provider handles a create or update subscription or resource request and has returned a success code. In this scenario, because SQL1 is already deployed so it can not be enabled automatically.
2nd: Yes. Deny is processed first so can't be deployed
3rd: No. Deny is processed first

upvoted 1 times

majstor86 1 year, 9 months ago

NO
YES
NO

upvoted 3 times

ltjones12 2 years ago

@fonte, SQL1 belongs in RG3, not RG1.

upvoted 4 times

fonte 1 year, 11 months ago

Yep, my bad.
It's one of those cases where at least I would still chose the same answer despite the mistake.

Btw, I have no memory of having commented on this question. Sleep deprivation is a serious thing :|

upvoted 1 times

fonte 2 years ago

No, Yes, No.
#1: SQL1 belongs in RG1, Policy #1 and #3 apply, but the deny is not retroactive. SQL will be marked as not compliante.
#2: SQL2 is to be deployed in RG2, Policy #1 will apply, SQL2 will not be deployed.
#3: SQL3 is to be deployed in RG1, Policy #1 will apply, SQL3 will not be deployed.

upvoted 1 times

JohnBentass 2 years ago

Correct answer is No, Yes, No

upvoted 1 times

Muaamar_Alsayyad 2 years, 2 months ago

No
Yes
No
Policy will not be applied to already created resources, it might mark them as incopliant
for SQL1 we need to run remediation task to add TDE

upvoted 2 times

Muaamar_Alsayyad 2 years, 2 months ago

Sorry after testing in the lab answer is
Yes
YEs
NO,

plicy evaluaiton order
Disabled
append/moidfy
Deny
audit
auditIfNotExist and DeployIfNotExist

upvoted 6 times

kabooze 2 years ago

I don't understand why you changed your mind on #1 ? It says here that

"Existing non-compliant resources can be remediated with a remediation task."

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists-evaluation

upvoted 2 times

dakasa 2 years, 3 months ago

Y - Deny will not take effect, but "deployifnotexist" will.

Y - Will not be created "Deny" will be evaluated

N - Will not be created "Deny" will be evaluated

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

upvoted 8 times

sivva 2 years, 3 months ago

So what is the correct answer

upvoted 1 times

joanjcanals 2 years, 3 months ago

All answers are wrong:

1st: SQL1 is already deployed so cannot be denied, then deployifNotExist enables TDE

2nd: Deny is processed first so no chance to be deployed (end)

3rd: Deny again, same reason of the 2nd

upvoted 1 times

joanjcanals 2 years, 3 months ago

sorry, 2nd was OK. LOL

upvoted 1 times

kabooze 2 years ago

Existing non-compliant resources can be remediated with a remediation task.

so that's not automatically for #1

upvoted 2 times

joanjcanals 2 years, 3 months ago

My 1st was partially wrong: Deny does not apply to SQL1, so deployifnotexist enables TDE anyway

upvoted 1 times

charlesr1700 2 years, 3 months ago

I was confused about SQL1, at an initial glance I thought it looked liked it should be enabled automatically. However deployifNotExist policies are not retroactive. They only apply to resources that are created after the policy is assigned

When creating a DINE policy assignment in the Az Portal a pop up reads:

"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 2 times

haitao1234 2 years, 7 months ago

SQL3 should be denied, since it falls under deny and audit policy.

Definitely deny is more restrictive..

upvoted 2 times

haitao1234 2 years, 7 months ago

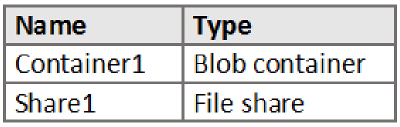
Each assignment is individually evaluated. As such, there isn't an opportunity for a resource to slip through a gap from differences in scope. The net result of layering policy definitions is considered to be cumulative most restrictive. As an example, if both policy 1 and 2 had a deny effect, a resource would be blocked by the overlapping and conflicting policy definitions.

upvoted 1 times

Question #2 *Topic 4*

HOTSPOT -

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named storage1 that contains the resources shown in the following table.



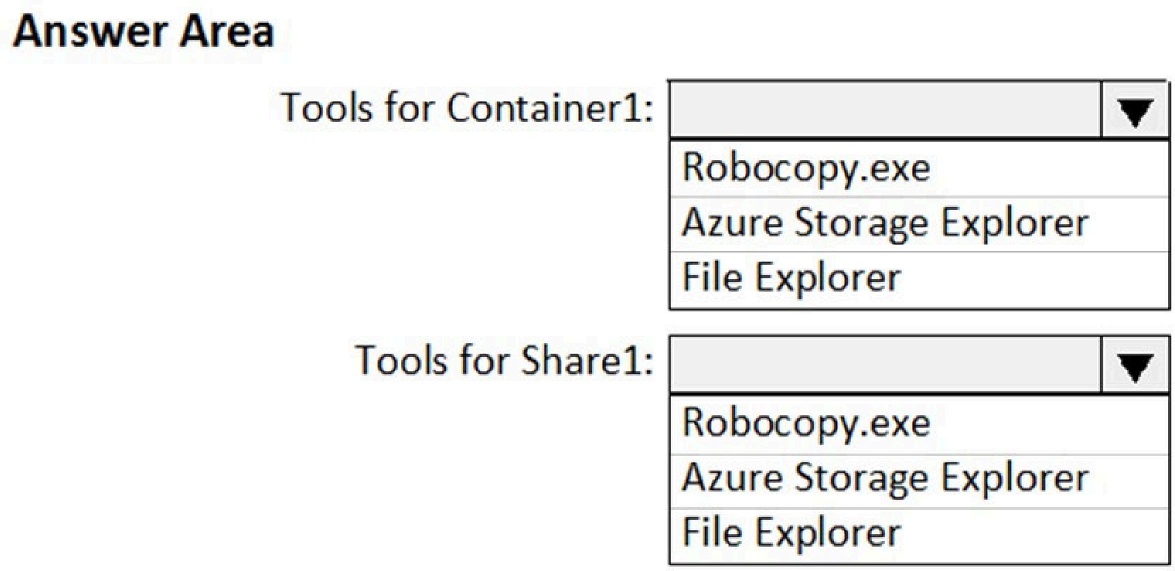
Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

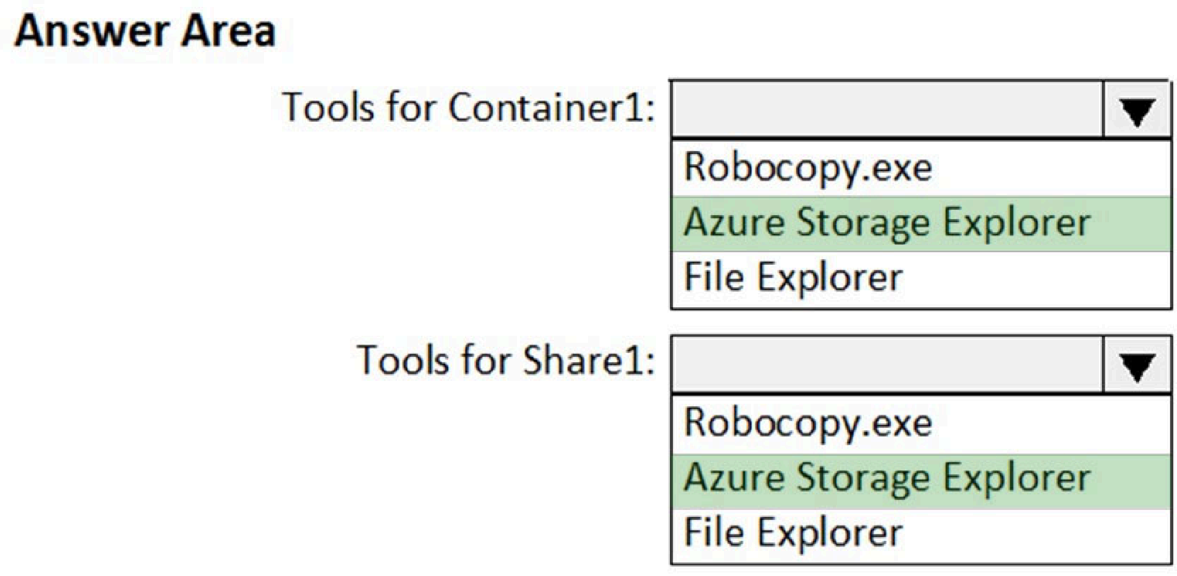


Answer Area

Tools for Container1:
- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Tools for Share1:
- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Suggested Answer:



Answer Area

Tools for Container1:
- Robocopy.exe
- [✓ Azure Storage Explorer]
- File Explorer

Tools for Share1:
- Robocopy.exe
- [✓ Azure Storage Explorer]
- File Explorer

Cisna Highly Voted 4 years, 1 month ago

in exam 02/05/2021

upvoted 21 times

8de3321 6 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/storage/storage-explorer/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows#:~:text=Shared%20access%20signature%20(SAS)%20URL

Read this exact part and you should find the answer to the question.

upvoted 1 times

JohnYinToronto Highly Voted 4 years, 3 months ago

answers correct

https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows

upvoted 15 times

91743b3 Most Recent 10 months, 3 weeks ago

On exam Aug 6 2024

upvoted 2 times

sudowhoami 10 months, 3 weeks ago

Is this dump still valid? Please let me know. I will be taking this exam in a few days.

upvoted 1 times

InfoSecGuy93 1 year ago

In exam

upvoted 1 times

foobar1985 1 year, 9 months ago

in exam 11/09/2023

upvoted 8 times

heatfan900 1 year, 10 months ago

using SAS you connect to both via the STORAGE EXPLORER thick client (too)

upvoted 2 times

Self_Study 1 year, 10 months ago

On an exam on 7/8/23, agree with the answer provided.

upvoted 4 times

majstor86 2 years, 3 months ago

Tools for Container1: Azure Storage Explorer

Tools for Share1: Azure Storage Explorer

upvoted 5 times

ligu 2 years, 4 months ago

Answers are correct

upvoted 2 times

another2 2 years, 5 months ago

if i'm not wrong this one was on an exam 7january2023.

upvoted 5 times

Diallo18 2 years, 8 months ago

In Exam 10/18/2022. One case study(6 ques), no lab.

upvoted 2 times

Diallo18 2 years, 8 months ago

In Exam 10/18/2022. One case study(6 ques), no lab.

upvoted 2 times

TtotheA2021 2 years, 11 months ago

answers are correct

upvoted 2 times

Exams_Prep_2021 3 years ago

In Exam - 20/6/2022 - 1 Case Study (6) - Lab (10 Tasks)

upvoted 5 times

tnagy 2 years, 11 months ago

What the lab was about?

upvoted 1 times

Irishtk 3 years, 1 month ago

Correct answer. "Storage Explorer can connect to a storage account using a connection string with a Shared Access Signature (SAS)" https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows

upvoted 4 times

⊟ **Eltooth** 3 years, 3 months ago

ASE

ASE

upvoted 2 times

⊟ **WhalerTom** 3 years, 6 months ago

Correct answer. In exam Dec 21. 40 questions, 1 case study, no labs.

upvoted 2 times

Question #3 *Topic 4*

You have an Azure Storage account named storage1 that has a container named container1.
You need to prevent the blobs in container1 from being modified.
What should you do?

A. From container1, change the access level.

B. From container1, add an access policy.

C. From container1, modify the Access Control (IAM) settings.

D. From storage1, enable soft delete for blobs.

Suggested Answer: *B*
References:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal

Community vote distribution
B (100%)

romanaa Highly Voted 4 years, 10 months ago
so many repetitions
upvoted 21 times

kiketxu 4 years, 9 months ago
agree!
upvoted 6 times

kumax Highly Voted 4 years ago
On exam, May 2021.
upvoted 11 times

pentium75 Most Recent 11 months ago
Selected Answer: B
Tricky because "Access policy" usually refers to the stored access policies for SAS. But under the same item there is also the "immutable blob storage" policy which is what we need.
upvoted 2 times

majstor86 2 years, 3 months ago
Selected Answer: B
B. From container1, add an access policy.
upvoted 5 times

ligu 2 years, 4 months ago
The answer is correct
upvoted 2 times

Irishtk 3 years, 1 month ago
Correct. Configure immutable storage policy on container.
https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-policy-configure-container-scope?tabs=azure-portal
upvoted 5 times

pentium75 11 months ago
Yes, but "Configure immutable storage policy" is something else than "add an access policy". The latter refers to stored access policies for SAS, and ADDING one will not change anything.
upvoted 1 times

Eltooth 3 years, 3 months ago
Selected Answer: B
B is correct answer.
upvoted 5 times

Patchfox 3 years, 6 months ago

I think B fits best but it should be called sth. like immutable - time based retention. The access policy is only for sas tokens.
Answer A makes the container in any kind public available, we don't want that. C needs specific principles to assign a role (like blob data reader) and D bringt the the container in a delete process.

upvoted 3 times

⊟ **arytech** 4 years ago

Why not A? it meets the goal as described in https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-configure?tabs=portal.
In the other hand, Access policy sounds tricky as an answer althoug immutable storage is a kind of policy https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage. What do you think?

upvoted 2 times

⊟ **smilinghacker** 3 years, 5 months ago

Because A is not right here.

upvoted 2 times

⊟ **mayenite** 4 years, 5 months ago

Given answer is correct

upvoted 7 times

Question #4 *Topic 4*

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to create several security alerts by using Azure Monitor.
You need to prepare the Azure subscription for the alerts.
What should you create first?

A. an Azure Storage account

B. an Azure Log Analytics workspace

C. an Azure event hub

D. an Azure Automation account

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **fpspam** Highly Voted 4 years, 11 months ago

I think this is correct. Source: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

upvoted 18 times

⊟ **poplovic** Highly Voted 3 years, 9 months ago

basically, you need LAW to store the security-related logs and use Kusto to query the logs. Base on the result of query, create security alert. Therefore, you have to create LAW first.

B is correct

upvoted 10 times

⊟ **91743b3** Most Recent 10 months, 3 weeks ago

On exam Aug 6 2024

upvoted 3 times

⊟ **foobar1985** 1 year, 9 months ago

in exam 11/09/2023

upvoted 4 times

⊟ **ExamStudy68** 2 years, 3 months ago

I think the answer is correct. Looking at this link it doesn't say anywhere to register first... https://learn.microsoft.com/en-us/previous-versions/azure/azure-monitor/app/availability-multistep#dealing-with-sign-in

In addition, multi-step web tests have been deprecated "Multistep web tests have been deprecated. We recommend using TrackAvailability() to submit custom availability tests instead of multistep web tests."

upvoted 1 times

⊟ **majstor86** 2 years, 3 months ago

Selected Answer: B

B. an Azure Log Analytics workspace

upvoted 2 times

⊟ **ligu** 2 years, 4 months ago

B is correct answer

upvoted 1 times

⊟ **F117A_Stealth** 2 years, 7 months ago

Selected Answer: B

B. an Azure Log Analytics workspace

upvoted 1 times

⊟ **NinjaSchoolProfessor** 2 years, 11 months ago

In exam 15-July-2022

upvoted 3 times

⊟ **Eltooth** 3 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

SecurityAnalyst 3 years, 10 months ago

# IN EXAM - 31/8/2021

upvoted 4 times

Rajesh123 4 years ago

ALA can store logs from 30 to 730 days (2 years)

upvoted 1 times

JohnYinToronto 4 years, 3 months ago

answer correct

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace

upvoted 4 times

deegadaze1 4 years, 4 months ago

in Exam

upvoted 7 times

tuta 4 years, 6 months ago

this page has too many repeatitions

upvoted 4 times

Question #5 *Topic 4*

You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights.
WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.
Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.
You need to ensure that web tests can run unattended.
What should you do first?

A. In Microsoft Visual Studio, modify the .webtest file.

B. Upload the .webtest file to Application Insights.

C. Register the web test app in Azure AD.

D. Add a plug-in to the web test app.

Suggested Answer: *B*

Community vote distribution

C (77%) B (23%)

Elpresidento27 Highly Voted 👍 4 years, 4 months ago

C is correct answer. The context of the question is from a Security/Access/Identities perspective, and not from developer's perspective. Check the answer here, section "Client Secret":

https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep#dealing-with-sign-in

upvoted 41 times

sureshatt 4 years, 3 months ago

I will also go with this answer. I would accept B if the app did not needed the client secret. But in this case, you need to get a token using client secret. For this, you need to first of all register your test app in Azure AD so that it can request tokens.

upvoted 12 times

111ssy Highly Voted 👍 4 years, 10 months ago

Correct answer: B

upvoted 16 times

91743b3 Most Recent 🕘 10 months, 3 weeks ago

On exam Aug 6 2024

upvoted 3 times

wardy1983 1 year, 7 months ago

Answer: C
Explanation:
The context of the question is from a Security/Access/Identities perspective, and not from developer's
perspective. Check the answer here, section "Client Secret":
https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep#dealing-with-sign-in

upvoted 2 times

heatfan900 1 year, 10 months ago

The answer is C. The question clearly states that WebApp1 requries OAuth 2.0 which is performed via Azure AD. Also, from MICROSOFT BELOW:

You'll need to create an app registration to use in your test environment.

This is the premise of this question. What is required from authentication standpoint to get this going.

upvoted 5 times

fahrulnizam 2 years, 2 months ago

Selected Answer: B

B. Upload the .webtest file to Application Insights

upvoted 2 times

d365ppp 2 years, 2 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/active-directory/develop/test-setup-environment

Multi-step test is deprecated. The answer is C

upvoted 4 times

d365ppp 2 years, 2 months ago

Most likely, this question will not appear as it is deprecated.

upvoted 2 times

ExamStudy68 2 years, 3 months ago

I think the answer is correct. Looking at this link it doesn't say anywhere to register first... https://learn.microsoft.com/en-us/previous-versions/azure/azure-monitor/app/availability-multistep#dealing-with-sign-in

In addition, multi-step web tests have been deprecated "Multistep web tests have been deprecated. We recommend using TrackAvailability() to submit custom availability tests instead of multistep web tests."

upvoted 1 times

majstor86 2 years, 3 months ago

Selected Answer: B

B. Upload the .webtest file to Application Insights.

upvoted 1 times

rgbykkk 2 years, 5 months ago

Going by the question, the web app is already registered 'sub1 contains azure web app name webApp1'. So answer must be B

upvoted 3 times

Fal991l 2 years, 4 months ago

AI: Azure Application Insights is a service that helps developers monitor and diagnose issues in web applications by collecting telemetry data from various sources, including web servers, custom code, and other Azure services. In order to authenticate users and authorize access to resources in Azure, web apps need to be registered in Azure AD.

Therefore, to ensure that the web test app can authenticate with WebApp1, you would need to register the WebApp1 in Azure AD and configure it to use OAuth 2.0 client secrets for authentication.

upvoted 3 times

Kelly8023 2 years, 8 months ago

Multi-step web test has been deprecated.

https://learn.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep

upvoted 2 times

mung 2 years, 7 months ago

So it won't come up on the exam right?

upvoted 2 times

omkhan 2 years, 10 months ago

B is the correct Answer in this scenario

upvoted 2 times

[Removed] 2 years, 11 months ago

Answer B is correct

https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep

upvoted 2 times

Irishtk 3 years, 1 month ago

Answer A. Use Visual Studio to mod the token parameters returned during OAuth authentication.

see the Open Authentication section

https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep

f your test must sign in using OAuth, the general approach is:

Use a tool such as Fiddler to examine the traffic between your web browser, the authentication site, and your app. Perform two or more sign-ins using different machines or browsers, or at long intervals (to allow tokens to expire). By comparing different sessions, identify the token passed back from the authenticating site, that is then passed to your app server after sign-in. Record a web test using Visual Studio. Parameterize the tokens, setting the parameter when the token is returned from the authenticator, and using it in the query to the site.

upvoted 1 times

samatar 3 years, 6 months ago