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

Custom View Settings

Topic 1 - Question Set 1

https://t.me/learningnets

Question #1 Topic 1

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

Correct Answer: *B*
Creating a new (additional) stored access policy with have no effect on the existing policy or the SASλ€™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

JohnCrawford Highly Voted 1 year, 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 43 times

awssecuritynewbie 9 months, 2 weeks ago
i agree, it just says create a new policy not " delete" or revoke the existing one that has caused this issue
upvoted 3 times

S_Khan Highly Voted 1 year, 4 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 18 times

peacegrace 2 months, 3 weeks ago
NO . Becaz .....Creating a new (additional) stored access policy with have no effect on the existing policy or the SASλ€™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 2 times

gchristina 2 months, 2 weeks 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

Deepmindx Most Recent 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 3 times

poplovic 3 weeks, 2 days ago
B is correct
https://docs.microsoft.com/en-us/rest/api/storageservices/create-service-sas#revocation-of-a-sas
The stored access policy referenced by the SAS is deleted, which revokes the SAS. If Azure Storage cannot locate the stored access policy specified in the shared access signature, the client is not able to access the resource indicated by the URI.

https://t.me/learningnets

If you recreate the stored access policy with exactly the same name as the deleted policy, all existing SAS tokens will again be valid according to the permissions associated with that stored access policy, assuming that the expiry time on the SAS has not passed. If you are intending to revoke the SAS, be sure to use a different name if you recreate the access policy with an expiry time in the future.

upvoted 1 times

kumax 3 weeks, 4 days ago

on exam

upvoted 3 times

rpm1234567 3 weeks, 3 days ago

Hi Kumax,
Can you confirm , is there any simulation and lab is available or not and also share exact questions and answers was appeared on the exam.

upvoted 1 times

KudlaTiger 1 month, 3 weeks ago

"Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant" - Is it not on-premise policies ?

upvoted 1 times

jessicamendez10 3 months, 3 weeks ago

In exam 20/03/2021

upvoted 2 times

sensa 4 months, 2 weeks ago

in exam..1

upvoted 2 times

abilioneto 4 months, 3 weeks ago

I believe the correct answer is "no".
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

upvoted 1 times

dadageer 5 months ago

Creating a new access policy will have no affect on the policy already there. Unless you delete or edit that policy a new policy is not going to change anything. I think the answer is 'No'.

upvoted 1 times

mayenite 5 months ago

In exam

upvoted 2 times

milind8451 5 months, 1 week ago

Right ans. Go to Storage account -> "Storage Explorer" -> Select your container and right click on it -> Click on "Get Shared Access Signature", here you get option to select Access policy and you can define timebound access. So given answer and logics are correct.

upvoted 1 times

MrGarak1 5 months, 2 weeks ago

in exam

upvoted 2 times

zhanabaur 5 months, 3 weeks ago

I'd vote for No, because: 'To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past.'. No info that to revoke access you need to create a new stored access policy.

upvoted 1 times

ham56141 5 months ago

I think the answer is No too. But technically you can create a new stored access policy with the same ID as the current one, with an expiry date in the past.

upvoted 1 times

Hacker1420 5 months, 3 weeks ago

Answer is Yes, refer section - 'Best practices when using SAS' and point - 'Define a stored access policy for a service SAS' from below link
Link - https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

upvoted 1 times

AshTac 5 months, 3 weeks ago

I believe the answer is Yes - In this article under Best Practises when using SAS, under section headed "Define a stored access policy for a service SAS." It mentions that this gives you the option of revoking permissions.

upvoted 1 times

Gathix444 5 months, 3 weeks ago

Take a look at topic1 question 1,2,16 and 21, they are the same questions. 1,16,21 are obviously wrong, so i dare to say 2 is "yes". We call know MS has some badly worded questions. Create a new stored access policy makes sense.

https://t.me/learningnets

upvoted 2 times

https://t.me/learningnets

Question #2 *Topic 1*

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

Correct 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

gfhbox0083 Highly Voted 1 year ago
B, for sure.
upvoted 7 times

justinp Most Recent 5 days, 9 hours ago
this question was in the test today
upvoted 1 times

markozoide 1 week, 2 days ago
es B, se pasa solo
upvoted 1 times

FK2974 4 months, 1 week ago
Correct answer B!
upvoted 1 times

abilioneto 4 months, 3 weeks ago
Yes, my guess is B
upvoted 1 times

ChandraSekhar 5 months ago
In the explanation provided , where is the use of Hybrid Active Directory ? Where is the Authentication happening without using Active Directory ?
upvoted 2 times

milind8451 5 months, 1 week ago
Right ans.
upvoted 1 times

kiketxu 7 months, 3 weeks ago
No doubts. B
upvoted 1 times

Mehblah 8 months ago
Yes B is the answer
upvoted 2 times

wzlinux 10 months, 1 week ago
I choos B
upvoted 2 times

https://t.me/learningnets

AS007 1 year, 2 months ago

Given answer is correct

upvoted 4 times

https://t.me/learningnets

Question #3 *Topic 1*

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

Correct 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

cloudguy365 Highly Voted 1 year, 2 months 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 30 times

server1 10 months, 2 weeks ago
excellent observation - we have to read the question carefully
upvoted 2 times

PDR Highly Voted 1 year, 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 13 times

kiketxu 9 months, 3 weeks 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 2 times

gagofure Most Recent 1 month, 3 weeks ago
Answer =NO
If you have an on-premises Active Directory instance or more complex Active Directory setups for your domain, you can sync those identities to Azure AD by using Azure AD Connect. You can then enable Azure AD DS on that Active Directory tenant.

https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture#on-premises-active-directory-or-active-directory-on-iaas-vms
upvoted 2 times

Lb83 2 months, 1 week ago
The chosen answer details how you would connect a HD insight cluster to an on prem network so that you could access over a VPN. The ability to allow the use of domain creds requires that Azure Active Directory Domain Services and the Enterprise Security Package be enabled. A no

https://t.me/learningnets

from me.
upvoted 2 times

Pinto 4 months ago
Answer is NO.
https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-create-configure-enterprise-security-cluster
upvoted 3 times

FK2974 4 months, 1 week ago
Given answer is correct Yes!
upvoted 2 times

azurecert2021 4 months, 3 weeks ago
correct answer is NO
VPN is incomplete solation
upvoted 2 times

milind8451 5 months, 1 week ago
Answer is correct but partially as it needs more step to authenticate using on-prem AD. Establishing S2S VPN is the first step.
upvoted 1 times

PaulRSE 5 months, 4 weeks ago
I think the correct answer is "Yes".

Here is why:
Question states: "You have a hybrid configuration of Azure Active Directory (Azure AD)."
So, AAD Connect is already installed and configured.
Question states: "You have an Azure HDInsight cluster on a virtual network."
You already have HDInsight configured.
Question States: "You 'plan' to allow users to authenticate to the cluster by using their on-premises Active Directory credentials."
Key word, "plan"
Question states: "You need to configure the environment to support the planned authentication."
The next logical step is to create the site-to-site VPN so that users can authenticate, using whatever method configured for authentication, using HDInsight. The VPN is needed so it meets the goal.
upvoted 7 times

nyflash1 6 months, 3 weeks ago
top 5 worst question, due to ambiguity...
upvoted 2 times

Ammugaa 7 months ago
Connection on Site-to-Site VPN is encrypted. It does not have anything to do with Authentication. For Authentication to happen, Active directory needs to connect to Azure AD.

Answer would be : NO
upvoted 1 times

Bluediamond 10 months, 1 week ago
Answer is correct. Read the question it says "You need to configure the environment to support the planned authentication." S2S will support the environment. Granted you need more like Azure AD connect ect.
upvoted 7 times

Sethoo 7 months, 1 week ago
Agree with your assessment. people are reading too much into this question. It is not about authentication but preparation towards authentication. What do you have to do before you can even authenticate? That is what the question is about. So the answer appears to be correct.
upvoted 3 times

wzlinux 10 months, 1 week ago
I choose B
upvoted 2 times

nidoz 10 months, 3 weeks ago
Guys part of question is "You need to configure the environment to support the planned authentication."
so setting up a VPN is definitely part of solution and then there comes planned authentication. My take here is YES
upvoted 2 times

gfhbox0083 1 year ago
A, for sure.
upvoted 4 times

idnildeb40 10 months, 3 weeks ago
Please justify
upvoted 2 times

kratos13 1 year ago
A lot of ambiguity (thanks Microsoft). I want to say "answer is correct" based on this article ::
~ https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

https://t.me/learningnets

upvoted 2 times

skb1996 1 year, 1 month ago

I think the main reason is to see how HDinsight authentication works out with ad, but I agree they are discussing identity and asking network security.

upvoted 1 times

https://t.me/learningnets

Question #4 Topic 1

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)

Correct 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

Ace786 Highly Voted 10 months, 2 weeks ago
PTA for sure as you need to enforce on prem password policies hence pass through to on prem
upvoted 20 times

rgullini 2 months, 4 weeks 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 2 times

Ilko Highly Voted 6 months, 4 weeks 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 18 times

ChinkSantana 1 week, 5 days 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

https://t.me/learningnets

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 1 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 3 times

babusartop17 2 weeks, 2 days ago

Advanced scenarios. Pass-through Authentication enforces the on-premises account policy at the time of sign-in. For example, access is denied when an on-premises user's account state is disabled, locked out, or their password expires or the logon attempt falls outside the hours when the user is allowed to sign in.

upvoted 1 times

Frosticus 2 weeks, 6 days ago

Answer is correct. pass the hash does enforce password policies and is less complex
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

upvoted 1 times

kumax 3 weeks, 4 days ago

On exam May, 2021.

upvoted 3 times

rpm1234567 3 weeks, 3 days ago

Hi Kumax,
what is you contact no or mail id. i am going to write exam next 2 days, i need your guidance to clear the exam

upvoted 1 times

Rajesh123 1 month, 1 week ago

PHS is correct due to less server to manage

upvoted 1 times

mailme 1 month, 1 week ago

Answer is C
Key is "Policy enforcement"
There is a decision tree in below link it clarifies all confusions.
Reference
"https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

upvoted 2 times

teehex 2 months ago

You are all tricked if you select C. PTA supports user-level policy enforcement and requires additional server for agent deployment. PHS (Password Hash Sync) does support PASSWORD policy by this property EnforceCloudPasswordPolicyForPasswordSyncedUsers (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization). The decision tree (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#decision-tree) doesn't say anything about password policy. Instead it uses user-level policy which is more than password

upvoted 4 times

peacegrace 2 months, 1 week ago

in exam in April 2021

upvoted 1 times

mailto_farhanraza 2 months, 1 week ago

Correct Answer is C

upvoted 2 times

Lb83 2 months, 1 week ago

Pass through Auth FTW. The authentication is passed directly to On premise AD servers. Technically you only need to install a single lightweight agent for this to work. You can install on multiple servers for resilience which is recommended. This means though that real-time policies are in effect. Password hash synchronisation would have limitations such as disabled accounts (upto 30 min delay) , on prem account lockouts not synched (have to use smart lock), password expiry not synced and logon hours (not synced)

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

lastly password policy sync - PTA , here is a good article, look at the table at the bottom
https://www.itpromentor.com/compare-sso/

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

Also PTA requires less infrastructure

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

PTA for sure - if there was no DC and if AAD was only used then PHS.

https://t.me/learningnets

We AD and DC then we use AD Connect to sync to AAD - PTA

upvoted 1 times

MQH 2 months, 2 weeks ago

it should be C as mentioned also in this tree :
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#:~:text=solution-,decision tree,-Details

upvoted 1 times

t2khan 2 months, 2 weeks ago

The answer is Pass-through for sure. If you carefully read the question its showing
*You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant (till here Password-hash could be the solution with only have to deploy AD Connect without any additional infra structure)
Then FOCUS on the next requirement =>
*Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant (this will clarify that the authentication is happening on the on-premises site not at the cloud and policy need to be enforced so Pass-through will be the correct answer)
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-user-signin

Please upvote to make it easier for future learners. thanks

upvoted 10 times

https://t.me/learningnets

Question #5 Topic 1

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

Correct 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

AS007 Highly Voted 1 year, 2 months ago
Correct Answer
upvoted 17 times

Fred64 Most Recent 3 months, 3 weeks ago
answer A
upvoted 2 times

finolweb 4 months, 4 weeks ago
In exam
upvoted 4 times

zic04 5 months, 3 weeks ago
A correct answer
upvoted 2 times

zic04 6 months ago
Correct Answer
upvoted 2 times

B1T3X 6 months, 1 week ago
Answer is correct.
Documentation: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-create-custom-sync-rule
upvoted 1 times

tuta 7 months ago
A is correct
upvoted 2 times

Attaxhan 11 months, 3 weeks ago
IN THE EXAM I CHOOSE A
upvoted 2 times

gfhbox0083 1 year ago
A, for sure.
Synchronization Rules Editor
upvoted 4 times

mackc13 1 year ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

Answer is correct
upvoted 4 times

kristiann21 1 year, 1 month ago
I have implemented editing attributes synchronization in Azure AD Connect. And this possible with the Azure AD connect rules editor, which edits the synchronization rules.

https://t.me/learningnets

upvoted 4 times

https://t.me/learningnets

Question #6 *Topic 1*

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.

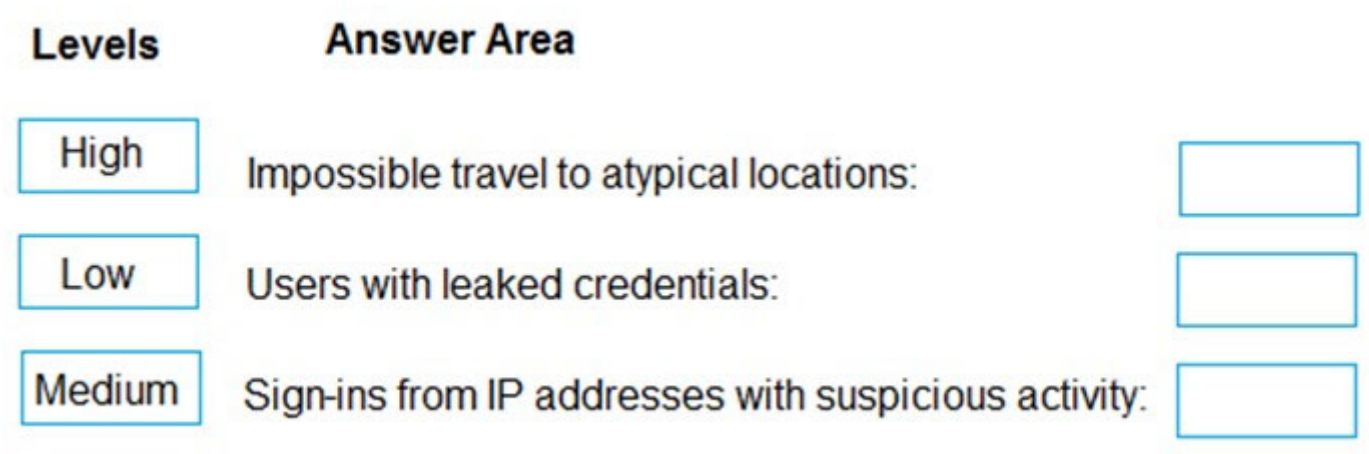
You need to identify the risk level of the following risk events:

- Users with leaked credentials
- Impossible travel to atypical locations
- Sign-ins from IP addresses with suspicious activity

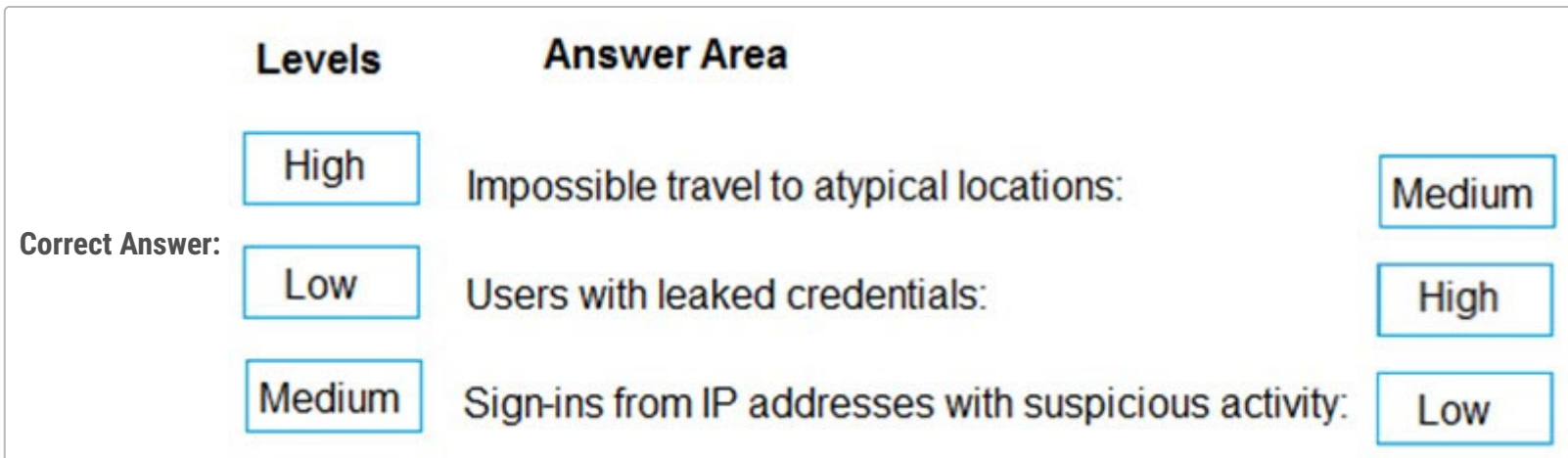
Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



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:

https://t.me/learningnets

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/

Oz Highly Voted 1 year, 7 months ago

True!
It's going to be:
Medium
High
Medium

upvoted 31 times

wongtony 1 month, 3 weeks ago

But it's a drag-and-drop, the option can only be used once.

upvoted 1 times

kimalto452 1 month, 1 week ago

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.

upvoted 1 times

Adamasbue Highly Voted 1 year, 7 months ago

Wrong see: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign-ins-from-ip-addresses-with-suspicious-activity

upvoted 27 times

peacegrace 2 months, 3 weeks ago

Adamasbue..the link you gave makes no sense. It just lists risks but does NOT give High - Medium - Low. Please read properly.

upvoted 3 times

awssecuritynewbie 9 months, 2 weeks ago

i know but if you look at this link you see it is the right answer i though first it was M , H , M but it is not the fact please check it out before deciding

https://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/#:~:text=These%20six%2Dtypes%20of%20events,%E2%80%93%20High%2C%20Medium%20%26%20Low.&text=We%20can%20use%20these%20risk,to%20protect%20sensitive%20application%20access.

upvoted 4 times

Dineshvishe Most Recent 1 week, 5 days ago

The answer is correct. In the description table, it is directly mapped one-one. The same table is provided by Microsoft. The main reason people get it wrong in exams is 1. Sometimes the things are simple but people try to find complexities in it. 2. Overthinking.

upvoted 1 times

mckiito 3 weeks, 2 days ago

Answer is wrong. It should be MHM. See Login from a suspicious IP Your resource has been accessed successfully from an IP address that Microsoft Threat Intelligence has associated with suspicious activity.) PreAttack Medium
or
Login from a suspicious IP
(SQL.PostgreSQL_SuspiciousIpAnomaly
SQL.MariaDB_SuspiciousIpAnomaly
SQL.MySQL_SuspiciousIpAnomaly) Your resource has been accessed successfully from an IP address that Microsoft Threat Intelligence has associated with suspicious activity. PreAttack Medium
search for suspicious activity on https://docs.microsoft.com/en-us/azure/security-center/alerts-reference

upvoted 2 times

mailme 1 month, 1 week ago

https://t.me/learningnets

Answer is correct.
Suspicious access to possibly vulnerable web page detected
(AppServices_ScanSensitivePage)

Azure App Service activity log indicates a web page that seems to be sensitive was accessed. This suspicious activity originated from a source IP address whose access pattern resembles that of a web scanner.
This activity is often associated with an attempt by an attacker to scan your network to try and gain access to sensitive or vulnerable web pages.
(Applies to: App Service on Windows and App Service on Linux) -

Low (Risk)

Reference
https://docs.microsoft.com/en-us/azure/security-center/alerts-reference

upvoted 1 times

sakibmas 2 months, 1 week ago

Threats are rated on the probability of compromise.

High: leaked credentials, malicious IP address

Medium: anonymous IPs, impossible travel, sign-ins from suspicious IP addresses, and unfamiliar locations

Low: sign-in from potentially infected devices, unfamiliar sign-in properties

upvoted 2 times

t2khan 2 months, 2 weeks ago

there is difference between *anonymous* (Medium) and *Suspicious* (Low) risk level. The answer is correct here as the sign in attempted from IP with suspicious activity considered as infected/malware device so it should be Low risk level. Hence the answer is correct.
*Medium
*High
*Low
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Please upvote to make it easier for future learners. thanks

upvoted 14 times

DCarma 3 weeks, 6 days ago

From that link:

"While Microsoft does not provide specific details about how risk is calculated, we will say that each level 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."

Honestly think this is an old question as these level are not even published by Microsoft, and people are using an old 'rebeladmin' page to justify their answers.

He even updated his article to say: "Due to security reasons, Microsoft does not provide exact details about how the risk levels are calculated. However, Microsoft says the following events contribute on risk level calculation."

upvoted 2 times

rodolfo2020 3 months, 3 weeks ago

Simulating risk detections in Identity Protection
06/05/2020
4 minutes to read

Administrators may want to simulate risk in their environment in order to accomplish the following items:

Populate data in the Identity Protection environment by simulating risk detections and vulnerabilities.
Set up risk-based Conditional Access policies and test the impact of these policies.
This article provides you with steps for simulating the following risk detection types:

Anonymous IP address (easy)
Unfamiliar sign-in properties (moderate)
Atypical travel (difficult)
Other risk detections cannot be simulated in a secure manner.

upvoted 1 times

Startkabels 3 months, 3 weeks ago

I have checked all risk level in my company's environment:
Leaked credentials: High
Impossible travel: Medium
Activity from suspicous IP: Medium
Activity from anonymous IP: Medium
Sign in from infected device: ?
Unfamiliar sign-in properties: Low

upvoted 4 times

zic04 5 months, 3 weeks ago

Medium / high / medium for me

upvoted 2 times

https://t.me/learningnets

Stuudent 8 months, 1 week ago

Seems outdated, direct quote:

Microsoft does not provide specific details about how risk is calculated

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

upvoted 8 times

deegadaze1 6 months, 1 week ago

check this-https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/media/concept-risk-events/91.png

upvoted 4 times

zhanabaur 7 months, 1 week ago

Agree, imho, it is up to the organization how to score the risk: H or M or L.

upvoted 2 times

deegadaze1 6 months, 1 week ago

No, it is not. Here is the link- https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/media/concept-risk-events/91.png

upvoted 2 times

shanan_ilen 8 months ago

Agree with you

upvoted 3 times

Cis 8 months, 3 weeks ago

Medium
High
Medium

upvoted 1 times

DeepMoon 9 months, 1 week ago

This is probably an old question that changed with newer updates to Azure.
Even Microsoft Tech writers are not able to answer this question: See Link below:
https://github.com/MicrosoftDocs/azure-docs/issues/63555#issuecomment-701546092

upvoted 5 times

awssecuritynewbie 9 months, 2 weeks ago

so sign in from unfaimilar location is not the same as "Sign-ins from IP addresses with suspicious activity " i just checked my own Azure tenant and it says that the answers provided are out of date .. can anyone confirm they got this in their exam recently please.

upvoted 2 times

kiketxu 9 months, 3 weeks ago

The answer is right. Seems the table was taken from here.
https://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/#:~:text=These%20six%2Dtypes%20of%20events,%E2%80%93%20High%2C%20Medium%20%26%20Low.&text=We%20can%20use%20these%20risk,to%20protect%20sensitive%20application%20access.

upvoted 1 times

kiketxu 9 months, 3 weeks ago

Upss, didn't saw the ref at the bottom, lol!

upvoted 1 times

pkasthur 9 months, 4 weeks ago

the answer should be Medium
High
Medium

upvoted 1 times

DrSushi 10 months ago

This one seems quite debatable.... one side here says: HIGH, MEDIUM, MEDIUM, the other side of the crowd seems embraces: HIGH, MEDIUM, LOW

Frankly speaking, the official page at Microsoft doesn't help much to settle this debate:

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

"While Microsoft does not provide specific details about how risk is calculated, we will say that each level 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 3 times

https://t.me/learningnets

Question #7 Topic 1

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.	○	○

Answer Area Yes,No,Yes

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.	○	○

Correct Answer:

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:

https://t.me/learningnets

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 ג€" High, Medium & Low:

References:

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

Geeky93 Highly Voted 4 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 39 times

rctm_bm Highly Voted 4 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 25 times

rgullini 2 months, 4 weeks ago

totally agree with rctm_bm

upvoted 2 times

JCWF 3 months, 3 weeks ago

Device containing malware refers to infected device which is Low Risk Level,

upvoted 3 times

rctm_bm 1 week ago

No. The only Low Risk Level is Sign-ins from IP addresses with suspicious activity. Everything else is medium\high

upvoted 2 times

cannibalcorpse 3 months, 1 week ago

Exactly,any event not related to credentials leakage, we may say as Low Risk Level.

upvoted 2 times

AcTiVeGrEnAdE 3 months, 4 weeks ago

I agree the answer should be YES, NO, YES.

upvoted 2 times

justinp Most Recent 5 days, 9 hours ago

this question was present in test today

upvoted 1 times

https://t.me/learningnets

babusartop17 2 weeks, 6 days ago

How about only a Certifed subject matter expert should give out answers and rest should take it easy? God, it's like a fish market in here -- you guys make things more confusing than the actual exam. Each person should be allowed only ONE answer period.

upvoted 3 times

ryta 1 month, 2 weeks ago

In my option, i think answer should be Y, Y for user 1 and 2 respectively. Simply because they both lie in the Medium and above catyegory. Answer for user 3 is tricky. What causes a computer to get malware?? Sign-ins from suspicious and unprotected ips right?? it could lie in medium or low priority.

upvoted 1 times

Dineshvishe 1 week, 5 days ago

The IP which is already suspicious, the risk level is defined as low. Hence the policy i not applicable. The answer is No.

upvoted 1 times

longtech 1 month, 2 weeks ago

The answer is wrong. it must be Y N Y. Because the policy is not set up for group 2. In addition, the user 3 sign in from malware which is considered with medium level, the user must change password.

upvoted 2 times

Ochman 1 month, 3 weeks ago

I felt that the answer should be Yes Yes Yes. Because the third option highlights he's connection from 1. an "Infected device" - (Risk Medium) 2. the device is also partaking in suspicious activities - (Risk Low). By virtue of point 1 the 3rd option should be yes too

upvoted 1 times

KudlaTiger 1 month, 3 weeks ago

Users with leaked credentials HIGH
Sign-ins from anonymous IP addresses MEDIUM
Impossible travel to atypical locations MEDIUM
Sign-ins from infected devices LOW
Sign-ins from unfamiliar locations MEDIUM
Sign-ins from IP addresses with suspicious activity LOW

upvoted 1 times

scks 1 month, 2 weeks ago

From where you got this info ? Please share

upvoted 3 times

Darvel 1 month, 3 weeks ago

Sign-ins from infected devices LOW >>> Are you sure? I need to see doc.

upvoted 2 times

teehex 2 months ago

User2 belong to Group1 and Group 2 but Group 2 is excluded so User2 is excluded. This basically means user2 doesn't need to change password (https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups#exclude-users)

"Sign-in from infected device" is marked as Low so the correct answer is Yes No No.

upvoted 8 times

Ed2learn 1 month, 3 weeks ago

directly from the source -" Exclude users

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. "

upvoted 3 times

davenny 2 months, 1 week ago

Answer should be YES,NO,YES

upvoted 3 times

Cyberbug2021 2 months, 2 weeks ago

Y, N, Y

2 - N - in Group 2 - excluded

3 - Y - not suspicious but confirmed infected - medium risk, policy applies

upvoted 1 times

Fred64 2 months, 2 weeks ago

MS doesn't document how risk level is computed. This should be an old question

upvoted 3 times

t2khan 2 months, 2 weeks ago

Agreed with Geeky. Answer should be YES,NO,NO

upvoted 2 times

Kumar1983 2 months, 2 weeks ago

https://t.me/learningnets

Yes, No and No
Consider 3rd as a low risk

upvoted 1 times

CASGTI 2 months, 3 weeks ago

Correct is: YES, NO, NO
1st: YES of course...
2nd: "NO" :exclude overrides include (verified in lab)
3rd: "NO" :infected machine is LOW risk (verified in lab)

upvoted 5 times

rgullini 2 months, 3 weeks ago

Agree with you and your explanations

upvoted 1 times

macco455 3 months, 2 weeks ago

Agree with Geeky:
Yes
No
No
See link in his post where is specifically tells us that exclude take precedence over includes

upvoted 1 times

Jade 3 months, 3 weeks ago

No, Yes, No
Unfamiliar location and Sign-ins from infected devices are risk level low.

upvoted 1 times

milad123 3 months, 3 weeks ago

Unfamiliar location has risk level medium

upvoted 2 times

https://t.me/learningnets

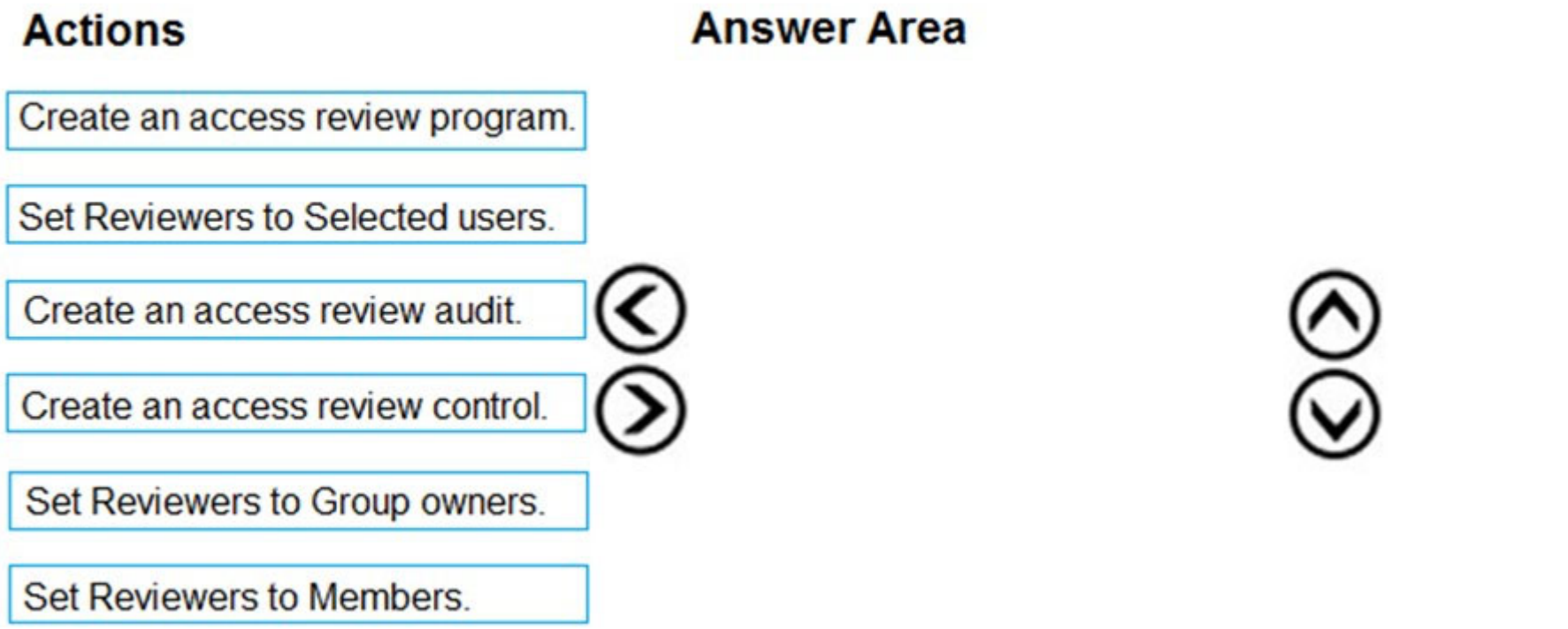
Question #8 Topic 1

DRAG DROP -

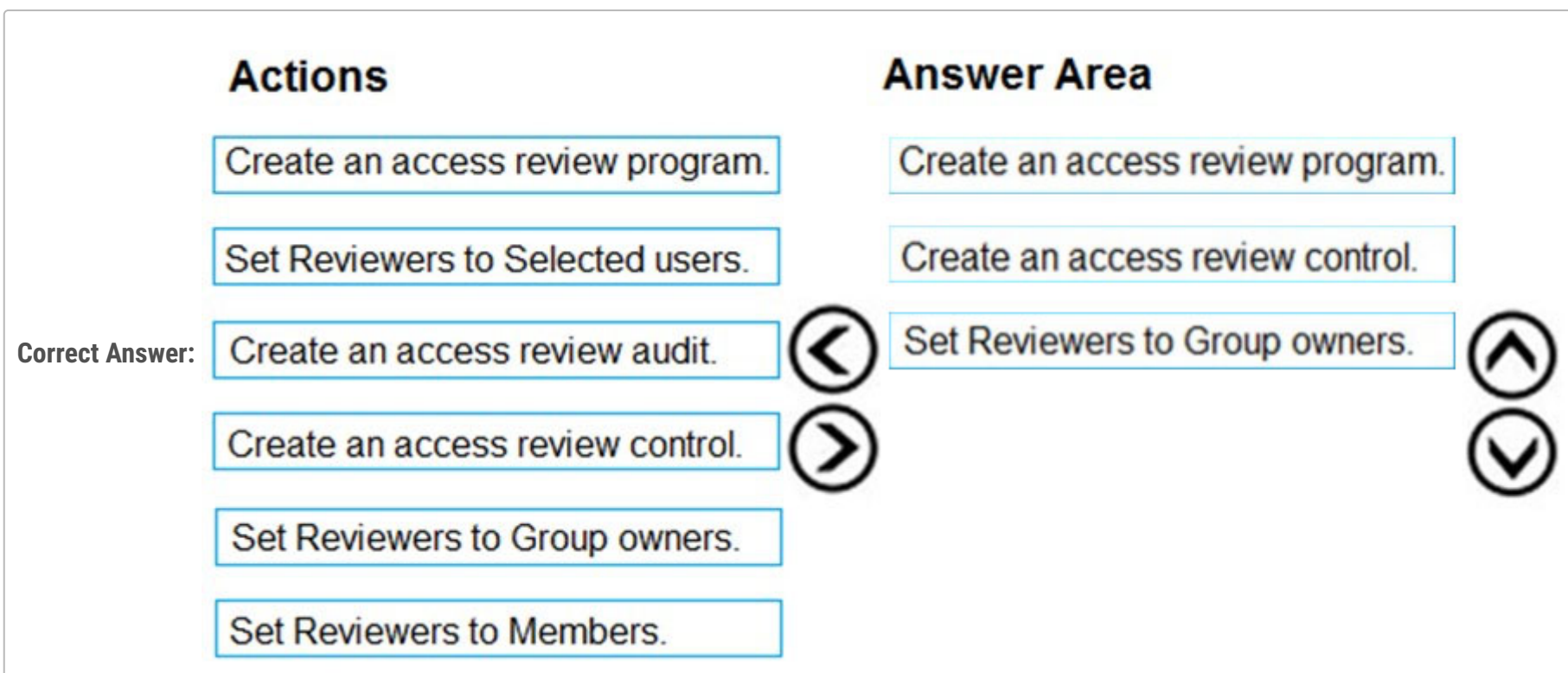
You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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:



Correct Answer:

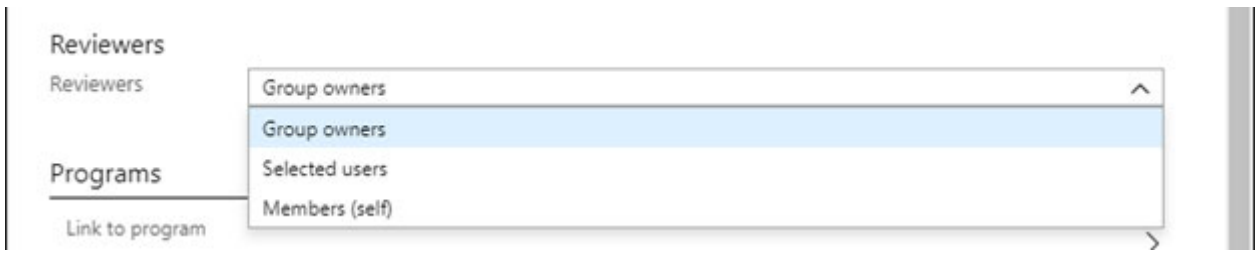


Step 1: Create an access review program

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.



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 1 year, 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 22 times

BobIsSearchingForTheMoon 1 year, 4 months ago

https://t.me/learningnets

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 2 times

justinp Most Recent 5 days, 9 hours ago

this question is present in test today

upvoted 1 times

FK2974 4 months, 1 week ago

correct ! Program/Control/Owner

upvoted 2 times

milind8451 5 months ago

Right ans.

upvoted 1 times

sureshatt 5 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 2 times

sureshatt 3 months, 2 weeks ago

as of today, 2021.03.28, access review programs and access review controls do not exists. Only access reviews exists.

upvoted 4 times

PaulRSE 5 months, 4 weeks ago

Answer is correct,

Create program
Create control
Set reviewers to Group owners

https://developer.microsoft.com/en-us/graph/blogs/retrieving-azure-ad-access-reviews/#:~:text=program%3A%20represents%20an%20Azure%20AD%20access%20review%20program.,AD%20access%20reviews%20has%20one%20program%2C%20%60Default%20program%60.

upvoted 1 times

sayak17 6 months ago

the second url in explanation is redirecting to the first one itself. here's another link https://www.rebeladmin.com/2019/03/step-step-guide-azure-ad-access-reviews-applications/

upvoted 1 times

sayak17 6 months ago

Is access review control still a thing or is it obsolete now?

upvoted 1 times

B1T3X 6 months, 1 week ago

Very poorly worded question. It doesn't say anywhere that there is any group, and even if there was, who said the owners of this group own any resources?

upvoted 3 times

AzureGurl 6 months, 1 week ago

Answer is correct , Create, Control, Assign

upvoted 1 times

aceking 6 months, 2 weeks ago

Given answer is correct. you can assign reviewers to Selected users , Members (self), group. It's in the MS AZ500 latest lab, Lab5 PIM, which can be found: https://www.youtube.com/watch?v=Ck9vqZbVLmU&list=PLOk7s22t7c87SdtLSD0ssPmo1oskEvtux&index=5

upvoted 1 times

Pinto 6 months, 3 weeks ago

As per https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/toc.json

Selected users - Use this option when you don't know who needs access. With this option, you can assign the review to a resource owner or group manager to complete.
Members (self) - Use this option to have the users review their own role assignments.
(Preview) Manager – Use this option to have the user's manager review their role assignment. Upon selecting (Preview) Manager, you will also have the option to specify a fallback reviewer. Fallback reviewers are asked to review a user when the user has no manager specified in the directory.

So it should be Selected Users. There is nothing in the selection called Group or Resource owners.

upvoted 1 times

https://t.me/learningnets

kiketxu 7 months, 3 weeks ago

correct answers

upvoted 1 times

jaredl 1 year ago

Are Group Owners equal to Resource Owners? No. I think the reviews should be the selected Resource Owners, who might no be the Group Owners.

upvoted 2 times

gfhbox0083 1 year ago

Given answer is correct.

upvoted 4 times

lnn_az 1 year, 1 month ago

Identity Governance is not included in the Microsoft Azure Security Technologies –
Skills Measured.

Configure Azure AD Privileged Identity Management
 monitor privileged access
 configure Access Reviews
 activate Privileged Identity Management

upvoted 1 times

gcpora 1 year, 2 months ago

Given answer is correct as the first step will be to create a review program, then create access review control and last set reviewers to group owners.

upvoted 2 times

AS007 1 year, 2 months ago

Correct Answers

upvoted 2 times

https://t.me/learningnets

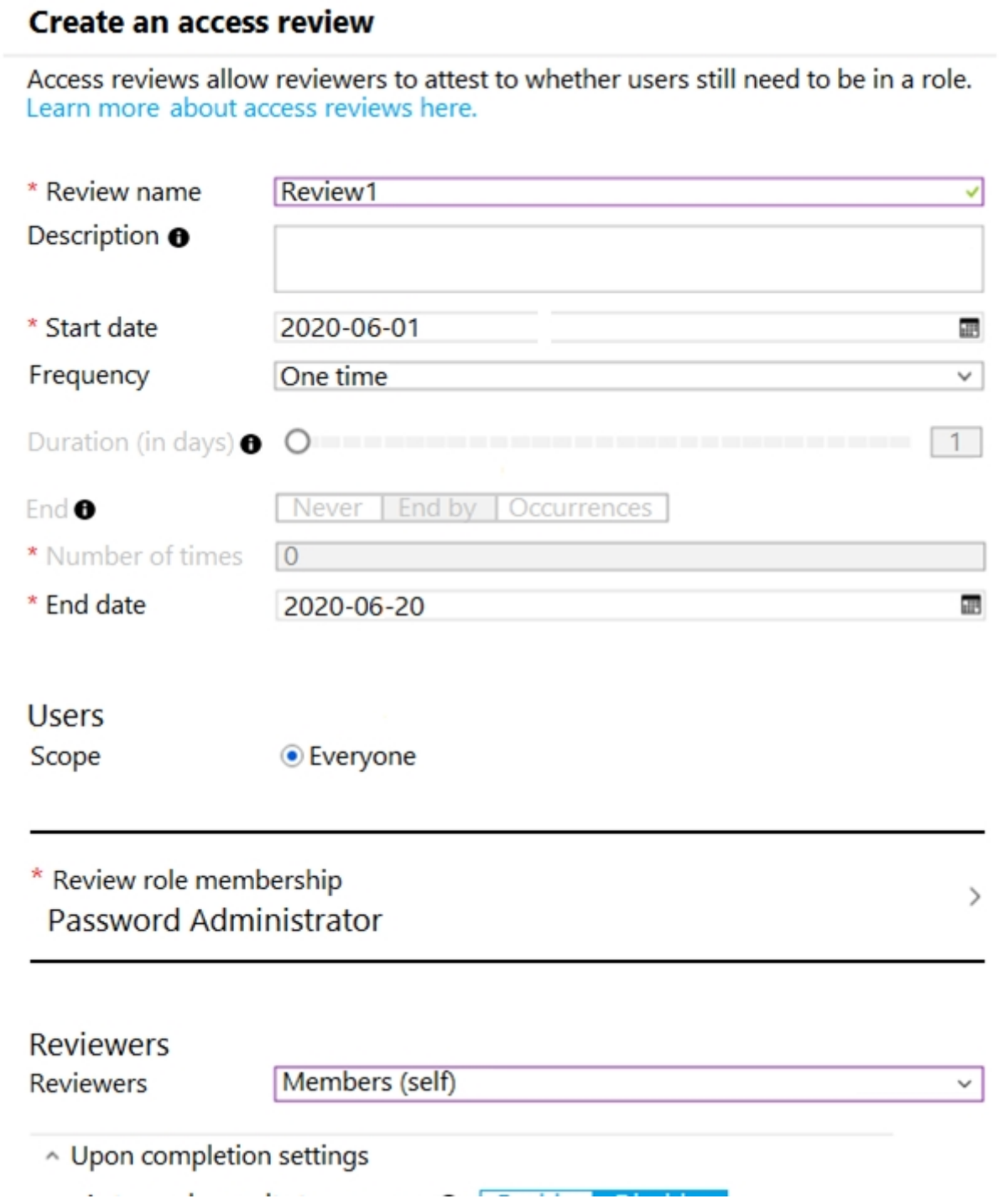
Question #9 Topic 1

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

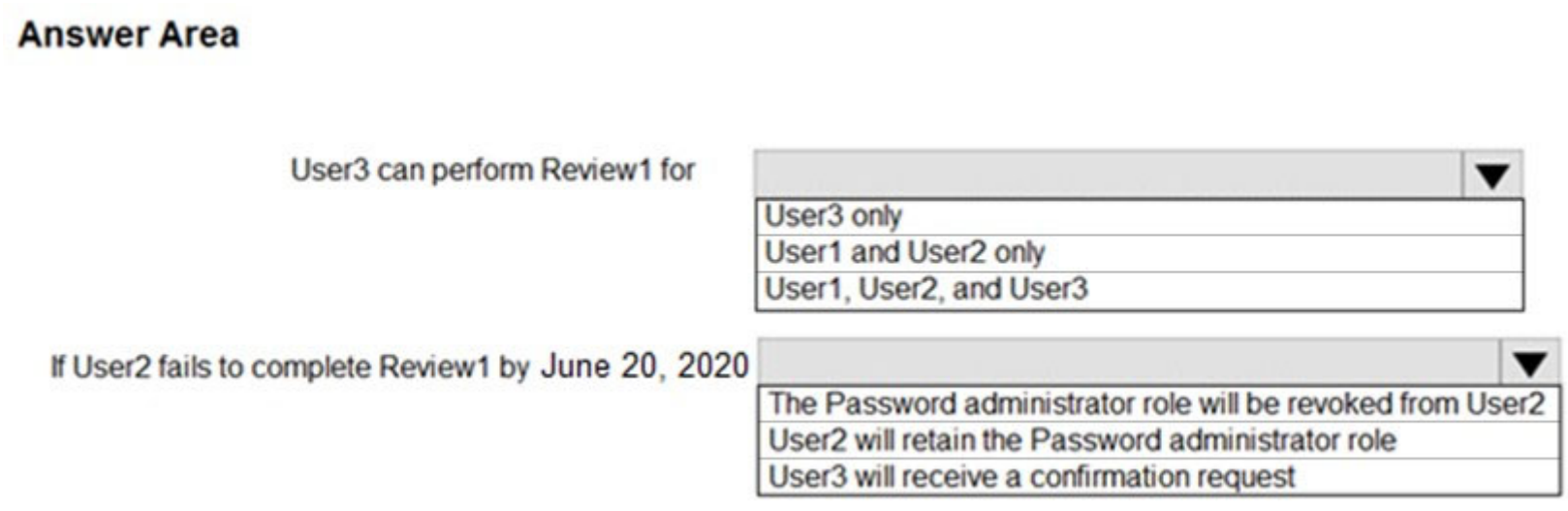
You configure an access review named Review1 as shown in the following exhibit.



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.

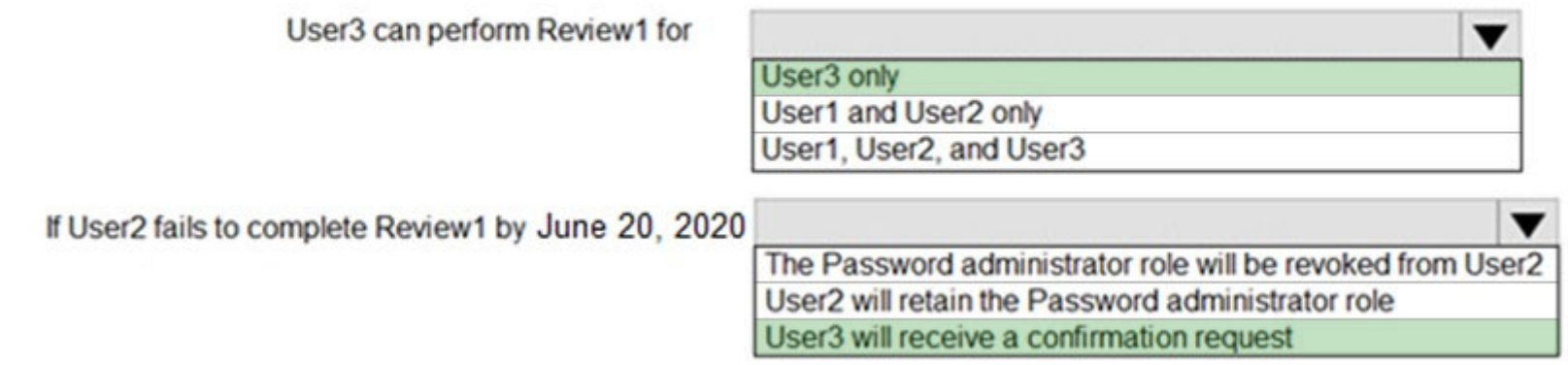
Hot Area:



https://t.me/learningnets

Correct Answer:

Answer Area User2 Will retain the password administrator role



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

Fred64 Highly Voted 4 months ago

how can we answer box 2. We don't see the bottom of the image?

upvoted 10 times

rgullini 2 months, 4 weeks ago

This question is useful only for orientation as seems not complete. Is not possible to provide an answer as there is information missing.

upvoted 2 times

justinp Most Recent 5 days, 9 hours ago

this question is present in test today

upvoted 1 times

miltonskt 1 week ago

The way the question is currently posed, would you have gotten box 2 right? If so, what is the hint?

upvoted 1 times

Vbr93 2 months ago

User2 will retain the password is answer...I have gone through the same question on official Practice test

upvoted 4 times

teehex 2 months ago

Lol this is a super tricky question. Even the screenshot is not actually a complete one you can still see Disable option to be selected. When Disable is selected there is no automatic process so the first option is incorrect.

Since the question is asking about user2 so it must be anything related to user2. So the correct answer is User2 will retain Password Administrator (if No change is selected). It doesn't matter to be honest because this question is asking about User2 lol. Option 3 is irrelevant because it is for user3.

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

there is more information there which would suggest box 2 answer C otherwise I would have to go with answer B, User 2 retains said password even if review is not complete

upvoted 1 times

Firedragon 2 months, 3 weeks ago

Auto apply results to resource is set to Disable and If reviewers don't respond is set to Take recommendation. So, Box 2 should be User2 will retain the Password administrator Role.

upvoted 3 times

rgullini 2 months, 4 weeks ago

This question is useful only for orientation as seems not complete. Is not possible to provide an answer as there is information missing.

upvoted 1 times

https://t.me/learningnets

cyber79 3 months, 1 week ago

Why User 3 cannot perform review for User 1 and User 2 ?

upvoted 2 times

Char1es 2 months, 2 weeks ago

cause they set reviewer as Members (Self)

upvoted 4 times

Cyberbug2021 2 months, 2 weeks ago

because it says "SELF" review only

upvoted 1 times

RameshSesetti 4 months ago

Box Option:2 -- is wrong answer. User2 can retain the password.

upvoted 3 times

longtech 1 month, 2 weeks ago

The answer is right. Because the reviewer is set for user with role Password Administrator, so when user 2 log in fail, the notification will be sent to for the user3 who has confirm for that.

upvoted 1 times

Pinto 4 months ago

Will the user 3 not get an email asking to either approve or deny the recommendations, whatever they are? If recommendation is to deny, then user2 will only retain password till the time user3 does not approve the recommendation or that is not the case?

upvoted 1 times

https://t.me/learningnets

Question #10 *Topic 1*

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

Correct 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

gfhbox0083 Highly Voted 1 year ago
C, for sure.
contoso.com and fabrikam.com only
upvoted 15 times

kumax Most Recent 3 weeks, 4 days ago
On exam May, 2021.
upvoted 2 times

peacegrace 2 months, 1 week ago
in exam in April 2021
upvoted 3 times

Squaiyumi 3 months, 1 week ago
In exam today
upvoted 4 times

sensa 4 months, 2 weeks ago
in exam.. 4
upvoted 3 times

milind8451 4 months, 4 weeks 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 2 times

mayenite 5 months ago
In exam
upvoted 2 times

ealcober 8 months, 1 week ago
Just remark that contoso is the actual owner, so no sense of transfer, and the transfer to another tenant is permitted with named conditions...!
upvoted 1 times

Startkabels 3 months, 1 week ago
its about transferring ownership to the user Admin1...
upvoted 2 times

LTTAM 11 months, 3 weeks ago

https://t.me/learningnets

Answer C is correct. Here is the link:

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer#transfer-a-subscription-to-another-azure-ad-tenant-account

upvoted 4 times

sf2020 1 year, 1 month ago

Answer is correct.
Because the account within Azure AD is Fabrikam it can only be transfered as per Microsoft Documentation.
Be aware of this important information when transferring accounts:

You can make these transfers:

From a work or school account to another work or school account.

From a Microsoft account to a work or school account.

From a Microsoft account to another Microsoft account.

The target account must be a valid Azure Commerce account to be a valid target for transfers. For new accounts, you are asked to create an Azure Commerce account when signing in to the Azure Enterprise portal. For existing accounts, you must first create a new Azure subscription before the account is eligible.

You can't make a transfer from a work or school account to a Microsoft account.

When you complete a subscription transfer, Microsoft updates the account owner.

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/ea-portal-get-started#change-account-owner

upvoted 2 times

lnn_az 1 year, 1 month ago

Hi sf2020,
the reference which you provided is for Azure Enterprise Portal. As per question, we need use Azure Account Center to transfer.

upvoted 1 times

mpknz 1 year, 3 months ago

anyone have a reference which supports the answer that you cant transfer the subscription to a hotmail or openid account?

upvoted 1 times

Remco 1 year, 2 months ago

You cannot pass a subscription to a Hotmail or OpenID account because they are not tenants. A subscription is owned by a tenant. That's the reason.

upvoted 14 times

IsildursHeir 1 year, 2 months ago

I have actually seen hotmail or outlook accounts being the admins of subscriptions. I guess the point here is that they are not in an AAD. They first need to be in that AAD with that hotmail or outlook and then they can be subscription admins. That wasn't the case here so thus we cannot make them admins. It requires a bit of wild imagination but seems most these questions do? I have no idea what an "OpenID account" is, or whether they are supported.

upvoted 3 times

Startkabels 3 months, 3 weeks ago

The point is ownership, not admin permissions

upvoted 1 times

https://t.me/learningnets

Question #11 Topic 1

HOTSPOT -

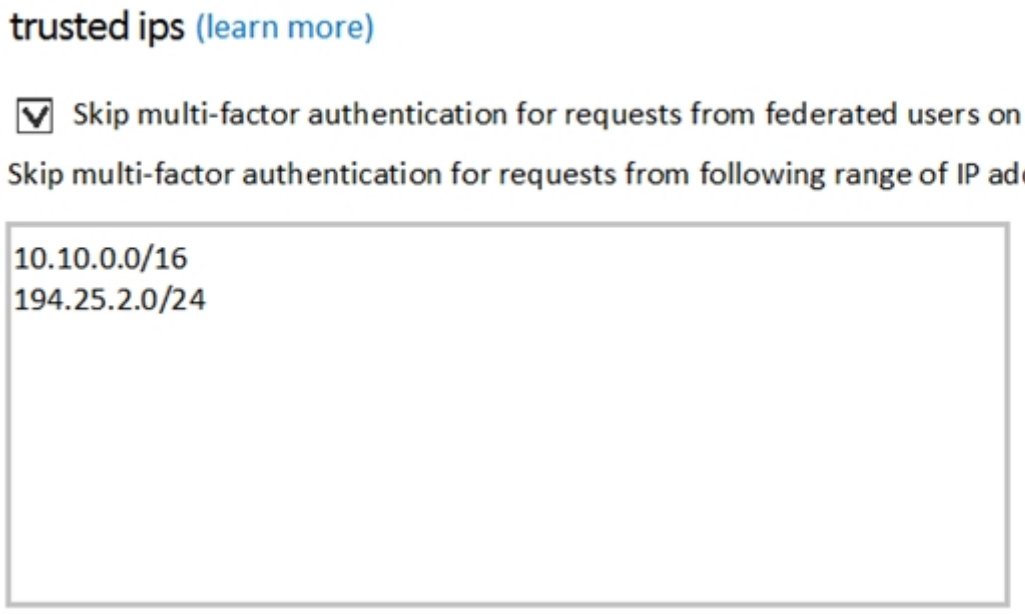
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

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.)



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	○	○

https://t.me/learningnets

Correct 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/

e3rh Highly Voted 1 year, 3 months ago

Yes
No
No

right ones

upvoted 40 times

Aston1818 1 year, 1 month ago

I think its no for the last question as the ip given in the exception is the public NAT one!

upvoted 3 times

gboyega Highly Voted 1 year 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 17 times

justinp Most Recent 5 days, 9 hours ago

this question is present in test today

upvoted 1 times

Goseu 1 month, 1 week ago

No,No,No
Box1: mfa registration process not completed.

upvoted 3 times

3abmula 1 month, 2 weeks ago

I'd go for N, N, N
No: User1 MFA "Enabled", he still didn't enroll, during enrollment he could choose text.
No: Auth App is not one of available methods
No: MFA will be bypassed (New office IP range is excluded).

upvoted 5 times

Ed2learn 1 month, 3 weeks ago

User 1 must authenticate with MFA as enable. But why only the phone? Why not text? The wording of the question seems to be MUST by phone. Is this just odd wording?

upvoted 3 times

https://t.me/learningnets

ryta 1 month, 2 weeks ago

My initial thoughts exactly.. why use the word MUST. There are 2 options.

upvoted 1 times

bimbokeem 2 months, 1 week ago

very correct

upvoted 1 times

Firedragon 2 months, 3 weeks ago

Yes
No
No - New York office's Public ip range is in the trusted ip list. According to the following Microsoft doc, MFA will be bypassed since this is a cloud-based MFA.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#:~:text=To%20enable%20trusted%20IPs%20using%20Conditional%20Access%20policies%2C,choose%20this%20option%2C%20select%20...%204%20Select%20Save.
Note
The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can only use public IP address ranges.

upvoted 1 times

Salacity 4 months, 3 weeks ago

1. Yes - The IP range is not included in the exception
2. No - Authenticator App is not an approved method
3. No - Assuming it means User2, the New York office would be included with the federated users exception. The private IP address range in the IP exclusions for the Seattle office is included to throw you off on this question. User2 is considered a federated user inside the intranet since they are in the office. Same would apply if the Seattle IP address range was not added to the IP range exclusion.

upvoted 3 times

Startkabels 3 months, 3 weeks ago

I would go for this too.
MFA enabled means users are not forced to register authentication methods if they havent done so already. It does not mean this MFA authentication will be applied.
MFA enforced means that all users are forced to register a MFA authentication method if they havent done so already, whether or not MFA is applied when they login.
Only the third question is somewhat confusing. Our company has offices that have a tunnel connection to Azure. We have the internal IP's in our trusted IP list, not the external IP's. I guess in this example the office connects to Azure over the internet?

upvoted 1 times

milind8451 5 months ago

Agree with ans given.
YES
NO
NO

upvoted 2 times

sukhdeep 5 months, 3 weeks ago

user 1 MFA status is enabled not enforced so how user1 can use MFA ?

upvoted 2 times

Arejay 5 months ago

Enabled

The user has been enrolled in multi-factor authentication, but has not completed the registration process. They will be prompted to complete the process the next time they sign in.

Enforced

The user may or may not have completed registration. If they have completed the registration process then they are using multi-factor authentication. Otherwise, the user will be prompted to completer the process at next sign-in

upvoted 2 times

zic04 5 months, 3 weeks ago

Yes / No / No agree

upvoted 3 times

kiketxu 7 months, 3 weeks ago

1. YES, that IP is not excluded.
2. NO, MS App is not allowed (the options are missing in the screenshot)
3. NO, as the IP is excluded. (considering a typo when says User1, it should refer to User2)

upvoted 5 times

PaulRSE 5 months, 4 weeks ago

Yes, no, no.

upvoted 2 times

realname007 8 months ago

https://t.me/learningnets

anyone knows the correct answer for
https://freedumps.certqueen.com/tag/az-500-exam-free-dumps-questions/
question 14
???

upvoted 1 times

Seagun 8 months, 2 weeks ago

3rd scenario does not make sense is it referring to user 1 or user 2? don't know how you can provide an answer without knowing which user, first 2 I agree with the answer provided

upvoted 1 times

Thi 5 months, 2 weeks ago

I agree

upvoted 1 times

server1 10 months, 1 week ago

YES NO NO given answer is correct

upvoted 6 times

Sanju101 10 months, 3 weeks ago

Trusted IP bypass works only from inside of the company intranet. If you select the All Federated Users option and a user signs in from outside the company intranet, the user has to authenticate by using two-step verification.

upvoted 3 times

awssecuritynewbie 9 months, 2 weeks ago

exactly so since if you pay attention the IP for newyork office is wrong man! so it will include the MFA ... so Yes NO YES

upvoted 2 times

https://t.me/learningnets

Question #12 *Topic 1*

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

Correct 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

Prash85 Highly Voted 1 year, 2 months ago
Azure Blueprint is the correct answer
upvoted 8 times

Atanu Highly Voted 1 year, 6 months ago
Conflict with Question 13. Same question .. but two different answers...Which one to go with?
upvoted 5 times

DA0410 7 months, 3 weeks ago
Good observation. If I am not wrong , Q13 answer should be blueprint.
upvoted 1 times

P4YDAY 1 year, 6 months ago
Azure Blueprint is the correct answer for both question.
upvoted 28 times

justinp Most Recent 5 days, 9 hours ago
this question is present in test today
upvoted 1 times

Deepmindx 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 1 times

teehex 2 months 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 2 times

bimbokeem 2 months, 1 week ago
question 12 is not conflicting with question 13 please. not in anyway that i know
upvoted 1 times

teamaws 3 months, 1 week ago
for sure, D
upvoted 2 times

seconazure 4 months, 3 weeks ago
Absolutely D.
Azure Blueprint
upvoted 3 times

https://t.me/learningnets

milind8451 4 months, 4 weeks ago
Blueprint is right ans.
upvoted 1 times

zic04 6 months ago
Blueprint good
upvoted 1 times

ajir 11 months ago
Azure Blueprint
upvoted 2 times

planb7000 11 months, 2 weeks ago
Blueprint
upvoted 1 times

gboyega 1 year ago
Azure Blueprint is correct
upvoted 2 times

gfhbox0083 1 year ago
D, for sure.
Azure Blueprint
upvoted 4 times

kingnag1 1 year ago
blue print
upvoted 1 times

lnn_az 1 year, 1 month ago
Azure Blueprint
upvoted 2 times

https://t.me/learningnets

Question #13 Topic 1

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

Answer Area

Correct Answer:

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.

https://t.me/learningnets

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

Giritharrram 3 days, 17 hours ago

Arcpush and contributor can Upload and download
Arcpull can only download
Arcimagesigner can only sign the images

upvoted 1 times

https://t.me/learningnets

Question #14 *Topic 1*

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.

Correct 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

FelipeBarbosa Highly Voted 4 months ago
In the exam, correct answer.
upvoted 7 times

kumax Most Recent 3 weeks, 4 days ago
On exam May 2021.
upvoted 2 times

BalderkVeit 1 month, 3 weeks ago
I think B and F are correct
upvoted 2 times

Sjn9 3 months ago
B and F are correct.
upvoted 1 times

Geeky93 4 months ago
Correct answer.
upvoted 2 times

Sethoo 4 months ago
Agree to given answer. B and F
upvoted 3 times

https://t.me/learningnets

Question #15 *Topic 1*

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

Correct 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

kristiann21 Highly Voted 1 year, 1 month ago
Correct Answer.
upvoted 13 times

gfhbox0083 Highly Voted 1 year ago
B, for sure
upvoted 6 times

kiketxu 9 months, 3 weeks ago
Agree with you. it must be a NO, because any lock doesn't revoke the access.
upvoted 2 times

sensa Most Recent 4 months, 2 weeks ago
in exam.. 3
upvoted 1 times

zic04 6 months ago
Correct Answer
upvoted 1 times

B1T3X 6 months, 1 week ago
Correct, answer is no since even the most restrictive lock (read only) doesn't prevent access to the storage account data.
upvoted 2 times

AzureGurl 6 months, 2 weeks ago
Correct answer. Lock will not work on authentication.
upvoted 1 times

kdkdk 7 months ago
In the exams I choose no
upvoted 3 times

Sam_samules 7 months, 2 weeks ago
Lock would ensure no deletion, but resources can still access it.
IMO B is the correct answere.
https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations
upvoted 2 times

ShefAZ 8 months, 3 weeks ago
How to delete SAS, means I can generate it again changing variables but I am not able to delete it.
upvoted 1 times

https://t.me/learningnets

musiman 7 months, 3 weeks ago

Not the SAS, but the Stored Access Policy should be deleted. You can create a SAS based on a Stored Access Policy. When you delete the Stored Access Policy, all the SAS uri's that were created based on this Stored Access Policy, will stop working.

upvoted 1 times

VinciTheTechnic1an 9 months, 2 weeks ago

NO, user must use a policy.

upvoted 2 times

Attaxhan 11 months, 3 weeks ago

IN THE EXAM

upvoted 3 times

maj79 1 year ago

agree to the answer

upvoted 3 times

https://t.me/learningnets

Question #16 *Topic 1*

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

Correct 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

Adamasbue Highly Voted 1 year, 7 months ago
Wrong: https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture
upvoted 23 times

PlasticMind 1 year, 6 months 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 9 times

ochiwi 1 year, 3 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

Hemn1990 Highly Voted 1 year 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 14 times

teehex Most Recent 2 months ago
The question already stated that hybrid configuration/deployment is in place so you won't probably need ADDS. The thing you need is the communication which vNet configuration is required.
upvoted 2 times

MQH 2 months, 2 weeks ago
the guys who said YES! how is it possible to connect the AADDS with ADDS ? the problem we need to solve is the connectivity from azure vnet to the on-premise network, if the question state that there is already a connection then the AADDS will fix this.
- implement the connection between AZ and local net
- install AADDS on azure and integrate it with out on-prem ADDS
upvoted 3 times

cannibalcorpse 3 months, 1 week ago
I would say YES
https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture#integrate-hdinsight-with-active-directory
""
o summarize, you need to set up an environment with:

An Active Directory domain (managed by Azure AD DS). The domain name must be 39 characters or less to work with Azure HDInsight."
upvoted 1 times

_adem 3 months, 2 weeks ago
Answer is A
https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/hdinsight-security-overview#authentication

https://t.me/learningnets

"Authentication
Enterprise Security Package from HDInsight provides Active Directory-based authentication, multi-user support, and role-based access control. The Active Directory integration is achieved through the use of Azure Active Directory Domain Services. With these capabilities, you can create an HDInsight cluster joined to an Active Directory domain. Then configure a list of employees from the enterprise who can authenticate to the cluster.

With this setup, enterprise employees can sign in to the cluster nodes by using their domain credentials. They can also use their domain credentials to authenticate with other approved endpoints. Like Apache Ambari Views, ODBC, JDBC, PowerShell, and REST APIs to interact with the cluster."

upvoted 2 times

macross 3 months, 2 weeks ago

Creating an AD domain will not solve the problem - there's more to that. I agree with the answer here. So No.

upvoted 1 times

deegadaze1 4 months, 2 weeks ago

A correct Answer:
ESP is generally available in HDInsight 3.6 and 4.0 for these cluster types: Apache Spark, Interactive, Hadoop, and HBase.
Enabling Azure AD DS is a prerequisite before you can create an HDInsight cluster with ESP-When Azure AD DS is enabled, all users and objects start synchronizing from Azure Active Directory (Azure AD) to Azure AD DS by default.

upvoted 1 times

sureshatt 4 months, 4 weeks ago

I think the question is little outdated. However, still the answer is B (NO), but for different reason than explained in this given answer.
Deployment of AD DS into the HDInsights cluster allows to authenticate users against Azure AD without having to do any additional network configurations. However, the catch here is that "Password Hashes" needs to be synced from On-Prem to Azure AD.
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-password-hash-sync

Though the question says there is a Hybrid Identity, it doesn't say there is a password hash sync, therefore simple deployment of AD DS won't solve the problem. It needs an additional setting to enable password sync.

Therefore I go with the answer "NO" but due to the missing password hash sync.

upvoted 2 times

milind8451 5 months ago

As per MS Docs "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." So given answer is wrong. A is right ans.

upvoted 1 times

B1T3X 6 months, 1 week ago

Question doesn't indicate a site-to-site VPN is in place hence the answer is no in my opinion.

upvoted 1 times

sayak17 6 months, 2 weeks ago

This question has occurred before. The explanation given there was same as here and people agreed with that. Not sure what should be the answer here though as the solution given in the 'question' is different from earlier

upvoted 1 times

kktpkktp 6 months, 2 weeks ago

the answer should be A. HDInsight clusters can be integrated with Azure Active Directory Domain Services if deployed using Enterprise Security Package. Azure AD Connect will synchronize all the credentials from on-prem to Azure AD which in turn will sync to Azure AD DS. So, authentication in the HDInsight cluster will happen via on-prem credentials.

upvoted 1 times

Srikanth_M 6 months, 3 weeks ago

I will go with answer A.
https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-create-configure-enterprise-security-cluster#sync-on-premises-users-to-azure-ad

upvoted 1 times

Lppl007 6 months, 3 weeks ago

https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/hdinsight-security-overview

Authentication
Enterprise Security Package from HDInsight provides Active Directory-based authentication, multi-user support, and role-based access control. The Active Directory integration is achieved through the use of Azure Active Directory Domain Services. With these capabilities, you can create an HDInsight cluster joined to an Active Directory domain. Then configure a list of employees from the enterprise who can authenticate to the cluster.

With this setup, enterprise employees can sign in to the cluster nodes by using their domain credentials. They can also use their domain credentials to authenticate with other approved endpoints. Like Apache Ambari Views, ODBC, JDBC, PowerShell, and REST APIs to interact with the cluster.

upvoted 1 times

amanp 7 months, 1 week ago

Answer is correct
For those saying the answer is wrong, the question says 'You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.'

https://t.me/learningnets

Why will you create a new Azure AD DS for this if you want to use on-premises DC. The correct is to set up a VPN gateway so that the authentication is done through a site-to-site VPN connectivity. Azure AD DS can be used as well but in this case it wont

upvoted 6 times

Sethoo 7 months, 1 week ago

Correct answer should be A. You already have the OnPrem and Azure connected so no need to set up the connection. The question want to find out if Azure AD DS is one of the means to access HDinsight from on Prem, and the answer is a YES

upvoted 1 times

Sethoo 5 months ago

Actually, the answer is no. There are more steps than just having the established the ADDS from Microsoft documentation

upvoted 1 times

https://t.me/learningnets

Question #17 *Topic 1*

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

Correct Answer: *CE*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

Solanki Highly Voted 1 year, 2 months 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 22 times

gfhbox0083 Highly Voted 1 year ago
C, E, for sure.
Role ==> Global administrator
Group ==> Enterprise Admins
upvoted 12 times

M21RUN Most Recent 1 month, 1 week ago
Correct
upvoted 1 times

peacegrace 2 months, 1 week ago
in exam in April 2021
upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago
In Express settings, the installation wizard asks for the following:
AD DS Enterprise Administrator credentials
Azure AD Global Administrator credentials
upvoted 1 times

Sjn9 3 months ago
Enterprise and Global admins for sure
upvoted 1 times

swati17 3 months ago
C&E are correct
upvoted 1 times

sureshatt 4 months, 4 weeks ago
Answer is correct: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express
upvoted 2 times

milind8451 5 months ago
Right ans
upvoted 1 times

zic04 6 months ago
C & E correct Answer
upvoted 1 times

https://t.me/learningnets

AzureGurl 6 months, 1 week ago
C,E are the correct options.
upvoted 1 times

AzureGurl 6 months, 2 weeks ago
Correct answer.
upvoted 1 times

VinciTheTechnic1an 9 months, 2 weeks ago
C and E is the correct.
upvoted 3 times

bj112 9 months, 2 weeks ago
CE is correct
upvoted 1 times

abosafi87 10 months, 2 weeks ago
Answre is C, E
upvoted 4 times

AZ_Student 11 months ago
The suggested answer is correct C and E.
upvoted 3 times

gfhbox0083 1 year ago
C, E for sure.
The Global administrator role in Azure AD
The Enterprise Admins group in Active Directory
upvoted 3 times

https://t.me/learningnets

Question #18 *Topic 1*

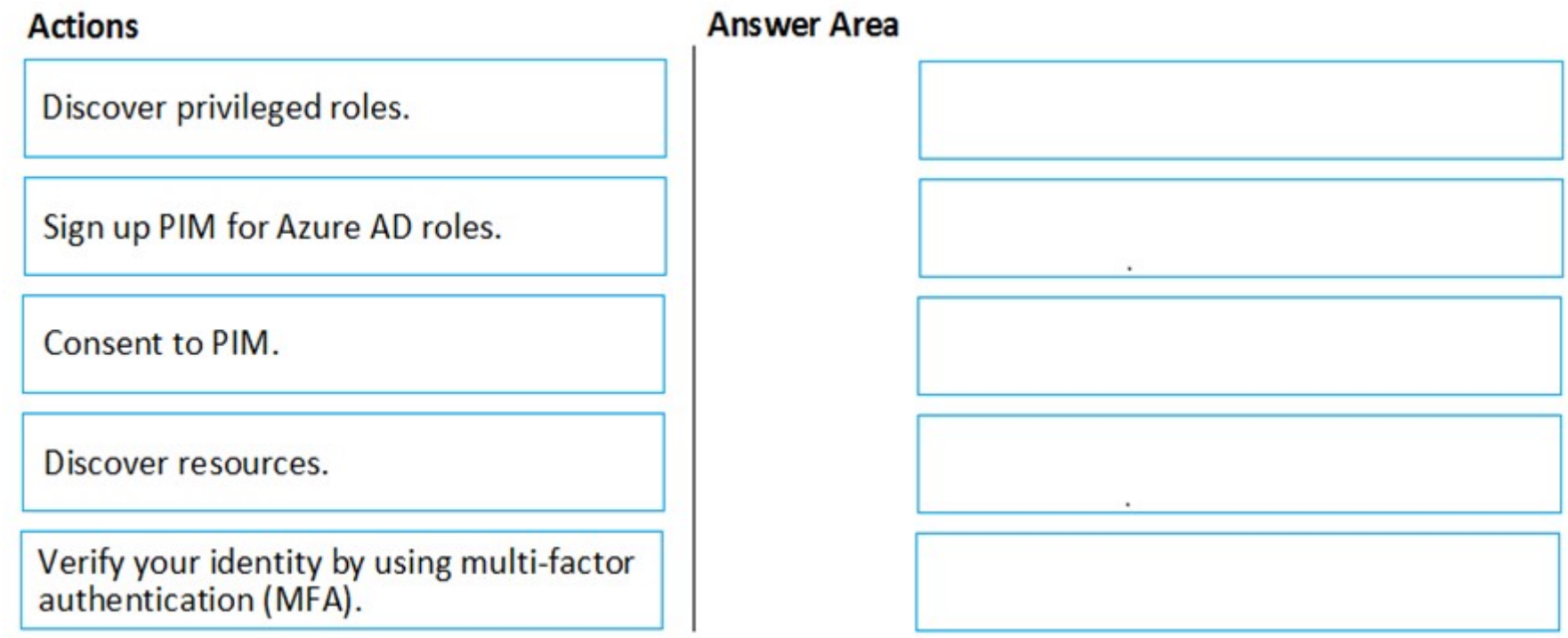
DRAG DROP -

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.

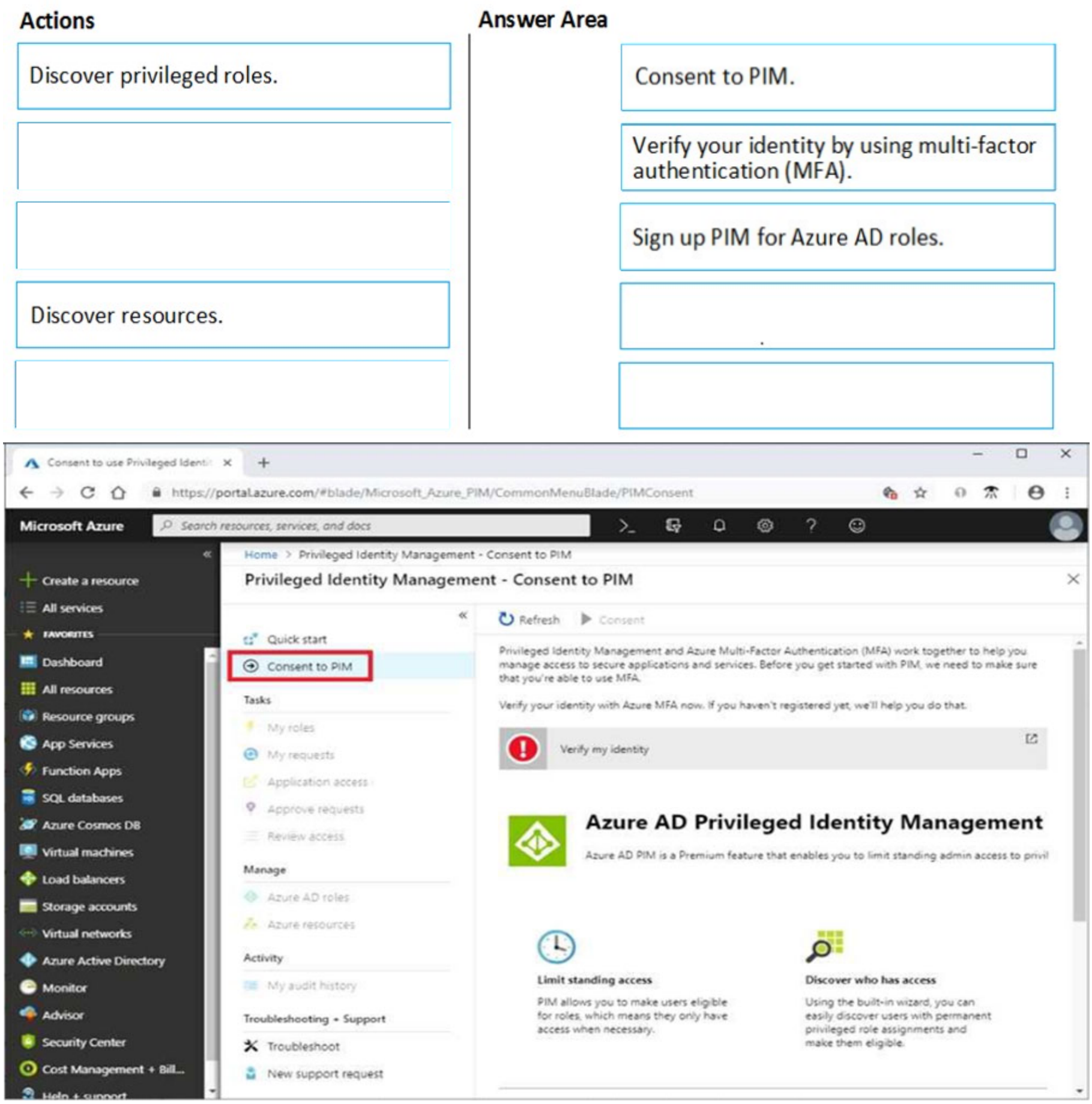
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



https://t.me/learningnets

Correct Answer:



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.

jessicamendez10 Highly Voted 3 months, 3 weeks ago

In exam 20/03/2021

upvoted 10 times

sureshatt 3 months, 2 weeks ago

strange that this is in a recent exam because now PIM is automatically enabled.

upvoted 3 times

aaronkho 2 weeks, 3 days ago

yup PIM is already automatically enabled

upvoted 1 times

justinp Most Recent 5 days, 9 hours ago

In exam, today

upvoted 1 times

Rume 2 weeks ago

Out dated - old question

https://t.me/learningnets

Question #19 Topic 1

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

Correct 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

gfhbox0083 Highly Voted 1 year ago
B, for sure.
upvoted 16 times

ManOnTheMoon Most Recent 1 month, 1 week ago
B, fo shizzle
upvoted 1 times

Sjn9 3 months ago
B is the correct answer
upvoted 1 times

swati17 3 months ago
B is correct
upvoted 1 times

teamaws 3 months, 1 week ago
B for shore
upvoted 1 times

seconazure 4 months, 3 weeks ago
B, ofc
upvoted 1 times

zic04 6 months ago
B agree
upvoted 2 times

prubio 6 months, 1 week ago
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. Nothing related to grant access to local users onto HD Insight

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy
upvoted 2 times

AZ_Student 11 months ago
Absolutely, B.
upvoted 4 times

orekz 12 months ago

https://t.me/learningnets

Definitely, B is the correct answer
upvoted 4 times

Question #20

Topic 1

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

Correct Answer: *A*
Generating new storage account keys will invalidate all SASλ€™s that were based on the previous keys.

Squaiyumi Highly Voted 3 months, 1 week ago
In the exam 6 April
upvoted 6 times

justinp Most Recent 5 days, 9 hours ago
In test, today
upvoted 2 times

teehex 2 months ago
A shared access signature URI is associated with the account key used to create the signature, and the associated stored access policy (if any). If no stored access policy is specified, the only way to revoke a shared access signature is to change the account key.
upvoted 2 times

teamaws 3 months, 1 week ago
Yes, for shore
upvoted 1 times

jessicamendez10 3 months, 3 weeks ago
In exam 20/03/2021
upvoted 4 times

Pinto 4 months ago
A. Yes. A bit confusing though. If only 1 access key is generated then SAS using other Access key will still work.
upvoted 3 times

Kumar1983 2 months, 3 weeks ago
interesting point but they have used the term "keys" in the question.. safe to say that the given answer is correct.
upvoted 1 times

debsauce 4 months ago
Correct answer
upvoted 3 times

https://t.me/learningnets

Question #21 *Topic 1*

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 enabled for the tenant.

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	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 activated the Password Administrator role, the user can approve their own request.	○	○

Correct Answer:

Answer Area	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 activated 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.

https://t.me/learningnets

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

Madball 6 days, 21 hours ago

Q: When User1 signs in, the user is assigned the Password Administrator role automatically?
A: Yes, because they have an active assignment type.

Q: User2 can request to activate the Password Administrator role?
A: Yes, because they have an eligible assignment type.

Q: If User3 wants to activate the Password Administrator role, the user can approve their own request?
A: No, users cannot approve their own elevation requests.

upvoted 2 times

gsidhwani77 1 week, 2 days ago

Yes No Yes - if user 2 is Disabled for MFA and hence he can not get access without making MFA Status enabled.

upvoted 3 times

Aanandan 1 week, 1 day ago

How you saying yes for user 3

upvoted 1 times

https://t.me/learningnets

Question #22 *Topic 1*

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

Correct 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

cannibalcorpse Highly Voted 3 months, 1 week 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 9 times

Deepmindx Most Recent 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 1 times

Deepmindx 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 1 times

kumax 3 weeks, 4 days ago
On exam May 2021.
upvoted 2 times

teehex 2 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 1 times

peacegrace 2 months, 1 week ago
in exam in April 2021
upvoted 3 times

https://t.me/learningnets

Sjn9 3 months ago
D is the right answer.
upvoted 4 times

dadageer 4 months ago
Domain joined device, Users are not created in Database as contained users so the given answer is correct!
upvoted 3 times

Super_Pun 4 months ago
Given answer is correct
Because you are connecting to the database instance from "the domain joined device"
upvoted 3 times

LJack 4 months ago
Answer is correct, you are signing in from domain joined machine.
upvoted 1 times

PSunny 4 months ago
It is correct, see the word SSO
upvoted 1 times

PSunny 4 months ago
Also Domain Joined Machine.
upvoted 1 times

Sethoo 4 months ago
The answer should be A, and not D. Password
upvoted 2 times

raguiar 4 months ago
wrong. The correct answer is A
upvoted 2 times

https://t.me/learningnets

Question #23 *Topic 1*

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?

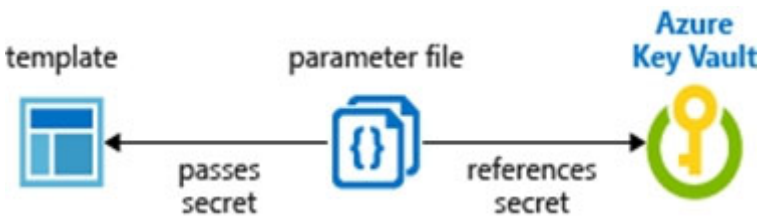
A. a key vault access policy

B. a linked template

C. a parameters file

D. an automation account

Correct Answer: *C* B
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

rharbeg Highly Voted 1 year, 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 58 times

Ed2learn 1 month, 3 weeks ago
The question states you need to dynamically generate the resource ID. From the source - "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."
upvoted 1 times

sureshatt 4 months, 3 weeks ago
100% correct. Answer should be B.
upvoted 3 times

vlq 1 year, 2 months ago
Yep, you are absolutely right!
upvoted 1 times

ExamUser 1 year, 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 2 times

shaheer1991 Highly Voted 1 year, 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 15 times

Amarvel Most Recent 6 days, 1 hour ago
Answer should be B. IN the same URLS states:
You can't dynamically generate the resource ID in the parameters file because template expressions aren't allowed in the parameters file.

https://t.me/learningnets

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#reference-secrets-with-dynamic-id

upvoted 1 times

Duffers 2 weeks ago

It's C, see diagram below.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/media/key-vault-parameter/dynamickeyvault.png

upvoted 1 times

kumax 3 weeks, 4 days ago

On exam May 2021.

upvoted 2 times

kvinaybabu 3 weeks, 6 days ago

Based on below explanation, it sounds that correct answer is B.

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. The following image shows how a parameter in the linked template references the secret.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

upvoted 1 times

parmendier 4 weeks ago

Answer should be B.

upvoted 1 times

teehex 2 months ago

Parameter file HAS NOTHING to do which dynamically constructing a resource ID in Azure ARM template. Parameter file is just one to store the artifact of your deployment.

Linked template is the solution to dynamically construct an past the value as a parameter (not parameter file).

Azure Automation could be an alternative but this is much more complicated while we already have Linked Template.

upvoted 1 times

peacegrace 2 months, 2 weeks ago

The discussions here are super confusing. I will go with Paramter File. my Reasoning is : https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/parameter-files?tabs=json

upvoted 1 times

sureshatt 3 months, 3 weeks ago

B for sure. Nothing to discuss.

upvoted 1 times

macco455 3 months, 2 weeks ago

Based on all the comments there is A LOT to discuss.

upvoted 1 times

milad123 3 months, 3 weeks ago

For me, response is Liked Template (B).
Because, as said in the documentation "You can't dynamically generate the resource ID in the parameters file because template expressions aren't allowed in the parameters file."

upvoted 1 times

Startkabels 3 months, 3 weeks ago

C wouldn't make any sense reading the linked article:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

The article explains 2 things:
Reference secrets with static ID
Reference secrets with dynamic ID
The question is You need to identify a method to dynamically construct a resource ID
This by itself is for me reason enough to choose B.
Also the description of the solution:
"In either case, you can dynamically generate the resource ID for a key vault secret by using a linked template." which is exactly what is asked here.

upvoted 1 times

jessicamendez10 3 months, 3 weeks ago

In exam 20/03/2021

upvoted 4 times

Super_Pun 4 months ago

https://t.me/learningnets

To dynamically construct a resource ID you need to use Linked Template
The correct answer is B

upvoted 1 times

mak791 4 months, 2 weeks ago

Correct answer is B (Linked Template)

upvoted 1 times

Vegazbabz 4 months, 2 weeks ago

Had it on an exam this week

upvoted 2 times

seconazure 4 months, 3 weeks ago

As stated, You need to identify a method to dynamically.
The answer shoudl be B. Becaue, You can't dynamically generate the resource ID in the parameters file because template expressions aren't allowed in the parameters file.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#reference-secrets-with-dynamic-id

upvoted 2 times

https://t.me/learningnets

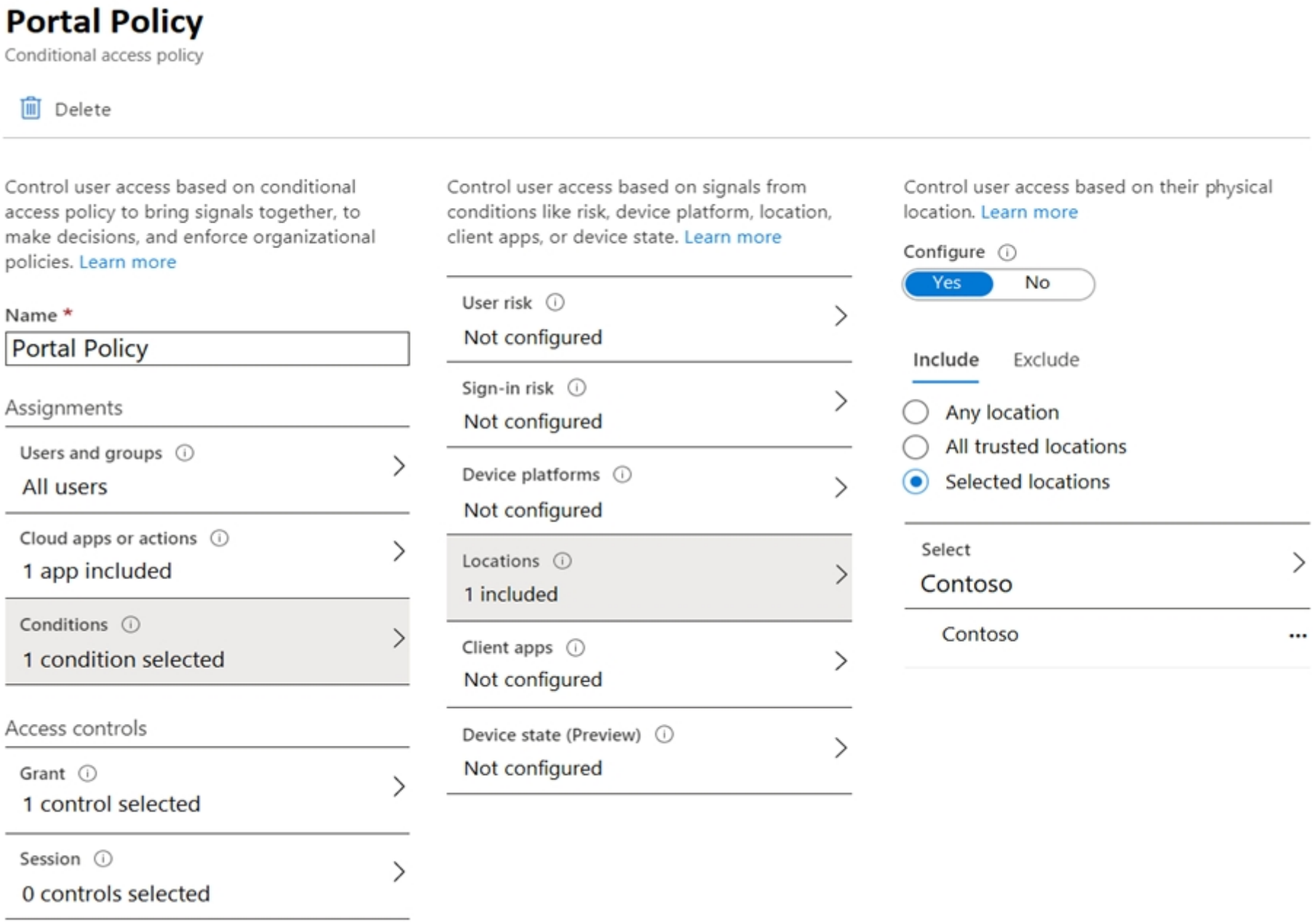
Question #24 *Topic 1*

HOTSPOT -

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

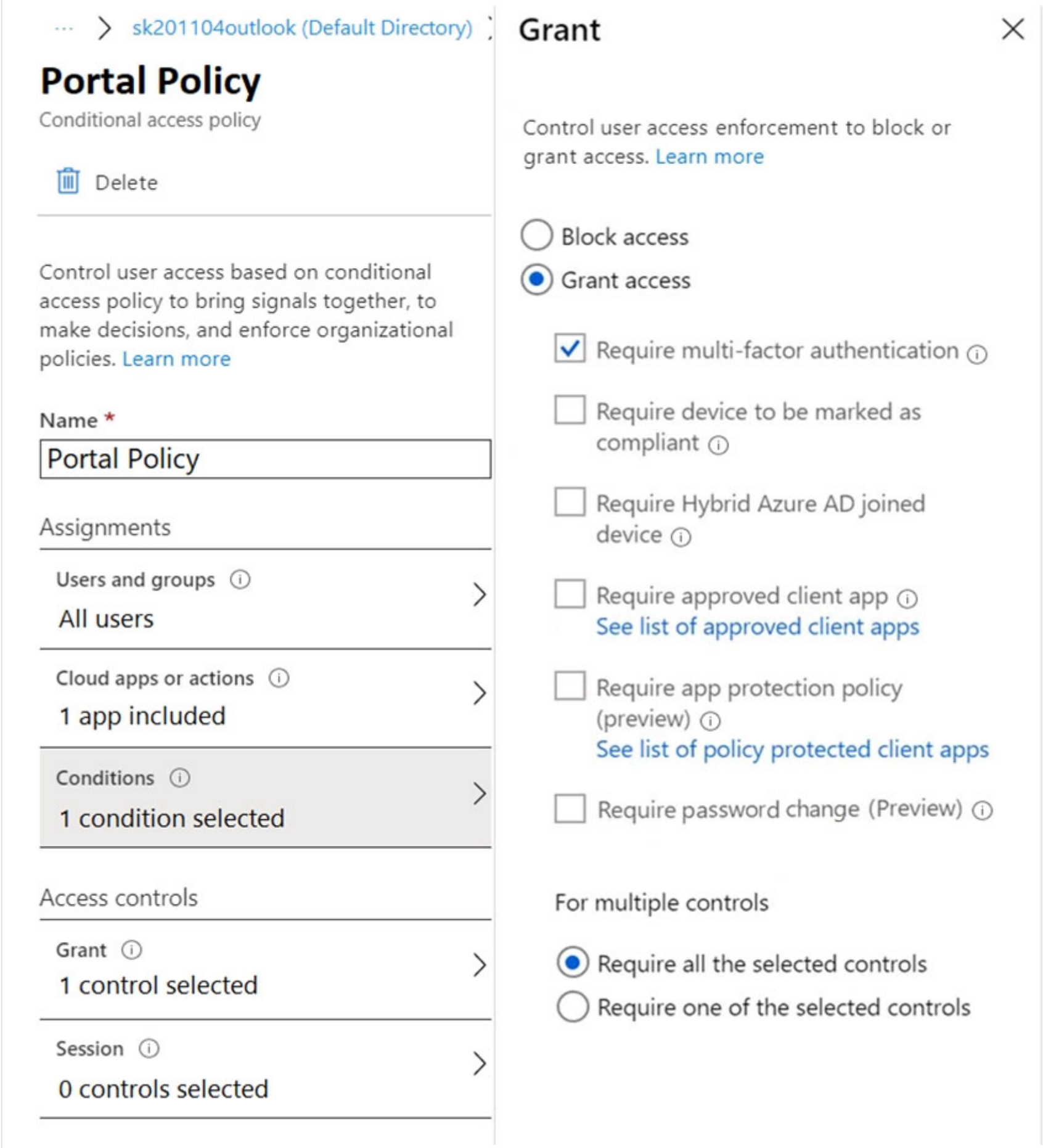
You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)

https://t.me/learningnets



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.	○	○

https://t.me/learningnets

Correct 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

justinp 5 days, 9 hours ago

on exam, today

upvoted 1 times

catsforthewin 3 days, 18 hours ago

What do you think the correct answer is?

upvoted 1 times

gsidhwani77 1 week, 2 days ago

Yes Yes No [Contoso is included for MFA] and hence OutSide Contose it will be allowed without MFA

upvoted 1 times

Jacquesvz 3 days, 15 hours ago

Given answers are correct. for nr2, The policy does not apply to web services host in Azure.

upvoted 1 times

gsidhwani77 1 week, 2 days 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

https://t.me/learningnets

Question #25 *Topic 1*

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	Bock 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.	○	○

Correct Answer:

Answer Area Yes,Yes,No

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.	○	●

nihao381 Highly Voted 3 months, 3 weeks ago

Since conditional access is being used the per-user MFA status is no longer applicable. Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

Thusly our answers will look like:

Yes -- User1 is excluded from Policy1 as exclusion takes precedence. That means she hits Policy2 which grants access with MFA.
Yes -- User2 is excluded from Policy1. Policy2 is a complete miss. Policy3 matches the include but misses the location. We drop down to a final match on Policy4 which is specific to User2 which does grant access with MFA.
No -- User2 is excluded from Policy1. Policy2 is a complete miss. Policy3 we match the include and location which results in blocking access.

upvoted 40 times

Dineshvishe 1 week, 5 days ago

https://t.me/learningnets

Comfused with Last answer, if ploicy3 blocks acces and Policy4 should provide user2 access.
upvoted 1 times

ChinkSantana 3 weeks, 4 days ago
SPot On!!!!
upvoted 1 times

macco455 3 months, 3 weeks ago
Yes, YES, NO, agree with nihao381 reasoning
upvoted 5 times

hang10z 3 months, 3 weeks ago
You are correct.
upvoted 1 times

rosietk Highly Voted 4 months ago
I think the answer is No, No, No.
User 2 cannot access from Seattle as from any location they are required to use MFA which is disabled User 2 and User 1.
upvoted 10 times

Fred64 4 months ago
This is not true:

https://www.vcloudnine.de/mfa-disabled-but-azure-asks-for-second-factor/
Provided answer is right: NO YES NO
upvoted 6 times

Geeky93 4 months ago
Agree with you
upvoted 3 times

gcpbrig01 4 months ago
policy2 and policy4 wont kick in since the MFA is not enabled for the users. with just policy1 and policy3 in play, i would say the answer is, No, Yes, No
upvoted 5 times

justinp Most Recent 5 days, 9 hours ago
on exam, today
upvoted 1 times

hasanreza 1 month, 2 weeks ago
Just tested this MFA : User disabled , however based on Conditional access the user would be given the option to sign in and then prompted for MFA .
upvoted 1 times

PSunny 1 month, 2 weeks ago
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies
upvoted 1 times

3abmula 1 month, 2 weeks ago
Correct answer Yes, Yes, No.

There is a big debate about the MFA status is "Disabled" for the users. So I have decided to test it. Well, if a conditional access policy requires MFA, and MFA is disabled for that user, anyways the user will be prompted to enroll in MFA, and even after completing the enrolment, status will remain Disabled in MFA page for that use, because everywhere else it doesn't require MFA, only for the app included the conditional access.
upvoted 2 times

teehex 2 months ago
Yes - Yes - No

If your organization is a previous user of per-user based Azure AD Multi-Factor Authentication, do not be alarmed to not see users in an Enabled or Enforced status if you look at the Multi-Factor Auth status page. Disabled is the appropriate status for users who are using security defaults or Conditional Access based Azure AD Multi-Factor Authentication.

https://docs.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, as an exclude action overrides an include in policy.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups#exclude-users

Only two references above you need to read to answer.
upvoted 1 times

Cyberbug2021 2 months, 1 week ago
Short answer - given answers are correct.

https://t.me/learningnets

this is policy, not asg, nsg or firewall rules block wins over everything, order doesn't matter
upvoted 2 times

Cyberbug2021 2 months, 1 week ago
If both grant and block policies match, block will always win. No exceptions!
upvoted 2 times

Cyberbug2021 2 months, 1 week ago
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
upvoted 1 times

Cyberbug2021 2 months, 1 week ago
the order of the policy does not matter, the more restrictive policy wins.
upvoted 2 times

Cyberbug2021 2 months, 1 week ago
This is policy, not firewall rules, ASG or NSG, order does not matter
upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago
YES, YES, NO
upvoted 1 times

Cyberbug2021 2 months, 1 week ago
Given answer is correct, No, Yes, No - sorry
upvoted 2 times

vijeet 2 months, 3 weeks ago
conditional access policies are not accessed in any order. if 2 policies match, where one policy allows and another blocks, the block policy wins without any exceptions.
User 1: YES - because Policy 1 and 3 excluded either Group 1 or 2 which user 1 is part of. The only policy that matches is Policy 2.
upvoted 3 times

teamaws 3 months, 1 week ago
Ahh, the penny drops. Enabling Azure AD Multi-Factor Authentication through a Conditional Access policy doesn't change the state of the user. Don't be alarmed if users appear disabled. Conditional Access doesn't change the state.

Don't enable or enforce per-user Azure AD Multi-Factor Authentication if you use Conditional Access policies.
upvoted 1 times

sureshatt 3 months, 3 weeks ago
Answer is YES, YES, NO.

User's MFA status has nothing to do with Conditional Access Policies. The default MFA status for any user in AAD is disabled. However, if a Conditional Access Policy enforce users to use MFA, then those users should enrol themselves for MFA. And that would also not change the MFA status. "Enabling Azure AD Multi-Factor Authentication through a Conditional Access policy doesn't change the state of the user. Don't be alarmed if users appear disabled. Conditional Access doesn't change the state." https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

YES: only Policy 2 affects the User 1. Therefore user1 can access from any location after registering for MFA
YES: in this case only Policy 4 is effective for user2, therefore user2 can access the app from any location.
NO: in this case Policy 3 (Boston location) is effective for user2, therefore the access will be blocked.
upvoted 6 times

Jeb 3 months, 4 weeks ago
The given answer is correct
upvoted 3 times

pittaya_r 3 months, 4 weeks ago
I think the first box should be Yes because
User1 is in both Group1 and Group2
In the ref. state that "When organizations both include and exclude a user or group the user or group is excluded from the policy"
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups#exclude-users
Policy1 include Group1 but exclude Group2 so it is exclude User1 from Policy1
Policy3 include Group2 but exclude Group1 so it is exclude User1 from Policy3
so there is no block access for User1 when access App1 from Boston IP
upvoted 6 times

https://t.me/learningnets

https://t.me/learningnets

Question #26 *Topic 1*

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

Correct 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

jessicamendez10 Highly Voted 3 months, 3 weeks ago

In exam 20/03/2021

upvoted 16 times

Sammy50 2 months, 1 week ago

Thanks

upvoted 1 times

hang10z 3 months, 3 weeks ago

https://t.me/learningnets

Thank you Jessica, important info
upvoted 4 times

teehex Highly Voted 2 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 14 times

Sjn9 Most Recent 3 months ago
Correct
upvoted 1 times

debsauce 4 months ago
The give answer is correct
upvoted 7 times

hang10z 3 months, 3 weeks ago
Verified
upvoted 1 times

https://t.me/learningnets

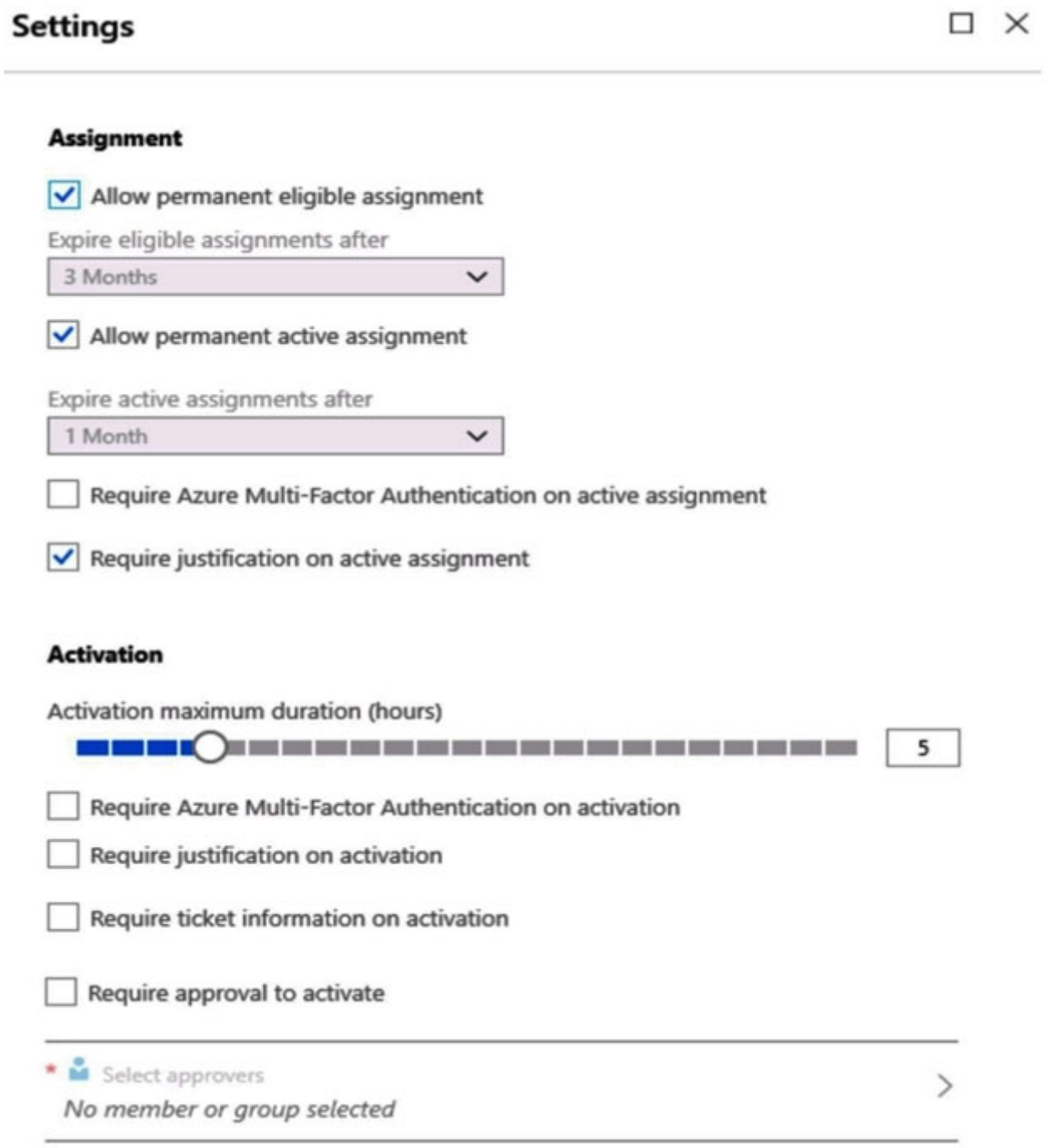
Question #27 Topic 1

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.



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.	○	○

https://t.me/learningnets

Correct 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

rosietk Highly Voted 4 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 34 times

BalderkVeit 1 month, 3 weeks 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 2 times

Startkabels 3 months, 3 weeks 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 2 times

Startkabels 3 months, 3 weeks 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 2 times

Pinto Highly Voted 4 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 11 times

justinp Most Recent 5 days, 9 hours ago
on exam, today
upvoted 1 times

Terminator10 1 month, 3 weeks ago
What would be the right answer? NNY?
upvoted 1 times

Ed2learn 1 month, 3 weeks ago

https://t.me/learningnets

The explanation is backward. Group 1 is active Group 2 is eligible. The explanations have this reversed. the answer is NO (active) Yes (the need to provide a justification but no approval) and No (active)

upvoted 2 times

MarioMK 1 month, 3 weeks ago

Q1: No. 5 hours is the duration
Q2: Yes. The role will appear under the Eligible assignments. The user must click on Active and provide justification.The browser will refresh and from that moment on,the role will be assigned.
Q3: No. Already active since he is member of group 1.

upvoted 1 times

AYap 2 months, 1 week ago

I setup the environment to test.
User1 doesn't need to activate the role because it is Active Assignment - No
User2 need to activate the role and once it is done, he/she will have the role assigned - Yes
User 3 has the role actively assigned when login, however, he/she also see an Eligible Assignment and he/she can proceed with activation process. At the end of activation, he/she has 2 entries appeared in Active Assignment with State showing Assigned and the other showing Activated - so if we read the words properly, User3 can activate the role, answer is YES

upvoted 6 times

Cyberbug2021 2 months, 2 weeks ago

No Yes NO

upvoted 2 times

Fred64 2 months, 2 weeks ago

NNY
box1: 5 hours is the duration the role is activated not in
box 2: user2 is eligible, so shoud manually activate
box3: users 3 checked everything, so...

upvoted 2 times

R_ae 2 months, 2 weeks ago

Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours....https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

upvoted 1 times

rgullini 2 months, 2 weeks ago

Box 1: No, the role is already assigned. The 5 hours period is the time the activation lasts.
Box 2: Yes, need to provide justification, but no approval is required
Box 3: No, the role is already assigned as the user is already member of group 1

upvoted 3 times

MikeB19 3 months ago

Agreed with rosietk at first but the more i read this the more i realize it is y y y. The reason is the role can only be active for 5 hours. Therefore it doesn't matter if u r an eligible or active user. The activation will always expire in 5 hours and I will be forced to re activate no matter what ur status is.

upvoted 3 times

souvik123 2 months, 2 weeks ago

I have the same view as Mark.
YES YES YES

upvoted 1 times

Startkabels 3 months, 3 weeks ago

Box 1: YES. Activation time is 5 hours meaning the role cannot be activated after 5 hours ("can only be activated in 5 hours")
Box 2: Yes. IF the user activated the role (for which he has to provide justification) it will be effective immediatly
Box 3: YES, the user is a member of both groups and so he can activate the rol.
Nowhere it states that he already has the rol as some people say.

upvoted 3 times

rgullini 2 months, 3 weeks ago

Box 1: NO, your explanation is not right. Please read: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

upvoted 2 times

macco455 3 months, 2 weeks ago

Box 1 wording is incorrect. You can only activate a role for a specific period of time that it can be used. Not a specific period of time you need to wait to use it. Therefore Bow 1=NO
Box 2: No, as use 2 would bee to put in a justification to have the role approved by an eligible approver before he can start using it
Box 3: Yes, user 3 can activate the role(see dadageer explanation above).

upvoted 4 times

Jeb 3 months, 4 weeks ago

No, Yes, No

upvoted 1 times

dadageer 4 months ago

https://t.me/learningnets

- User1 can only activate the Security Admin role (for)* five hours: NO (mem of Group 1, perm assigned)
- If User2 activates the Sec Admin role, the user will be assigned role immediately: NO (mem of Group 2, Eligible, will have to manually activate)
- User3 can activate the Security Admin role: This is tricky! In this scenario as user is member of an "active" group and an "eligible" group, he will have the role assigned immediately BUT will also have the privilege to ACTIVATE the role when the Active role Expires in 1 month! So the answer is YES, user can activate the role.

upvoted 4 times

dadageer 4 months ago

Sorry User2 is YES! If he goes and activates the role will be assigned immediately
Answers: No, Yes, Yes

upvoted 3 times

abrahamtek 1 month ago

No role will not be assigned immediately. User 2 has to provide Justification .The check box is checked if you look at the question

upvoted 1 times

abrahamtek 1 month ago

Please remove my post .i am wrong

upvoted 1 times

dadageer 4 months ago

So Answers are: No, No, Yes

upvoted 2 times

OhBee 3 months, 2 weeks ago

I'll have what you're drinking!

upvoted 5 times

gcpbrig01 4 months ago

No – user will be active on the role when logged in.
No – "Require justification on active assignment" conditions are enforced for activating the role.
https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings#require-justification
You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the Require justification on activation box.

No – User will be active on the role when logged in.

upvoted 1 times

Startkabels 3 months, 3 weeks ago

When user1 will activate the role it will be effective immediately but I think they mean that the user can only activate the role in 5 hours and not after that.
It doesnt matter that there is a justification requirement. When the user activates the role, meaning he did provide a justification, the role will be effective immediately. If the user would not provide a justification he would not be able to activate to begin with.

upvoted 2 times

https://t.me/learningnets

https://t.me/learningnets

Question #28 Topic 1

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.

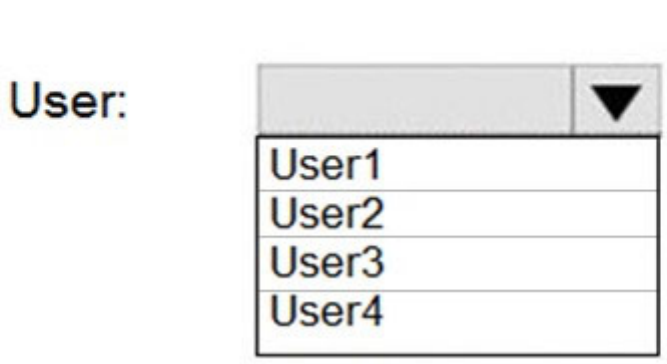
The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

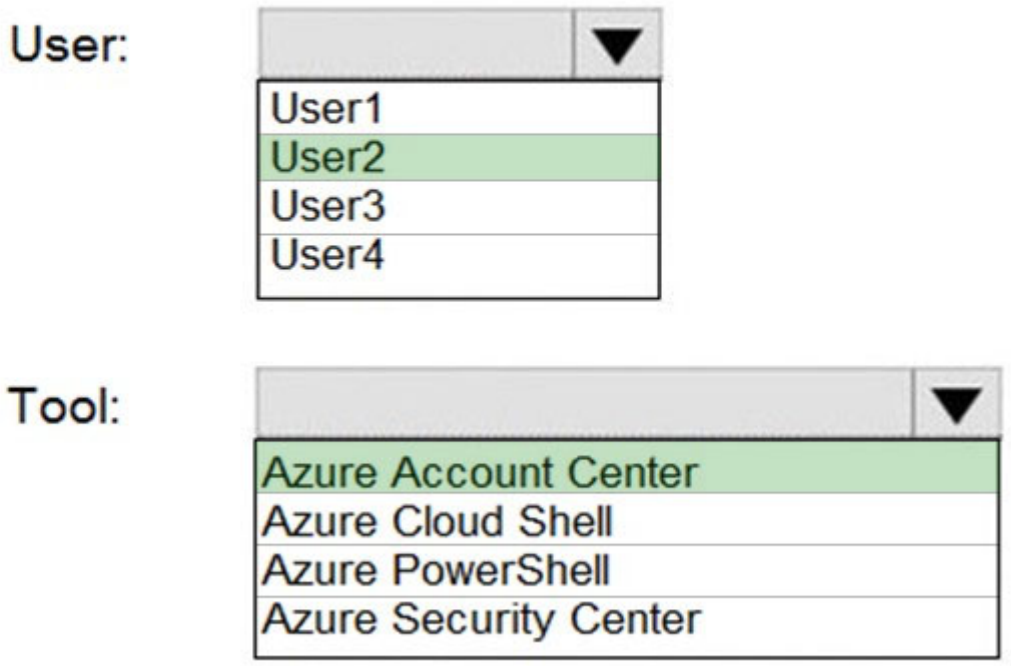
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Answer Area



Correct Answer:

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 -

https://t.me/learningnets

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

https://t.me/learningnets

Question #29 *Topic 1*

SIMULATION -

The developers at your company plan to create a web app named App10598168 and to publish the app to https://www.contoso.com.

You need to perform the following tasks:

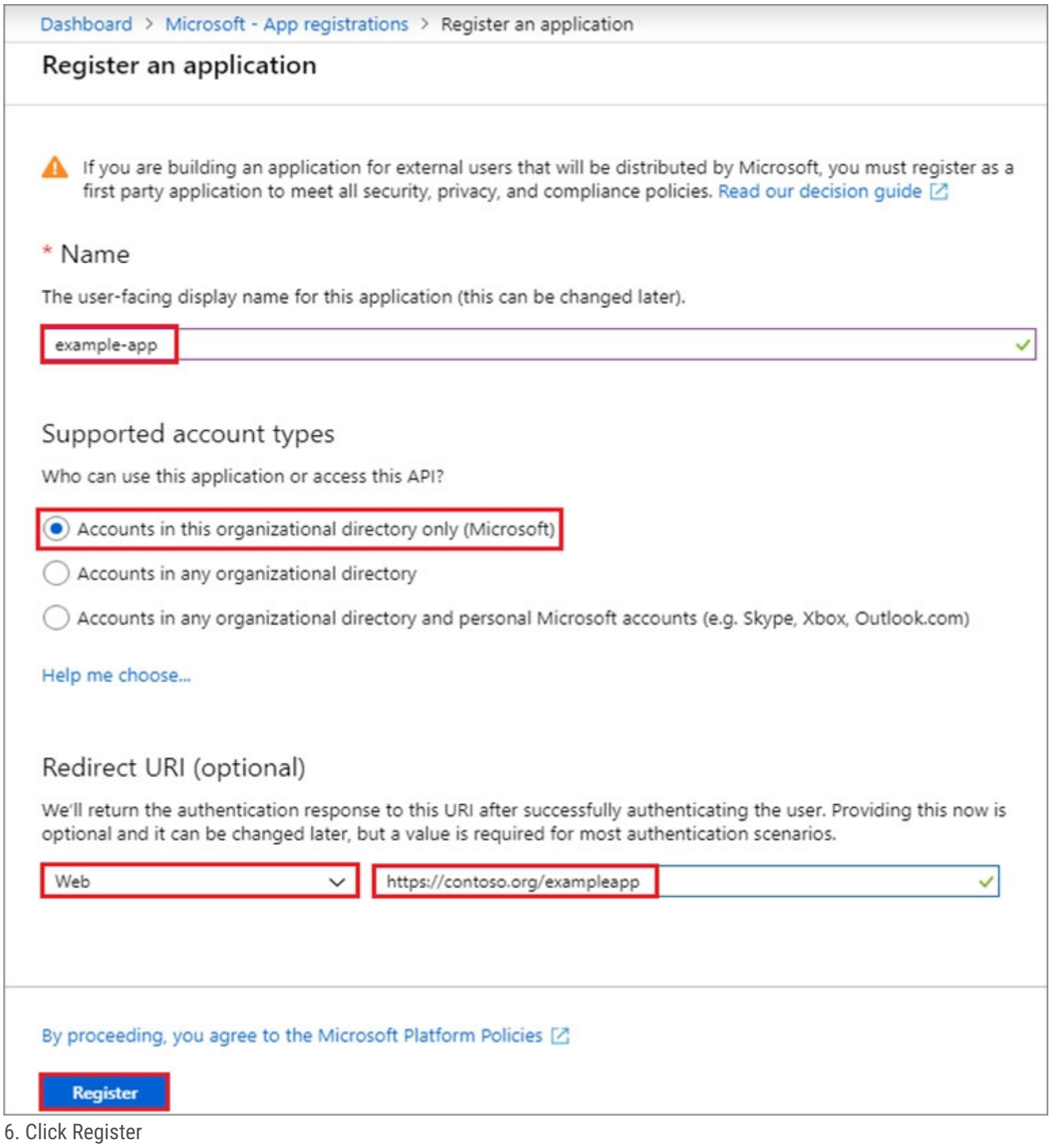
- Ensure that App10598168 is registered to Azure Active Directory (Azure AD).
- Generate a password for App10598168.

To complete this task, sign in to the Azure portal.

Correct 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 App10598168 . 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.



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

https://t.me/learningnets

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

RAY2021 1 month, 2 weeks ago

This is an experiment task. But not in exam any more since COVID.

upvoted 1 times

JohnYinToronto 4 months ago

Not sure what the questions are, but the said procedure is verified.

upvoted 1 times

https://t.me/learningnets

Question #30 *Topic 1*

SIMULATION -

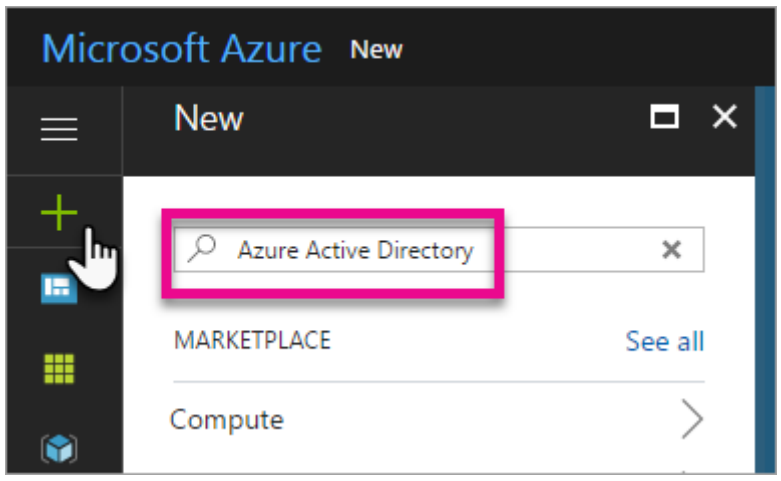
You need to create a new Azure Active Directory (Azure AD) directory named 11641655.onmicrosoft.com and a user named User1 in the new directory. The solution must ensure that User1 is enabled for Azure Multi-Factor Authentication (MFA).

To complete this task, sign in to the Azure portal.

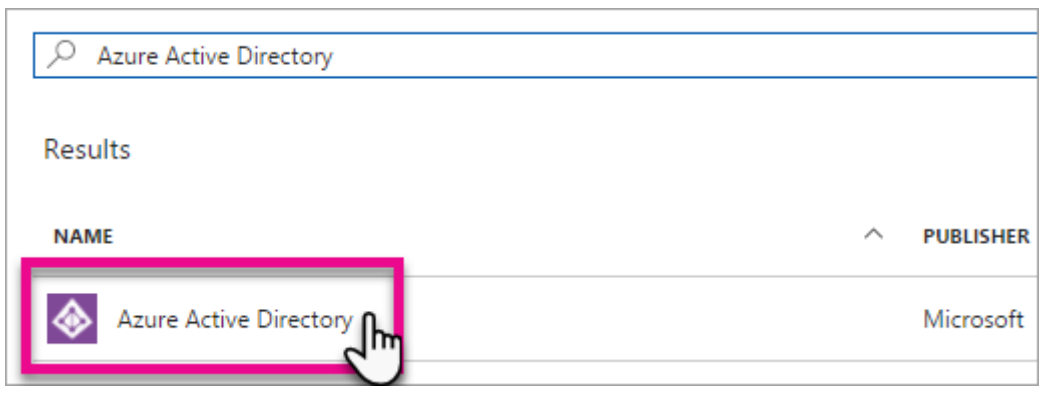
Correct Answer: *See the explanation below.*

Step 1: Create an Azure Active Directory tenant

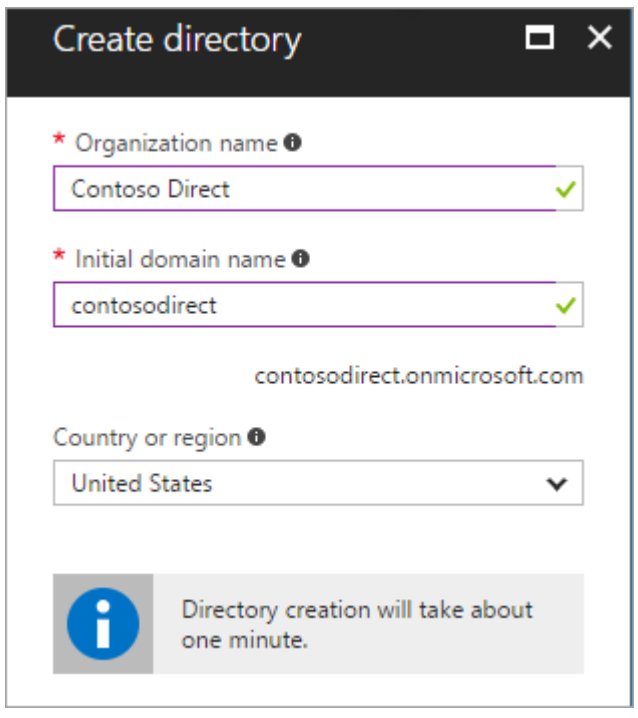
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



4. Select Create.
5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory is created.

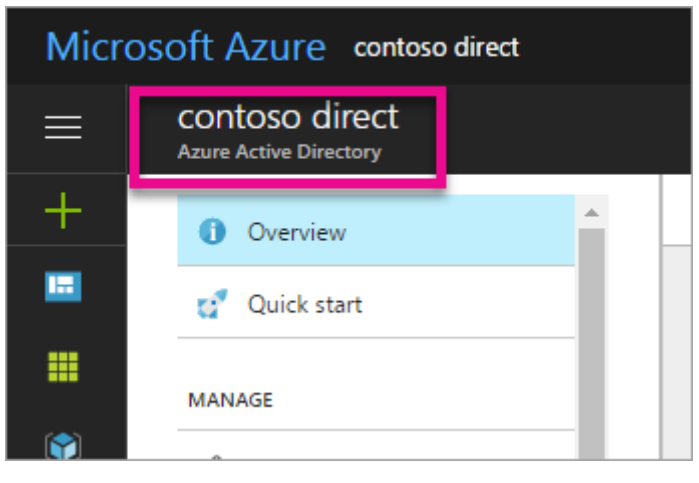


6. After directory creation is complete, select the information box to manage your new directory.

Next, you're going to add tenant users.

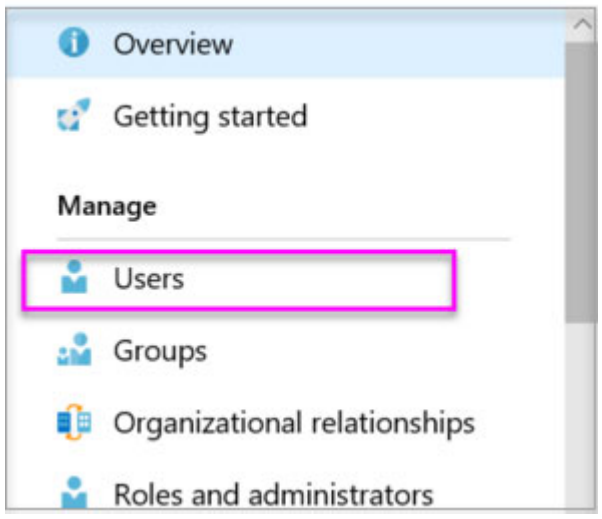
Step 2: Create an Azure Active Directory tenant user

7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



https://t.me/learningnets

8. Under Manage, select Users.

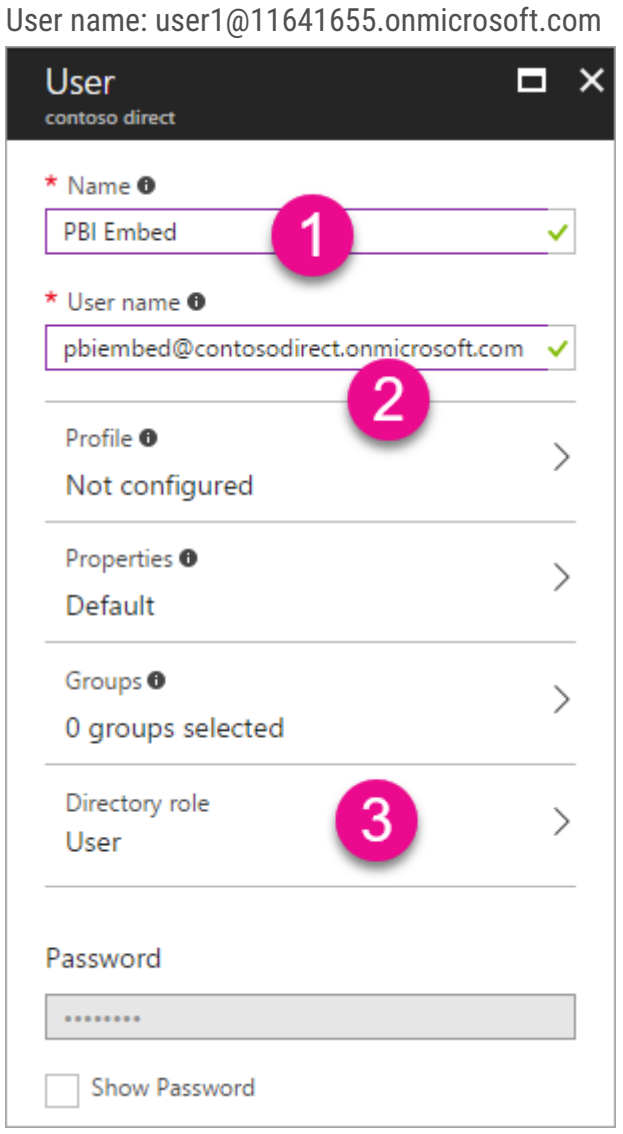


9. Select All users and then select + New user.

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@11641655.onmicrosoft.com



Reference:

https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

Geeky93 Highly Voted 4 months ago

To implement MFA, you can mainly follow the task 5 of this official Az-500 lab :

https://microsoftlearning.github.io/AZ500-AzureSecurityTechnologies/Instructions/Labs/LAB_04_MFAConditionalAccessandAADIdentityProtection.html#exercise-2-implement-azure-mfa

upvoted 7 times

Lyonel Most Recent 1 week, 2 days ago

Will there be simulation questions in the AZ-500 Exam?

upvoted 1 times

Vanht 4 days, 10 hours ago

This is an experiment task. But not in exam anymore since COVID

upvoted 1 times

PSunny 4 months ago

Missing MFA stesps

upvoted 4 times

rgullini 2 months, 2 weeks ago

Right. Missing MFA steps.

https://t.me/learningnets

upvoted 1 times

https://t.me/learningnets

Question #31 *Topic 1*

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

Correct Answer:

Answer Area MFA,MFA,MFA

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:

https://t.me/learningnets

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

canonigo Highly Voted 3 months, 3 weeks 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 30 times

cjace 1 month, 2 weeks ago

MFA MFA MFA

upvoted 8 times

Denn81 1 month, 2 weeks ago

Sign-ins from infected devices - Medium thus MFA

upvoted 4 times

eroms 1 month, 3 weeks ago

User 3 --> Prompted for MFA

upvoted 3 times

OhBee 3 months, 2 weeks 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 4 times

3abmula 1 month, 1 week 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 1 times

macco455 3 months, 2 weeks 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 4 times

Narragr Highly Voted 4 months ago

User1 belongs to Group1 and Group2, since exlusion take precedence over inclusion, therefore the policy will not be enforced on the user1.
User1 can sign-in by using a Username/Password method.

upvoted 17 times

macco455 3 months, 3 weeks ago

Yes the user is in both group and the exclude group takes precedence, BUT the users is enabled to use MFA so that supersedes the sign in risk policy being excluded thus he will be prompted for MFA

upvoted 11 times

A365 3 months, 3 weeks ago

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

upvoted 1 times

Startkabels 3 months, 3 weeks ago

True, user 1 is excluded and is promped username and password

upvoted 2 times

Geeky93 4 months ago

Agree with your explanation

upvoted 1 times

ManOnTheMoon 3 months ago

Agreed

upvoted 1 times

Rahulbard Most Recent 6 days, 14 hours ago

MFA will be applied in all cases
If user does not have MFA, they will be forced to register
All conditions are Medium or higher risk. The only low risk is suspicious IP activity

upvoted 1 times

Kilroy 1 week, 6 days ago

https://t.me/learningnets

it's correct
"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
upvoted 1 times

Deepmindx 3 weeks ago
how come you are saying that infected device is low while it is clearly shown in the table as medium !?!

Sign-in Activity

Risk Level

Users with leaked credentials

High

Sign-ins from anonymous IP addresses

Medium

Sign-ins from infected devices

Medium

Sign-ins from IP addresses with suspicious activity

Low

Sign-ins from unfamiliar locations

Medium
upvoted 2 times

Rajesh123 1 month ago
If MFA status for user 2 and user 3 is disabled the MFA will not be Prompted so it will be Blocked
upvoted 1 times

Goseu 1 month, 1 week ago
Given answers seem correct :
At first the most important thing is to pay attention that this is not a CA policy but a Sign in risk policy .
So for the first user is excluded from the risky sign in policy but he will be prompted for MFA in any case.
For the 2nd and 3rd case the user will be blocked because MFA registration is a prerequisite and only works on registered users.
Check https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies video after 1:00.
upvoted 2 times

teehex 2 months ago
The given answers aren't correct.

User1 belongs to Group 2 which is excluded so he won't be asked by MFA. User1's MFA is Enabled. It is not enforced. It means if he hasn't registered MFA he doesn't need MFA.

User2 needs MFA because it meets all conditions. "Sign-in from unfamiliar location" is a Medium risk level.

User3 doesn't need MFA because "Sign-in from an infected device" is a Low risk level.

Correct answers:
- Sign in by using a username and password only
- Be prompted for MFA
- Sign in by using a username and password only.
upvoted 8 times

3abmula 1 month, 2 weeks ago
User1 will always have to use MFA, sign in from anonymous IP or not, MFA is enabled so will have to enroll and use MFA every time.
upvoted 1 times

eroms 1 month, 3 weeks ago
How is "Sign-in from an infected device Low risk ? That is Medium risk. They all Use MFA to sign in

https://t.me/learningnets

upvoted 3 times

Fred64 2 months, 1 week ago
Blocked is never the answer because it is not asked by the conditions
upvoted 1 times

Cyberbug2021 2 months, 1 week ago
user+pw, MFA, MFA

user 1 - policy doesn't apply group 2 excluded, but MFA enabled but not enforced
upvoted 2 times

Cyberbug2021 2 months, 1 week ago
Sorry - MFA, MFA, MFA

user 1 enabled MFA meaning he will be prompted for MFA registration and his stated will change to MFA enforced.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

other two are medium risk so policy applies
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
User 3 is signing in from INFECTED device - medium risk - MFA applies
upvoted 3 times

CASGTI 2 months, 3 weeks ago
Tested in LAB:
a) MFA ... User1, will be asked MFA if the MFA status is enabled. (here, is not required by the CA policy, but is required by the MFA status)
b) MFA ... User2, will be asked MFA. (here, is required by the CA policy, and will ask for it regardless the MFA setup is disabled.)
c) User/Password. (here is not required by CA policy or MFA)

Notes: Unfamiliar location and anonymous IP are "medium", but infected device is "low"
upvoted 7 times

DigitalDelta 1 month, 3 weeks ago
C - WRONG. infected device is a MEDIUM

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
upvoted 1 times

cs4vEr 2 months ago
exactly !
upvoted 1 times

vijeet 2 months, 3 weeks ago
Users will be prompted for MFA when the conditional access policy applies to them. Users do not (and should not) be configured for user-based MFA for conditional access (CA) policies to work. If user-based MFA is enabled, it will override the CA policies for that user.

For User1: YES
upvoted 2 times

alexvno 2 months, 3 weeks ago
1. MFA - U1 MFA Enabled
2. MFA - U2 Unfamiliar location risk level Medium

https://t.me/learningnets

3. MFA - U3 Infected devices risk level Medium

upvoted 5 times

teamaws 3 months, 1 week ago

User+PW
Prompted MFA
Prompted MFA

upvoted 3 times

Startkabels 3 months, 1 week ago

1: Sign in (user is excluded)
2: Sign in (I believe unfamiliar location is low risk nowadays)
3: MFA (Infected device is medium risk i believe, user based MFA settings are not relevant when using conditional access or AIP risk policies)

upvoted 1 times

jessicamendez10 3 months, 3 weeks ago

In exam 20/03/2021

upvoted 5 times

sureshatt 3 months, 3 weeks ago

Not really sure what microsoft is trying to test here. They themselves are saying "While Microsoft does not provide specific details about how risk is calculated" and yet, they want us to know what microsoft doesn't tell ? frustrating...

upvoted 6 times

_adem 3 months, 2 weeks ago

Good point

upvoted 2 times

https://t.me/learningnets

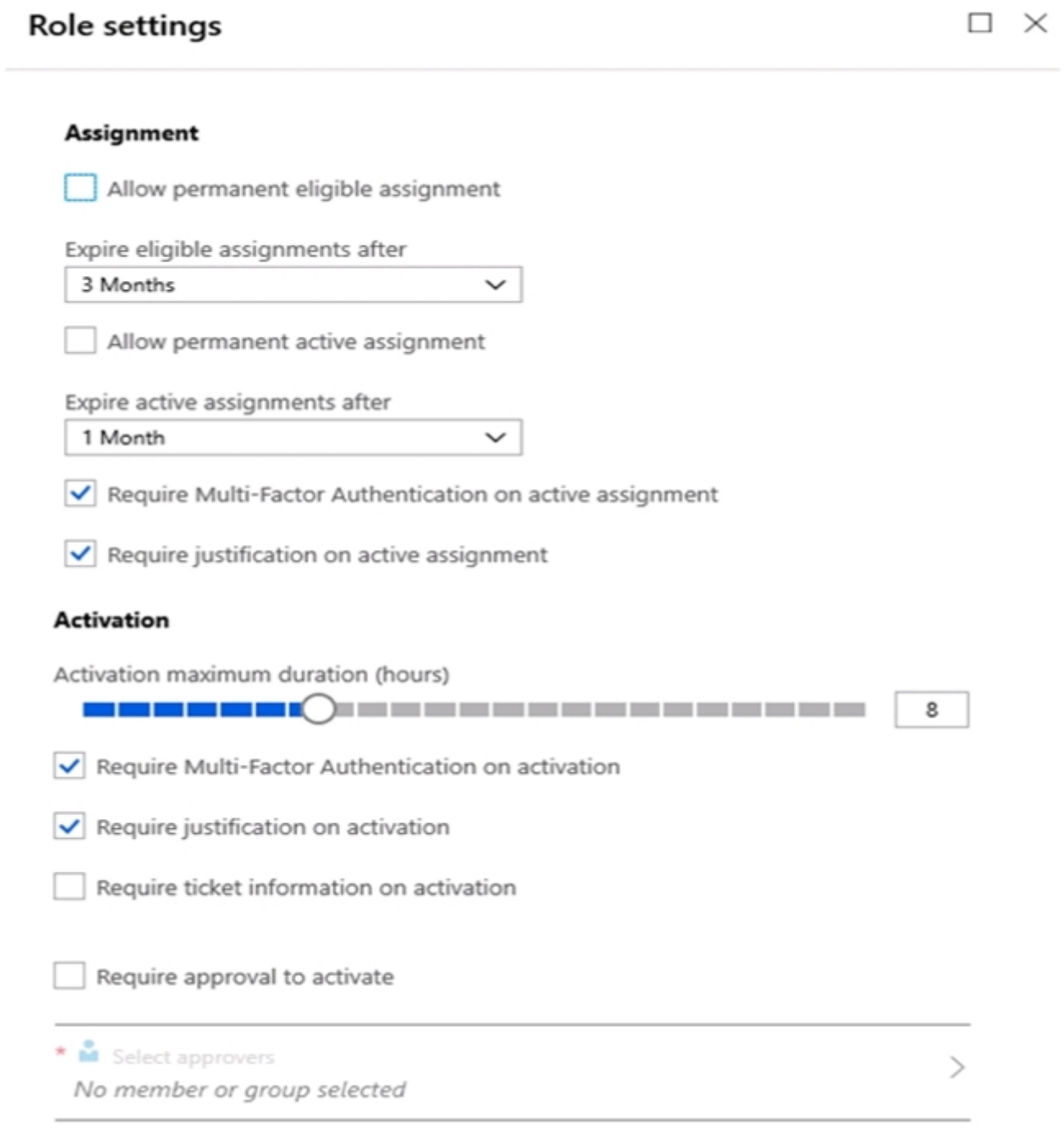
Question #32 Topic 1

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.)



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.	○	○

https://t.me/learningnets

Answer Area Yes,Yes,No

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.	○	○

Correct Answer:

References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

hang10z Highly Voted 3 months, 3 weeks 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 33 times

BalderkVeit 1 month, 3 weeks ago
agree:
Yes - as MFA doesn't make a difference in that case. PIM does not care about it
YES - he can use is, that's legit.
No - double kill - he couldn't activate it, as he had "active role" (he would receive error. He could USE it), but it was active for 1 month, so has neither active nor eligible now. (15th june)
upvoted 2 times

Jacquesvz 3 days, 15 hours ago
Agreed. YES, YES, NO.

User 3, no because, they would need to request for extension or renewal. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Extend and renew assignments:
After you set up your time-bound owner or member assignments, the first question you might ask is what happens if an assignment expires? In this new version, we provide two options for this scenario:

Extend – When a role assignment nears expiration, the user can use Privileged Identity Management to request an extension for the role assignment
Renew – When a role assignment has already expired, the user can use Privileged Identity Management to request a renewal for the role assignment
Both user-initiated actions require an approval from a Global Administrator or Privileged Role Administrator. Admins don't need to be in the business of managing assignment expirations. You can just wait for the extension or renewal requests to arrive for simple approval or denial.
upvoted 1 times

rgullini 2 months, 2 weeks 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 2 times

OhBee 3 months, 2 weeks 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

Startkabels 3 months, 3 weeks 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

Narragr Highly Voted 4 months ago
User3 cannot because his active right is expired on the 15th June 2019

https://t.me/learningnets

upvoted 15 times

Geeky93 4 months ago

How can User2 use contributor role if he has MFA disabled ? For me it seems to be No No NO

upvoted 6 times

sureshatt 3 months, 2 weeks 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 5 times

gcpbrig01 4 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 14 times

LJack 4 months ago

Agree, no yes no

upvoted 4 times

HusainK Most Recent 1 month, 1 week ago

The given answer is correct IMO.
YES YES YES
For third question, the date is 15th June, that is 45 days since assignment. Which means the active role has expired (1 month) and he is currently having eligible role assignment (which shall expire 3 months from 1st of May).

upvoted 3 times

Finae 1 month, 1 week ago

I don't understand, are you saying the user will assume eligible assignment automatically at the expiration of the active assignment without being reassigned? Will the user not lose the role at the expiration of the active assignment?

upvoted 2 times

DCarma 3 weeks, 5 days ago

Yes, I would also assume they just lose their active assignment and aren't automatically 'eligible' for the next 2 months.

upvoted 1 times

MarioMK 1 month, 3 weeks ago

Q1: Yes. Even with the MFA disabled, once the user clicks on Activate,the following warning will be shown"Additional verification required. Click to continue ". The user must then do the MFA challange. Therefore, for PIM it does not make no difference at all whether MFA for the specific user is enabled or disabled.
Q2: Yes.
Q3: No. Already active. If a user tries to activate an already active role, an error message will be shown.
Tested in Azure.

upvoted 1 times

3abmula 1 month, 2 weeks ago

Q3: Even active assignment has already expired.

upvoted 2 times

souvik123 1 month, 3 weeks ago

The answer is YES, YES, NO.

upvoted 2 times

teehex 2 months ago

User1's assignment is eligible so it can activate the role - Yes
User2's assignment is active so it can use Contributor role. However it needs to complete MFA setup . Still a Yes
User3's assignment is active so basically it has the role. However look at "Expire active assignments after" setting it is set 1 month. On June 15, 2019 the active assignment already expired so User3 can't use Contributor role. It could only activate when its assignment is Eligible. Correct answer is NO

YES - YES - NO

upvoted 4 times

IlPerdan0 2 months, 1 week ago

I think the answer for no 3 is Yes as the given answer stated. Because we can still renew the expired assignment on PIM.
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-renew-extend

upvoted 2 times

Cyberbug2021 2 months, 1 week ago

Given answer is correct - User 3 can activate after June 1st as the first activation is only for a month, he is still eligible fro 3 month, so he can activate again for a during of 8hrs at a time.

upvoted 1 times

ChiragA 2 months, 2 weeks ago

Yes
Yes
No

https://t.me/learningnets

upvoted 3 times

Azuriste 2 months, 3 weeks ago

YES YES NO

upvoted 4 times

rraviska 2 months, 3 weeks ago

N N N
User1 can't activate the role since activation requires MFA and its is disabled for the user (N)
User2 is role activated when logged in on May 15, 2019 but requires MFA for use. (N)
User3 active role expired after 1 month on 1st June 2019. Ccannot activate on June 15 MFA disabled (N

upvoted 3 times

cannibalcorpse 3 months, 1 week ago

With "security defaults" all users are forced to use MFA so we can bypass the if the MFA status is enabled/disabled for the users
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414
"For starters, we're doing the following:

Requiring all users and admins to register for MFA.
Challenging users with MFA - mostly when they show up on a new device or app, but more often for critical roles and tasks.
Disabling authentication from legacy authentication clients, which can't do MFA."

Even though, you can force any users to use MFA with conditional access and PIM
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?tabs=new#require-multi-factor-authentication-on-activation

upvoted 2 times

Emperor 3 months, 2 weeks ago

Y- user can activate role thru PIM since he's eligible
Y - active
N - Expired

upvoted 7 times

gcgonzales 3 months, 3 weeks ago

No. No. Yes.

Users must register first to the Azure AD Multi-Factor Authentication so PIM can use the MFA validation.

https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-how-to-require-mfa

upvoted 1 times

Startkabels 3 months, 3 weeks ago

No, Yes, No
Box 1: No, Because user1 has an eligable assignment which requires MFA to activate and MFA is disabled for user1
Box 2: Yes, because user2 has an active assignment that does not require MFA to activate
Box 3: No, because the assignment is expired

upvoted 4 times

jessicamendez10 3 months, 3 weeks ago

In exam 20/03/2021

upvoted 3 times

Jeb 3 months, 4 weeks ago

Yes, No, No

upvoted 2 times

https://t.me/learningnets

https://t.me/learningnets

Question #33 Topic 1

HOTSPOT -

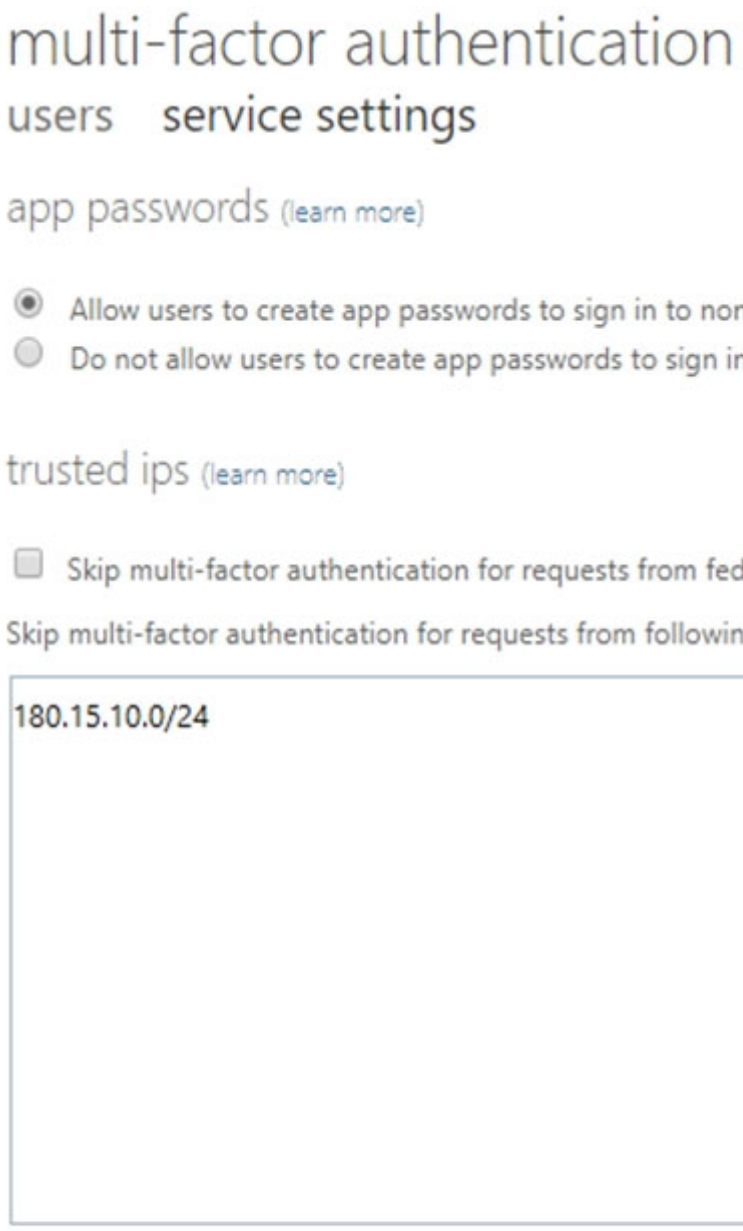
You work at a company named Contoso, Ltd. that has the offices shown in the following table.

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.



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

https://t.me/learningnets

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.	○	○

Correct Answer:

Answer Area No,No,Yes

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 months ago

Answer is : No-No-Yes.

upvoted 57 times

LJack 4 months ago

Agree should be no, no, yes

upvoted 9 times

Sethoo 4 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 7 times

Narragr 4 months ago

Why the option trusted ip is not checked

upvoted 1 times

xaccan 4 months ago

Check box is not for trusted ip, it is for federated users

upvoted 10 times

Pinto Highly Voted 4 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 19 times

LazyEngineer Most Recent 1 day, 7 hours ago

Should be No-No-Yes

upvoted 1 times

Madball 6 days, 20 hours ago

Q: When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA?
A: No, because User1 selected to not be asked again for 14 days.

https://t.me/learningnets

Q: When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA?
A: No, because Boston is a trusted location (Ignore the checkbox, this is for federated users, meaing if the environment is using ADFS).

Q: When User1 signs in to a new device from Seattle office on June 7, the user will be prompted for MFA?
A: Yes, because Seattle is not a trusted location.

upvoted 2 times

Jacquesvz 3 days, 14 hours ago

Perfect, agree100%. thank you for the explanation! 👍

upvoted 1 times

Dineshvishe 1 week, 2 days ago

The answers are perfectly correct. Don't get confuse with trusted IP. It is not checked.
No
Yes
Yes

upvoted 1 times

sathas 3 weeks, 1 day ago

Answer : No, Yes , Yes
1) No: user selected not to ask for 14 days
2) Yes: Skip IP option not selected so MFA will be done
3) Yes: Because of new device

upvoted 3 times

Tribhuvan 4 weeks ago

The box for trusted IPs is unchecked. This makes the answer to second question as yes.

upvoted 1 times

DCarma 3 weeks, 5 days ago

The box is for 'federated' users on the intranet. The exclusion still applies.

upvoted 1 times

Enitan 1 month, 2 weeks ago

No
No
Yes

upvoted 1 times

teehex 2 months ago

Because the Remember MFA is set (14 days) so User1 isn't asked by MFA. Correct answer is NO.

The statement #2 is a little tricky. The screenshot is showing that Cloud-based Azure MFA is being used. Note that the given IP from Boston is a Public IP range (which is legit) so User2 isn't asked MFA. Correct answer is NO. Check more here https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips

With statement #3, the keyword to pay attention to is "New Device". User1 doesn't sign in from either Device 1 or 2 so User1 will be asked by MFA. Correct answer is Yes

upvoted 3 times

Cyberbug2021 2 months, 2 weeks ago

No, No, Yes

upvoted 1 times

kenchin123 2 months, 2 weeks ago

im not sure if you guys notice but the checkbox for trusted ip is. not check, thats why i feel th answer for Box 2 is yes.

upvoted 8 times

Micronerd 2 months, 2 weeks ago

Answer is correct. Boston IP address space is an internal /24 subnet not the Public IP with which the actual sign in is coming from.

upvoted 1 times

DCarma 3 weeks, 5 days ago

That's not true - it's a legit 'external' IP Address range and belongs to OCN.

upvoted 1 times

MikeB19 2 months, 3 weeks ago

Q2 is interesting. The ip for Boston is excluded but the box is not checked. Therefore the excluded ip does not apply and the answer is yes.
Therefore answer should be n y y

upvoted 4 times

coolfinesse 3 months ago

Answer:
No - Selected 14 days
No - Excluded IP range
Yes - New device

https://t.me/learningnets

upvoted 1 times

BowHound 3 months, 2 weeks ago

Whilst the Boston IP is listed as trusted IP the option is not selected as active. So correct answer is No, Yes, Yes.

upvoted 9 times

rgullini 2 months, 3 weeks ago

Answers are No, No, Yes. The "not-selected" option you mention is a different one for federated IP´s

upvoted 3 times

AcTiVeGrEnAdE 3 months, 3 weeks ago

Correct answers are N, N, Y

upvoted 2 times

testexams 3 months, 4 weeks ago

Correct answers:
1) No - After approving the MFA, it is remembered for 14 days, within the time range given
2) No - Boston IP range is in the "Skip MFA"
3) Yes - New Device

upvoted 5 times

https://t.me/learningnets

Question #34 Topic 1

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.

Correct Answer: *AB*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

Exam_Master_Me Highly Voted 12 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 21 times

tuta Highly Voted 7 months ago

tested - AB

upvoted 12 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 2 times

SandroAndrade 1 month, 3 weeks ago

Correct Answer

upvoted 2 times

teehex 2 months 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 3 times

JohnYinToronto 4 months ago

Answer correct. AB

upvoted 3 times

milind8451 4 months, 2 weeks ago

Right Ans.

upvoted 2 times

ipindado2020 9 months, 1 week ago

ok for AB

upvoted 7 times

https://t.me/learningnets

Question #35 *Topic 1*

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

Correct 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

PDR Highly Voted 1 year, 4 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 13 times

gfhbox0083 Highly Voted 1 year ago
B, for sure.
upvoted 8 times

Deepmindx Most Recent 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 1 times

macco455 3 months, 3 weeks ago
Definitely B, creating a new one will do nothing to the old one.
upvoted 1 times

canonigo 3 months, 3 weeks ago
You can have up to ~2000 SAS, so adding a new one doesn't make any sense to invalidate previous.
Answer is correct.
upvoted 1 times

rgullini 2 months, 3 weeks ago
Yes, but just a maximum of five access policies may be set on a container, table, queue, or share at any given time.

https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy
upvoted 1 times

dadageer 4 months ago
I am not sure why people are saying B, it does not meet requirements! Yes I agree this is not ideal solution BUT it does meets the requirement and will invalidate previous SAS token! They have not asked for an ideal solution, all they are asking is does it meet the requirement and it does.
Answer is A. Ideal solution would be Access Policy off course but that is not the only solution!!
upvoted 2 times

mayenite 5 months ago
In exam
upvoted 4 times

milind8451 5 months, 1 week ago

https://t.me/learningnets

Right ans. Go to Storage account -> "Storage Explorer" -> Select your container and right click on it -> Click on "Get Storage Access Signature", here you get option to select Access policy and you can define timebound access. So given answer and logics are correct.

upvoted 1 times

Jend 5 months, 2 weeks ago

screw this only 30 percent of all these questions were in the exam.

upvoted 1 times

AshTac 5 months, 3 weeks ago

Agreed. I believe this is B. In this article https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview under section "Best practises when using SAS". It says the below: "Stored access policies give you the option to revoke permissions for a service SAS without having to regenerate the storage account keys. Set the expiration on these very far in the future (or infinite) and make sure it's regularly updated to move it farther into the future." - Note the word revoke..

upvoted 2 times

PaulRSE 5 months, 4 weeks ago

I chose answer B, since a store access policy exists to control the SAS. See https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy

upvoted 1 times

B1T3X 6 months, 1 week ago

Answer is no. Generating new SAS will not affect the existing ones.

upvoted 1 times

rflbrbs 6 months, 3 weeks ago

I choose B

upvoted 1 times

celomomo 6 months, 4 weeks ago

To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past.

If a service SAS is not associated with a stored access policy (SAP) you cannot revoke it. You would need to regenerate the access key that was used to create the SAS. You could generate another SAS using the other key and have that in place before regenerating the key.

upvoted 2 times

zhanabaur 5 months, 3 weeks ago

agree, according to the given conditions, we are talking about stored access policy. So, the answer is No.

upvoted 1 times

kdkdk 7 months ago

In the exams

upvoted 1 times

Sjn9 7 months, 2 weeks ago

The answer is B.

upvoted 1 times

jennyka76 8 months ago

Answer - B read the whole article
https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy

Its call study

upvoted 3 times

https://t.me/learningnets

Question #36 Topic 1

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.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

Exam_Master_Me Highly Voted 12 months ago
Correct, https://docs.microsoft.com/nl-nl/azure/security-center/security-center-just-in-time
upvoted 24 times

Pinto Highly Voted 4 months, 1 week ago
C. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc
upvoted 5 times

LazyEngineer Most Recent 10 hours, 49 minutes ago
Correct
upvoted 1 times

zic04 5 months, 3 weeks ago
Agree correct
upvoted 5 times

tuta 7 months ago
correct
upvoted 4 times

https://t.me/learningnets

Question #37 Topic 1

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.	○	○

Correct 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 months ago

Answer is correct : Yes-No-Yes

upvoted 15 times

teehex Most Recent 2 months ago

the only exception here is User2 because it belongs to Group2 which is excluded in the Policy.

Yes - No - Yes

https://t.me/learningnets

upvoted 4 times

Fred64 2 months, 1 week ago

policy applies on group1 except if user also apply to group2

upvoted 1 times

Mular5 3 months, 4 weeks ago

It would be interesting if someone could share the documentation to support option 2. Does exclude take precedence over include?

upvoted 1 times

nihao381 3 months, 4 weeks ago

Exclusion does take precedence over inclusion. Reference here: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups#exclude-users

upvoted 9 times

Pinto 4 months ago

Can someone point to the MS docs that tell if a user is in 2 groups then what happens when you have MFA policy on 1 but not on other?

upvoted 2 times

nihao381 3 months, 4 weeks ago

Exclude users
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.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups

upvoted 5 times

gcpbrig01 4 months ago

Option 2 - can the user skip the MFA registration when it login next time as it is in the "exclude" section ?

upvoted 1 times

xaccan 4 months ago

yes, to exclude take over the include

upvoted 2 times

https://t.me/learningnets

Question #38 *Topic 1*

SIMULATION -

The developers at your company plan to publish an app named App11641655 to Azure.

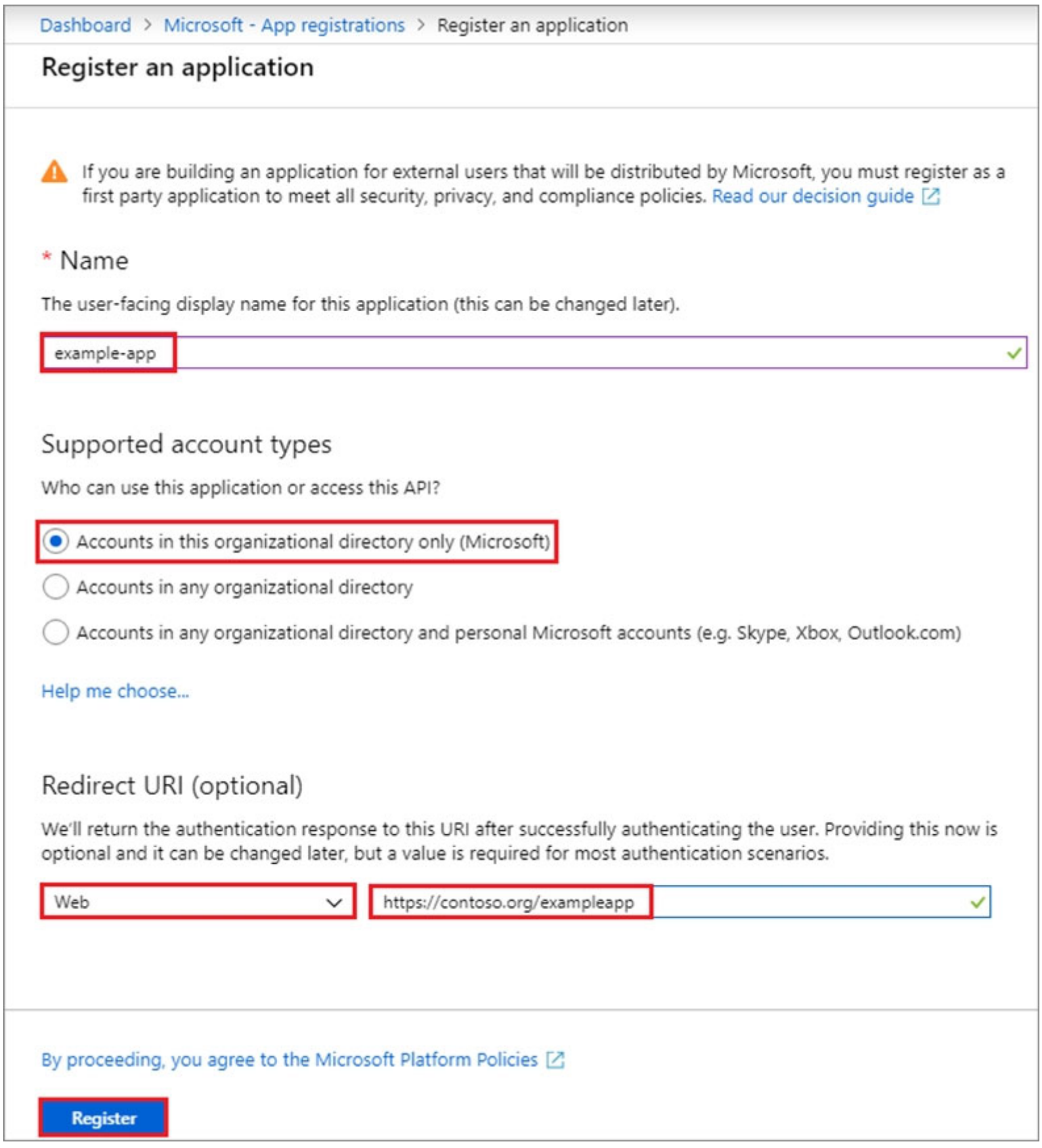
You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of https://app.contoso.com.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Correct 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 App11641655. 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.



6. Click Register

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

avicoder 3 months, 2 weeks ago

Correct

upvoted 4 times

https://t.me/learningnets

Question #39 *Topic 1*

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: ג€Unable to invite user user1@outlook.com Generic authorization exception.ג€
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.

Correct Answer: *D*
You need to allow guest invitations in the External collaboration settings.

Teesmd Highly Voted 10 months, 2 weeks 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 22 times

thomastrain 8 months ago
D is right, but the setting is located in Azure Active Directory -> External Identities -> External collaboration settings.
upvoted 13 times

teehex Most Recent 2 months ago
Set Members can invite = Yes in External Collaboration settings.

D is the correct answer.
upvoted 1 times

milind8451 4 months, 2 weeks ago
Right ans, Go to AAD -> Users -> User Settings -> "Manage External Collaboration Settings", here you need to allow "Guest Invite"
upvoted 4 times

reha 5 months, 3 weeks ago
D is correct!
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/generic-authorization-exception-inviting-azure-ad-gests/m-p/274742
upvoted 3 times

https://t.me/learningnets

Question #40 *Topic 1*

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

Correct 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

jessicamendez10 Highly Voted 3 months, 3 weeks ago

In exam 20/03/2021

upvoted 17 times

Protonenpaule Highly Voted 3 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 6 times

sathas Most Recent 3 weeks, 2 days 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 weeks, 2 days ago

Sorry wrong comment.. Can;t edit here

upvoted 1 times

Samxrg 1 month ago

Ignore previous comment, security group restore not support - azure portal doesn't spell this out!

upvoted 1 times

Samxrg 1 month ago

Why can't Group 1 (Answer A) also be restored

upvoted 1 times

teehex 2 months ago

B and C are correct answers.

You might read it wrong. User1 was deleted on March 25 (you might see May if reading too fast lol) which was 40 days ago. So User1 is not restorable.

User2 was deleted 4 days ago which it is restorable.

upvoted 3 times

hf443 3 months, 2 weeks ago

Correct are answers are BD. User 1 was deleted more than 1 month ago!

upvoted 3 times

souvik123 2 months, 2 weeks ago

I guess you have a typo though explanation is correct. It is BC

upvoted 1 times

https://t.me/learningnets

macco455 3 months, 2 weeks ago

User 2 and Group 2 is the correct answer which is B&C for me.

upvoted 3 times

Zipak 3 months, 2 weeks ago

BD.. User 1 was deleted more than 1 month ago

upvoted 3 times

hf443 3 months, 2 weeks ago

Spot on!

upvoted 1 times

testexams 3 months, 4 weeks ago

Correct answer, was also present on today's exam

upvoted 5 times

dadageer 4 months ago

Correct answer

upvoted 3 times

LJack 4 months ago

Correct answer, 30 days restore for azure ad deleted objects

upvoted 4 times

https://t.me/learningnets

Question #41 Topic 1

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.	○	○

Correct 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

Deepmindx 1 week, 6 days ago

IN THE EXAM 29/6/2021

upvoted 2 times

https://t.me/learningnets

thienvupt 2 weeks ago

Correct!

upvoted 1 times

https://t.me/learningnets

Question #42 *Topic 1*

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

Correct Answer: *BC*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

arunjana Highly Voted 7 months, 1 week ago
Granting tenant-wide admin consent requires you to sign in as Global Administrator, an Application Administrator, or a Cloud Application Administrator.
upvoted 21 times

deegadaze1 Highly Voted 4 months, 2 weeks ago
in exam
upvoted 9 times

trevax Most Recent 1 week, 1 day ago
"A user can also be authorized to grant tenant-wide consent if they are assigned a custom directory role that includes the permission to grant permissions to applications."
From https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent
upvoted 1 times

Dineshvishe 1 week, 2 days ago
Global Administrator,
an Application Administrator, or
a Cloud Application Administrator.
can grant tenant-wide admin consent from App registrations:
upvoted 1 times

kumax 3 weeks, 4 days ago
On exam, May 2021.
upvoted 3 times

mayenite 5 months, 2 weeks ago
Confirmed
upvoted 2 times

cunlu 6 months, 2 weeks ago
o grant tenant-wide admin consent from App registrations:

Sign in to the Azure portal as a Global Administrator, an Application Administrator, or a Cloud Application Administrator.
Select Azure Active Directory then App registrations.
Select the application to which you want to grant tenant-wide admin consent.
Select API permissions and then click Grant admin consent.
Carefully review the permissions the application requires.
If you agree with the permissions the application requires, grant consent.
upvoted 3 times

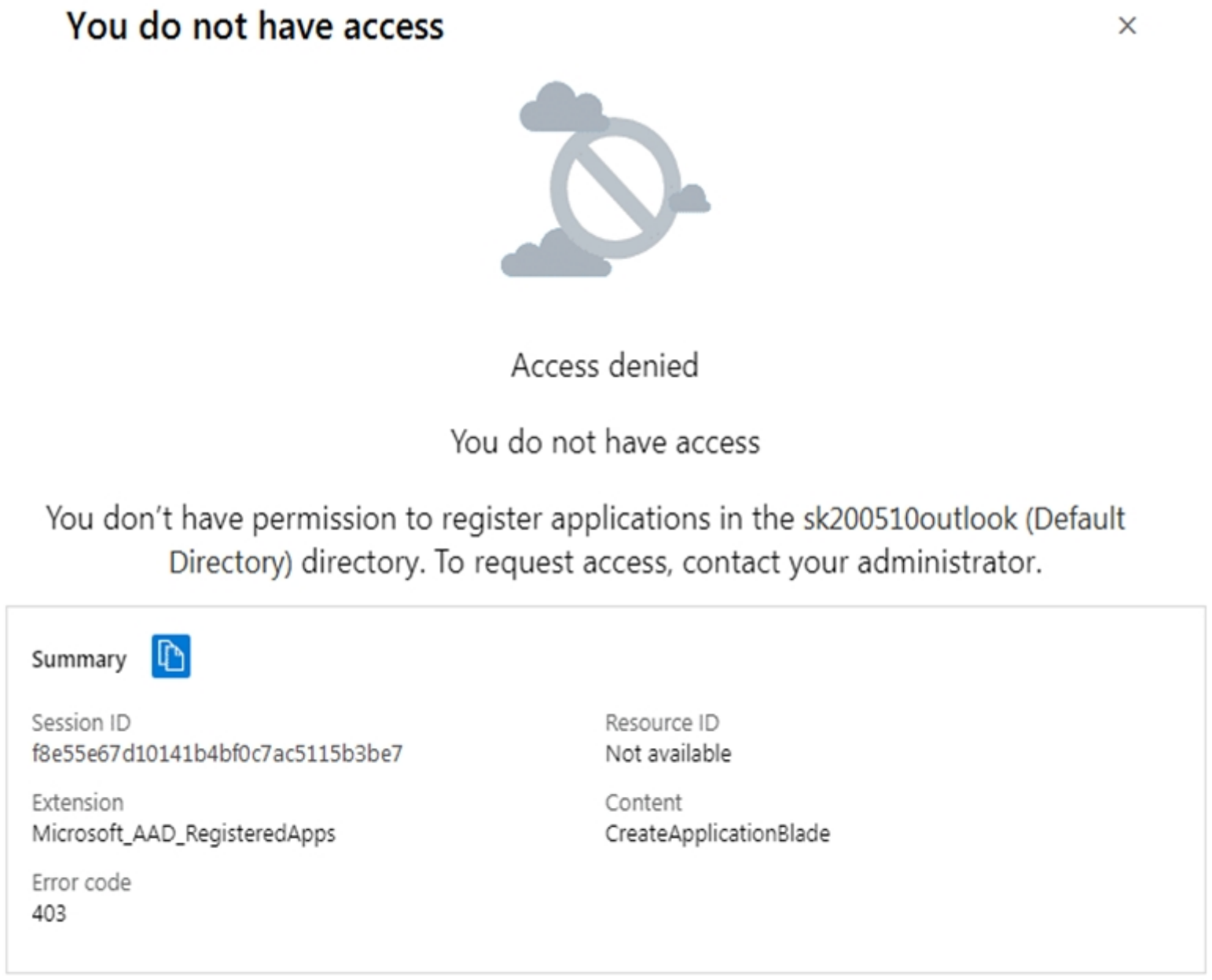
kcinofni 6 months, 3 weeks ago
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#grant-admin-consent-from-the-azure-portal
upvoted 3 times

https://t.me/learningnets

Question #43 Topic 1

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 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.

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

JohnYinToronto Highly Voted 4 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 10 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 3 times

teehex 2 months ago

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles#restrict-who-can-create-applications

upvoted 4 times

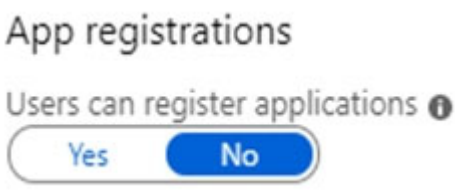
https://t.me/learningnets

https://t.me/learningnets

Question #44 *Topic 1*

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.



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

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

Amin_7 2 weeks, 5 days ago

Application Developer - Create application registration when ability is disabled for all users

upvoted 2 times

SIDNASIR 3 weeks, 3 days 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 3 times

teehex 2 months ago

Cloud Application Administrator has the same permissions as the Application Administrator role, excluding the ability to manage application proxy.

Since the question is asking about least privilege then Application Administrator is the correct answer.

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-application-administrator

upvoted 3 times

bmanu 1 month, 3 weeks ago

Application Administrator is not part or the 4 options. Application Developer meets the principle of least privileges req

upvoted 4 times

Cyberbug2021 2 months, 1 week ago

Answer is correct app dev - Can create application registrations independent of the 'Users can register applications' setting
But Cloud app admin can also do same - Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
Key is - Least privilege

upvoted 4 times

macco455 3 months, 3 weeks ago

Correct

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

upvoted 2 times

JohnYinToronto 4 months ago

Answer correct.
Create application registration when ability is disabled for all users: Application developer

upvoted 1 times

LJack 4 months ago

Correct answer

upvoted 2 times

https://t.me/learningnets

https://t.me/learningnets

Question #45 Topic 1

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

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

gcpbrig01 Highly Voted 4 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 16 times

MarioMK Highly Voted 2 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 5 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 3 times

teehex 2 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 4 times

AMMANANA 2 months, 1 week ago

M2 and VM3 only
because VM5 it's in another VNET -yesssssssssssssss

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

ASG - In Same Vnet

upvoted 2 times

Azuriste 2 months, 3 weeks ago

VM2 VM3 and VM5 .
ASG is applied to VM1 means the ASG will be apply to Nics in the same region as VM1

upvoted 1 times

MedIT 2 months, 2 weeks ago

VM2 and VM3 only
because VM5 it's in another VNET.

upvoted 3 times

Riyasr1 3 months, 1 week ago

It should be VM2 and VM3 as both are in same virtual network

upvoted 3 times

https://t.me/learningnets

macco455 3 months, 3 weeks 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
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups#allow-database-businesslogic

upvoted 3 times

JohnYinToronto 4 months ago

Answer correct.

upvoted 3 times

https://t.me/learningnets

Question #46 *Topic 1*

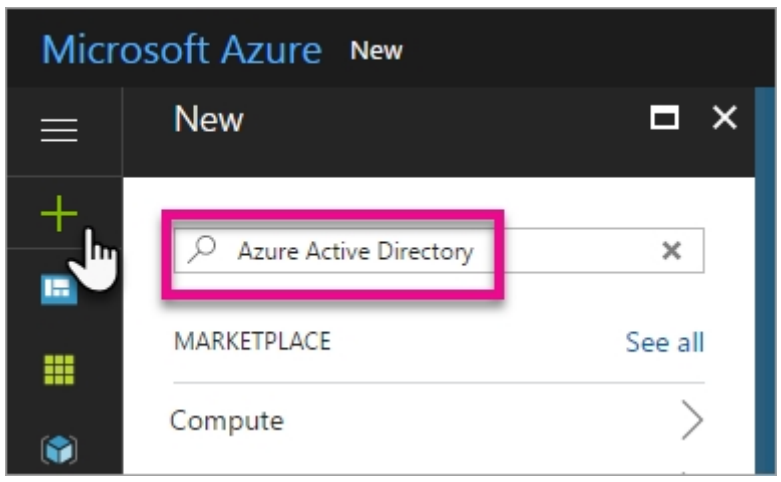
SIMULATION -

You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

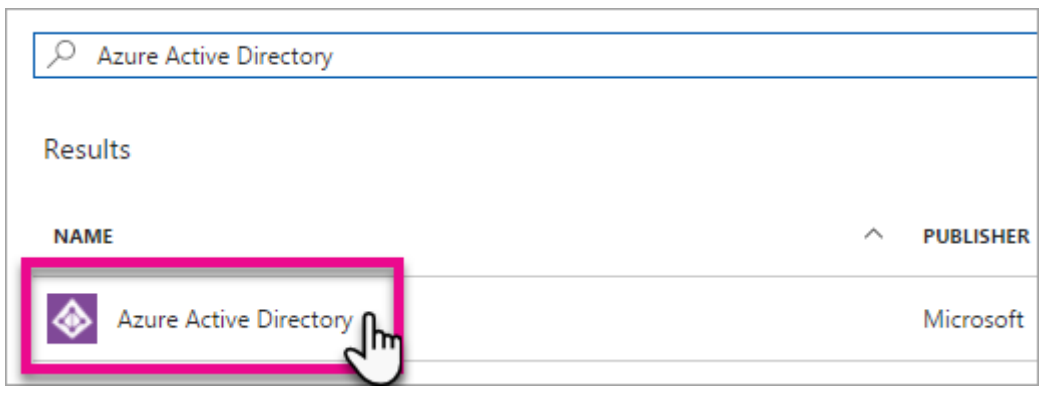
Correct Answer: *See the explanation below.*

To create a new Azure AD tenant:

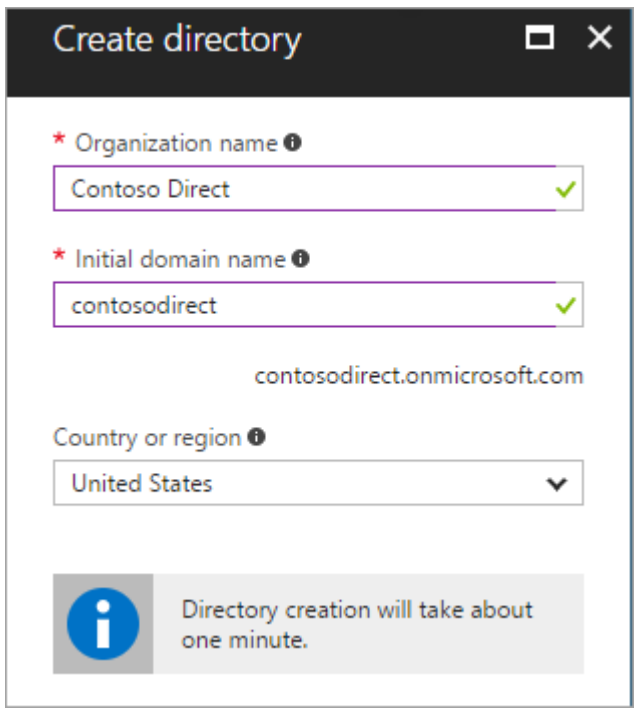
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



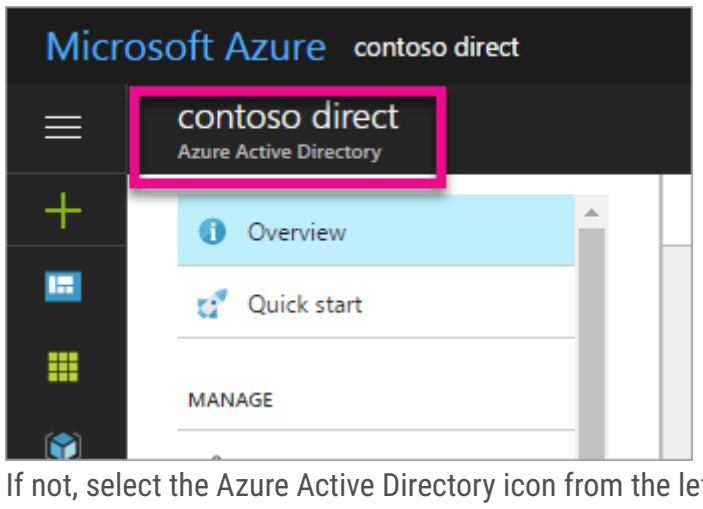
4. Select Create.
5. Provide an Organization name (10317806) and an Initial domain name (10317806). Then select Create. This will create the directory named 10317806.onmicrosoft.com.



6. After directory creation is complete, select the information box to manage your new directory.

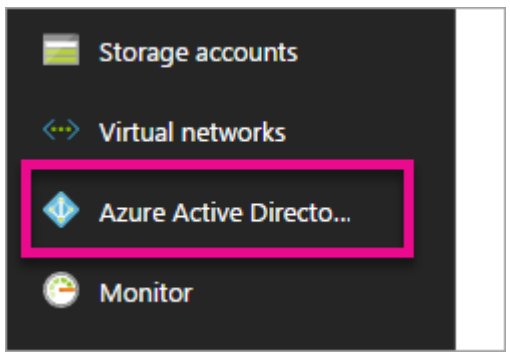
To create the user:

1. In the Azure portal, make sure you are on the Azure Active Directory fly out.

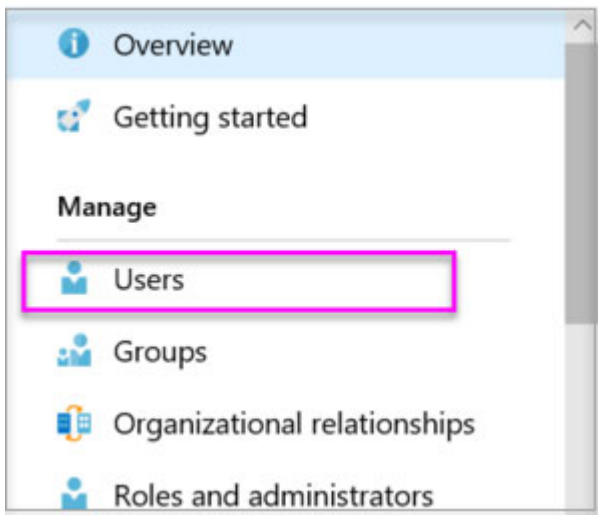


If not, select the Azure Active Directory icon from the left services navigation.

https://t.me/learningnets



2. Under Manage, select Users.

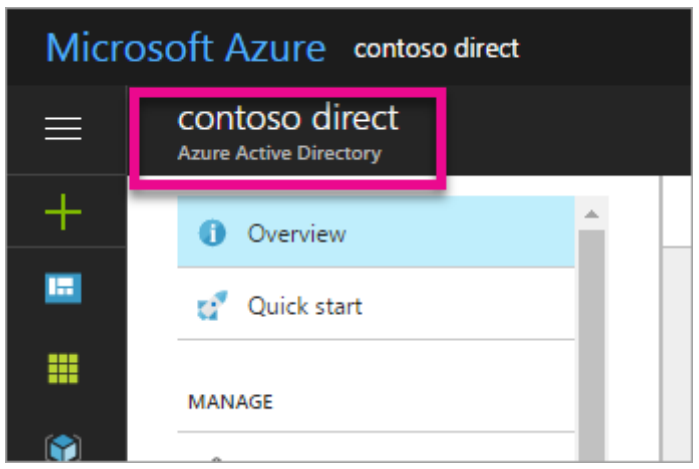


3. Select All users and then select + New user.

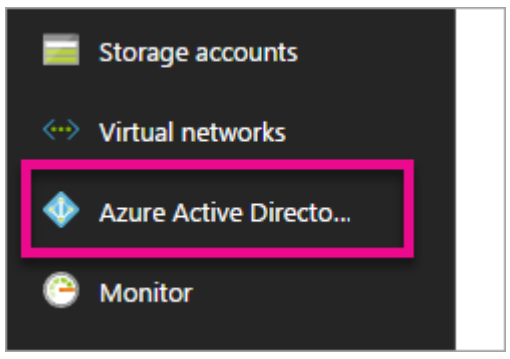
4. Provide a Name and User name (user10317806) for the user. When you're done, select Create.

To enable MFA:

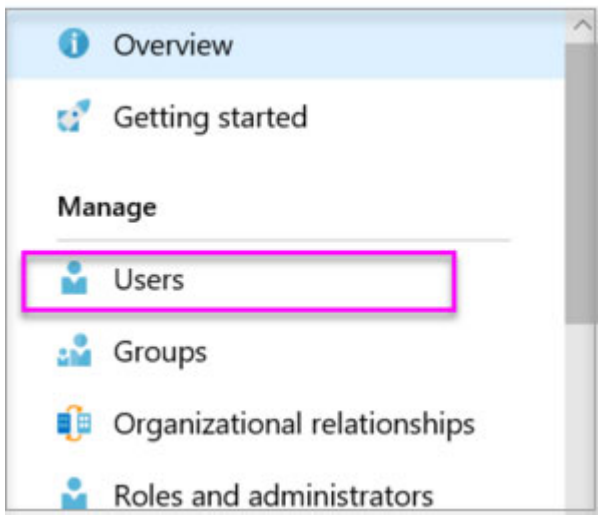
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



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 userג€™s name and click the Enable link.

Reference:

https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

thienvupt 2 weeks ago

Correct Answer, can enable MFA from Users do not use Default Security Setting.

upvoted 1 times

https://t.me/learningnets

Fred64 4 months ago

step 3 or 4 in the answer is not usefull. MFA is activated by default by Default Security Settings

upvoted 2 times

Question #47

Topic 1

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

Correct Answer: *D*

Rahulbard 6 days, 12 hours ago

Answer is D .. once a custom role is assinged to a user, the access can be at any level

upvoted 2 times

mehdimed 1 week, 2 days ago

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles#create-and-assign-a-custom-role-preview
Based on that link I think answer D is correct. When you create a custom role, you can assign it to any "scope" within the organisation - i.e the AD tenant.

upvoted 1 times

thienvupt 2 weeks ago

Correct Answer: A

upvoted 1 times

jpons 2 weeks 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 2 times

Jacquesvz 5 days, 18 hours 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 1 times

https://t.me/learningnets

Question #48 *Topic 1*

You have an Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

Your companyλ€™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

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

arunjana Highly Voted 7 months, 1 week ago

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

upvoted 10 times

milind8451 4 months, 3 weeks ago

This link tells that D is correct.

upvoted 4 times

JhonyTrujillo Highly Voted 3 months, 4 weeks ago

In Exam. D - Correct Answer.

upvoted 7 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 1 times

kumax 3 weeks, 4 days ago

On exam, May 2021.

upvoted 3 times

macco455 3 months, 3 weeks 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 4 months ago

correct

upvoted 2 times

deegadaze1 4 months, 2 weeks ago

in Exam

upvoted 3 times

mayenite 5 months, 2 weeks ago

Correct

upvoted 2 times

chrisp1992 7 months, 1 week ago

D is correct

upvoted 4 times

https://t.me/learningnets

Question #49 *Topic 1*

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

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

deegadaze1 Highly Voted 4 months, 2 weeks ago
It was in Exam
upvoted 15 times

deegadaze1 Highly Voted 5 months ago
Correct
upvoted 11 times

Luketen Most Recent 4 months, 2 weeks ago
Confirm.
upvoted 5 times

https://t.me/learningnets

Question #50 Topic 1

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

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

fabianotrd Highly Voted 4 months ago
Only global admin with MFA enabled can configure PIM
upvoted 19 times

teehex Highly Voted 2 months 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 17 times

M3ridi3n Most Recent 4 days, 18 hours ago
Correct Answer : D
PIM requires Azure AD P2, which must be enabled before you can configure it.
Enabling PIM is done at the subscription level.
upvoted 1 times

Rume 4 weeks, 1 day ago
Only owners of subscriptions and management groups can bring these resources under management by Privileged Identity Management. After it is under management, the PIM functionality is available for owners at all levels including management group, subscription, resource group, and resource

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan
upvoted 2 times

Lb83 2 months, 1 week ago
Technically all 3? "If your goal is to deploy Privileged Identity Management for Azure resources, you should follow our discover Azure resources to manage in Privileged Identity Management article. Only owners of subscriptions and management groups can bring these resources under management by Privileged Identity Management. After it is under management, the PIM functionality is available for owners at all levels including management group, subscription, resource group, and resource. If you're a Global Administrator trying to deploy Privileged Identity Management for your Azure resources, you can elevate access to manage all Azure subscriptions to give yourself access to all Azure resources in the directory for discovery. However, we advise that you get approval from each of your subscription owners before managing their resources with Privileged Identity Management." https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan
upvoted 6 times

Cyberbug2021 2 months, 2 weeks ago

https://t.me/learningnets

"Only owners of subscriptions and management groups can bring these resources under management by Privileged Identity Management"
upvoted 3 times

bmanu 1 month, 3 weeks ago
Answer D, User1 Only
upvoted 1 times

bmanu 1 month, 3 weeks ago
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan
upvoted 1 times

Ppetr0 2 months, 2 weeks ago
But do they ask about that? Question is about enabling PIM, not resource management
upvoted 1 times

cyber2905 3 months, 2 weeks ago
Azure AD roles are all in Azure Active Directory (such as Global Administrator, Exchange Administrator, and Security Administrator). You can read more about the roles and their functionality in Administrator role permissions in Azure Active Directory.

Azure roles are roles that are linked to an Azure resource, resource group, subscription, or management group. You can use PIM to provide just-in-time access to built-in Azure roles like Owner, User Access Administrator, and Contributor, and also to custom roles. For more information about Azure roles, see Azure role-based access control.

I will go with User 1 only, because it is only talking about a subscription here, and only the owner can do that in this context.
upvoted 3 times

sureshatt 3 months, 3 weeks ago
Answer is A.

"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"

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan
upvoted 3 times

macco455 3 months, 3 weeks ago
This question is only asking who can enable PIM not who can discover the resources, and the only person that can consent to PIM is a Global Administrator. Tus my answer is A. User 2&3.
upvoted 6 times

JhnCanthern12 4 months ago
Didn't read the question properly here, jumped to "Global Admin Needed to enable PIM" - its specifically talking about assignments on subscriptions, you need to be an owner to make PIM assignments on subs

Although there is a way to bypass this technically https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin?toc=/azure/active-directory/privileged-identity-management/toc.json
upvoted 2 times

gcpbrig01 4 months ago
Since enabling PIM must be done on subscription level, discovering resources is a prerequisite and user with owner role can only do that. Therefore suggested answer is correct
upvoted 17 times

https://t.me/learningnets

Question #51 *Topic 1*

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 []

Correct Answer: *D*
To λ€˜Read a storage accountλ€™, ie. list the blobs in the storage account, you need an λ€˜Actionλ€™ permission.
To read the data in a storage account, ie. open a blob, you need a λ€˜DataActionλ€™ permission.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

milind8451 Highly Voted 4 months, 2 weeks ago
Right ans, DataAction[] is used at blob level, Action [] is used at container and storage acc level.
upvoted 9 times

mayenite Highly Voted 5 months, 1 week ago
Correct
upvoted 7 times

teehex Most Recent 2 months 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 3 times

Appuni 3 months, 2 weeks ago
correct
upvoted 2 times

https://t.me/learningnets

Question #52 *Topic 1*

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 AD.

D. Upgrade Azure Security Center to the standard tier.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

mayenite Highly Voted 5 months, 1 week ago
Correct
A working Azure AD tenant with at least an Azure AD Premium P2 or trial license enabled.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa
upvoted 11 times

teehex Most Recent 2 months ago
It is mentioned here https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

You need either AAD Premium P2 or Enterprise Mobility + Security (EMS) E5.
upvoted 2 times

Super_Pun 4 months ago
P2 is needed to enable MFA. So, the given answer is correct
upvoted 4 times

dadageer 4 months ago
Correct
upvoted 3 times

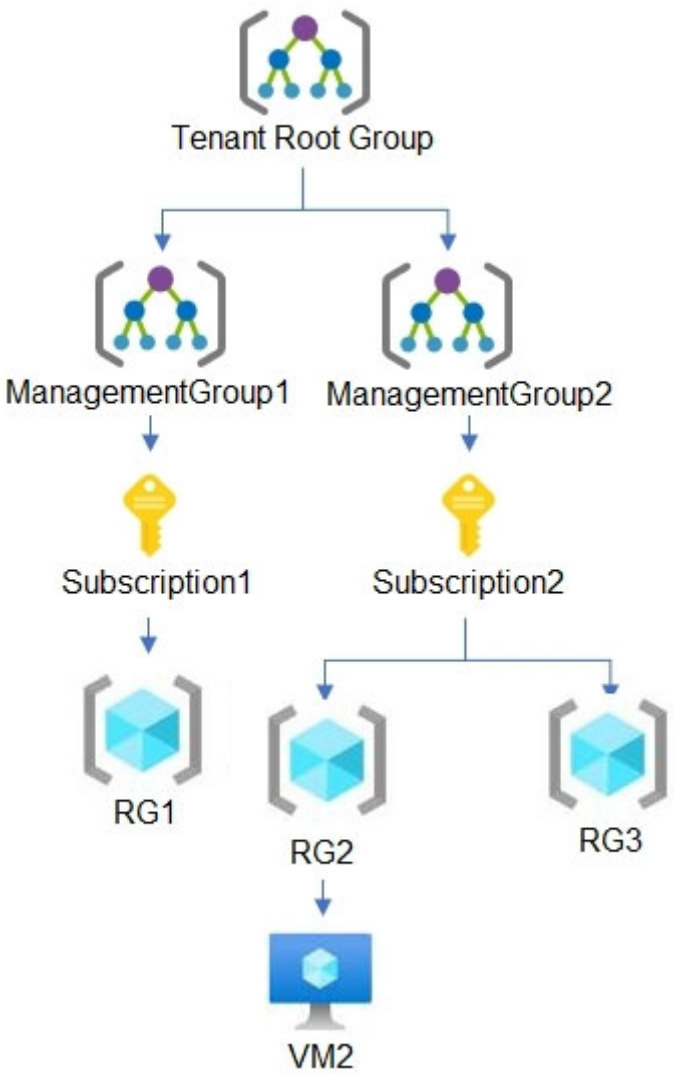
JohnYinToronto 4 months ago
P2 needed
upvoted 2 times

https://t.me/learningnets

Question #53 Topic 1

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 VM1.

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.	○	○

Answer Area

Correct Answer:

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.	○	○

https://t.me/learningnets

Geeky93 Highly Voted 4 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 27 times

Frosticus 2 weeks, 5 days 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 1 times

3abmula 1 month, 2 weeks ago

3). Why No.
If user can login to a VM as an Administrator, then he can reset the built-in Admin password.

upvoted 1 times

eroms 1 month, 3 weeks ago

Microsoft.Compute/virtualMachines/loginAsAdmin/action Log in to a virtual machine with Windows administrator or Linux root user privileges.. so 3). Yes

upvoted 1 times

rgullini 2 months, 3 weeks ago

Agree with you in all three answers after reading the references.

upvoted 2 times

teehex Highly Voted 2 months 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 7 times

MarioMK Most Recent 1 month, 3 weeks ago

All the answers should be set to Yes. If the user is able to login as an administrator to the respective VM, he will have no problem to create and/or modify a user present on that Vm.

upvoted 4 times

souvik123 1 month, 3 weeks ago

Box 3 : Yes. Virtual Machine contributor can reset virtual machine root user password using virtual machine extensions, and manage accounts local users using virtual machine extensions.

upvoted 3 times

Na_v 2 months ago

User 3 can reset the builtin admin password since user3 can login as admin to the VM. the answer is
A
A
A

upvoted 4 times

https://t.me/learningnets

https://t.me/learningnets

Question #54 Topic 1

HOTSPOT -

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

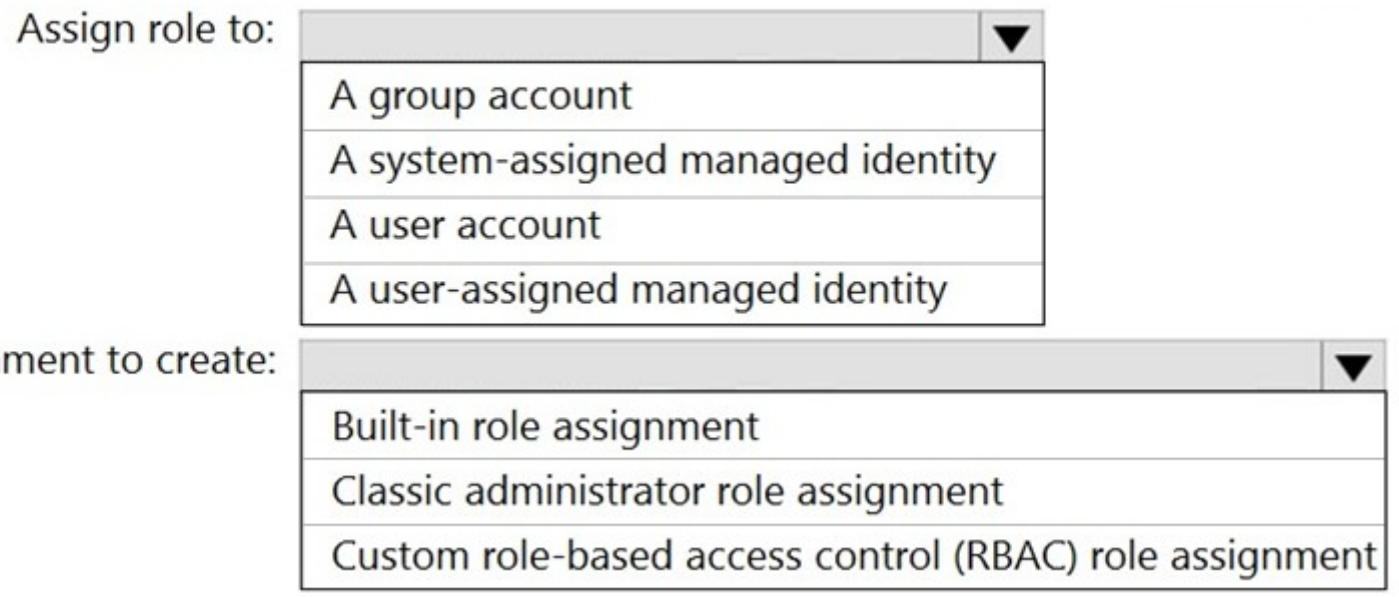
You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

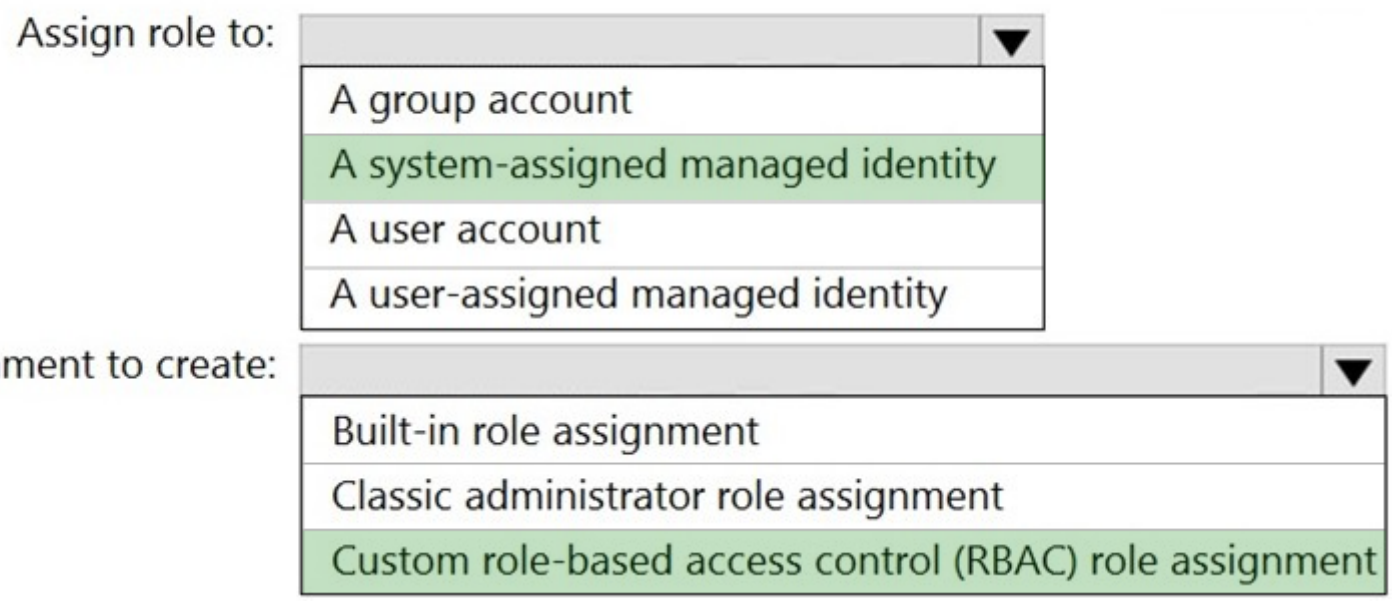
Hot Area:

Answer Area



Correct Answer:

Answer Area



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 2 months, 3 weeks ago

minimize admin effort=> system assign MI
minimum required priviledge => Custom role. All other role have too much priviledges

upvoted 8 times

teehex Most Recent 2 months 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 4 times

Cyberbug2021 2 months, 2 weeks ago

Correct answers

upvoted 2 times

macco455 3 months, 3 weeks 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 3 times

https://t.me/learningnets

macco455 3 months, 2 weeks ago

Also, creating a custom role will be more administrative effort than is needed for this.

upvoted 2 times

A365 3 months, 2 weeks 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 5 times

Fred64 2 months, 3 weeks ago

The scenario is: minimum required priviledge. Where do you take into account this reequirement?

upvoted 1 times

nihao381 3 months, 4 weeks ago

I would like to add that you can assign roles to system-assigned managed identities.
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal-managed-identity

upvoted 1 times

dadageer 4 months ago

Yeah seems right!

upvoted 3 times

Question #55 *Topic 1*

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

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

LJack Highly Voted 4 months ago

Correct answer

upvoted 14 times

lakshmi001s Most Recent 1 month, 2 weeks ago

yes correct

upvoted 1 times

BalderkVeit 1 month, 3 weeks ago

agreee

upvoted 1 times

https://t.me/learningnets

Question #56 Topic 1

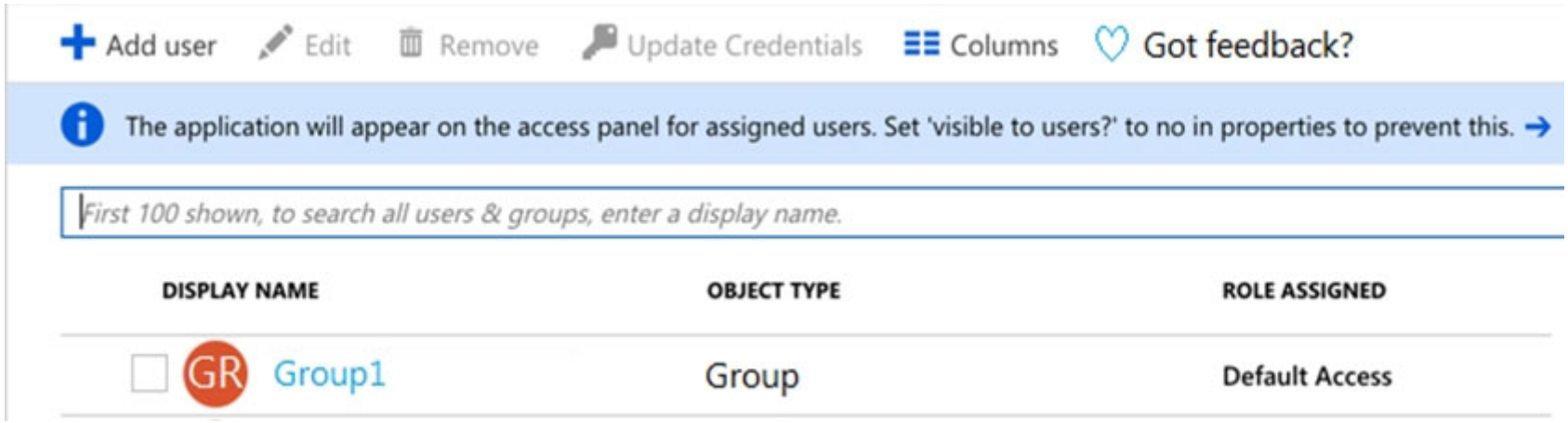
HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.

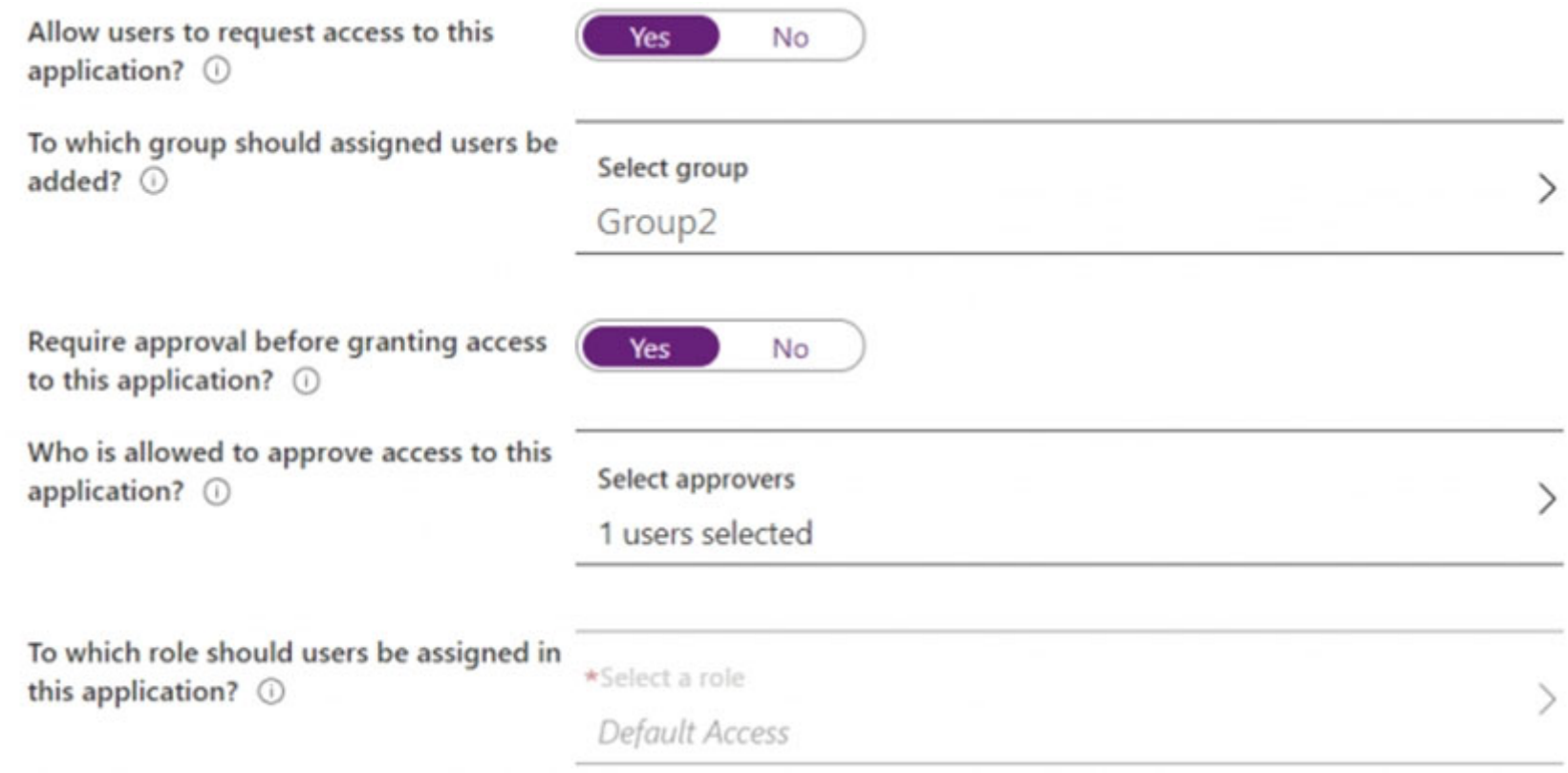
Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.



You enable self-service application access for App1 as shown in the following exhibit.



User3 is configured to approve access to App1.

You need to identify the owners of Group2 and the users of App1.

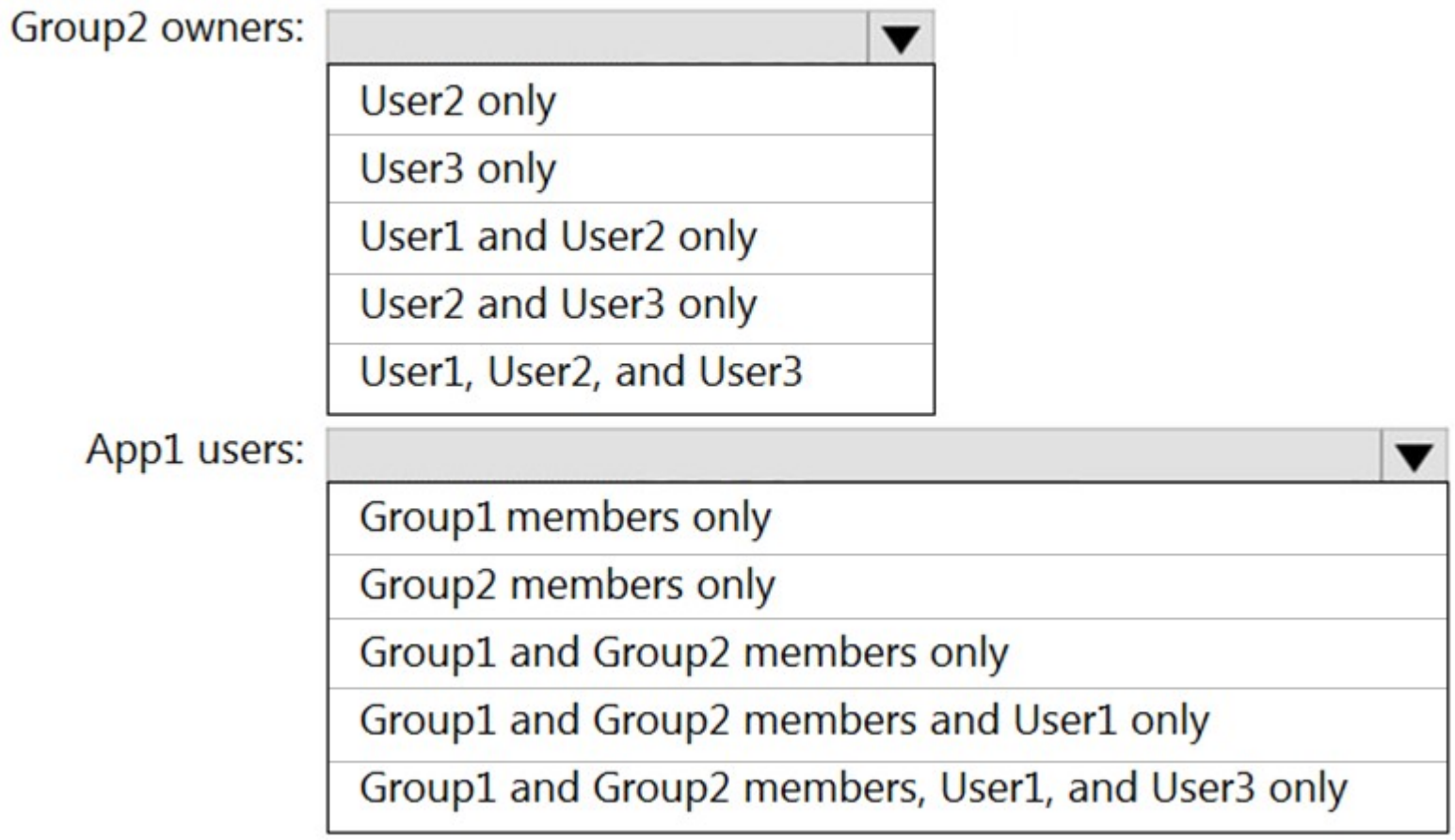
What should you identify? To answer, select the appropriate options in the answer area.

https://t.me/learningnets

NOTE: Each correct selection is worth one point.

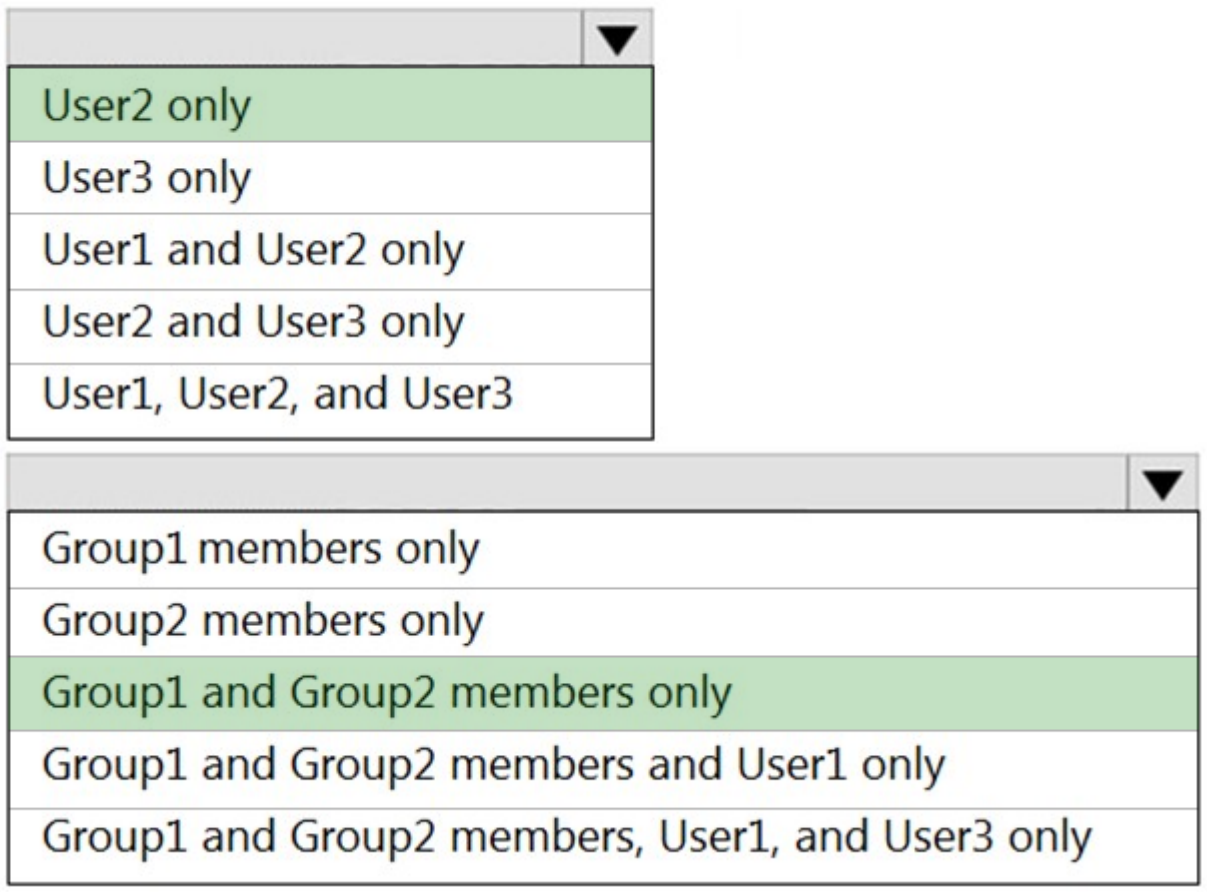
Hot Area:

Answer Area



Answer Area User3 Only

Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

nihao381 Highly Voted 3 months, 4 weeks ago

After testing this out in a lab it show the first answer as incorrect. The answers are Group2 owner is User3 only and both Group1 and Group2 members have access. When you configure self-service and set an approver it resets the list of owners in the target group to the selected approver. Also, when you set a group in self-service it adds that group to the user and groups list.

upvoted 25 times

sakibmas 2 weeks, 2 days ago

Please provide reference. As per https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access, we can set 10 approver. But I have not found any article that mention that set an approver resets the list of owner.

upvoted 1 times

JAGUDERO 2 months, 3 weeks ago

WHY GROUP 1 MEMBERS?

upvoted 1 times

rgullini 2 months, 2 weeks ago

https://t.me/learningnets

Becasue the Group1 is added "manually". Also Group2 members will have access using the self-service setting.
upvoted 1 times

Fred64 2 months, 3 weeks ago
Why? It is said: User2 is the owner of Group2. So answer can't be user3 only
upvoted 2 times

Fred64 2 months, 3 weeks ago
OK I understant, dadageer explain what happen, so box 1 is user3
upvoted 2 times

dadageer Highly Voted 4 months ago
First Answer incorrect. When you assign a user under 'Who is allowed to approve access to this application?' the owner of Group changes to this 'approver'. You even get a warning that Group owner will change. So for the first box it is 'User 3 only'.
upvoted 22 times

Rahulbard Most Recent 5 days, 14 hours ago
User 2 and Group 1 members only. The application setting states that the app will be visible to Group 1 members only. That means the rest will not view this ..

Group owner must not be confused by approver. User 2 is the group owner
upvoted 1 times

Samandre 2 weeks ago
Tested this on portal, assigned owner access for Group2 to user2 and after app settings approver to user3. Under the owner tab user 2 disappeared and user3 is seen. The first answer is user 3 only
upvoted 1 times

fabianotrd 4 months ago
First question nothing to do with app permission. The owner remains "user 2". Second question only group 1 was added on settings. So "user 2" and "Group 1 members only"
upvoted 1 times

rgullini 2 months, 2 weeks ago
Sorry, but this is wrong. The owner of the Group 2 changes to User3 because User3 becomes the approver.
Second question is correct. Members of group 2 because the self-service and members of Group 1 because they are added manually
upvoted 3 times

Pinto 4 months ago
A bit confused. In the exhibit for app permission, Group2 does not show. Only Group1 shows, so only members of Group1 should have access to the app?
Or when the first user is added via the self service mechanism, Group2 automatically gets added to the App1? But, this does not look to be the safe way.
upvoted 2 times

JohnYinToronto 4 months ago
Answers correct
upvoted 2 times

rgullini 2 months, 2 weeks ago
No, answer to question 1 is User3
upvoted 2 times

https://t.me/learningnets

Question #57 *Topic 1*

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.

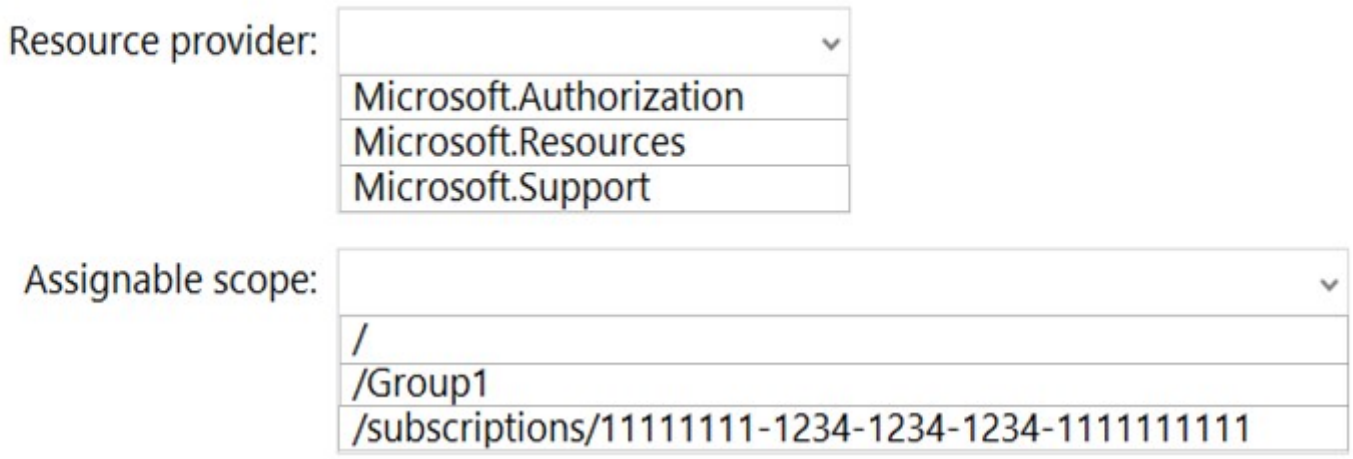
You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.

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.

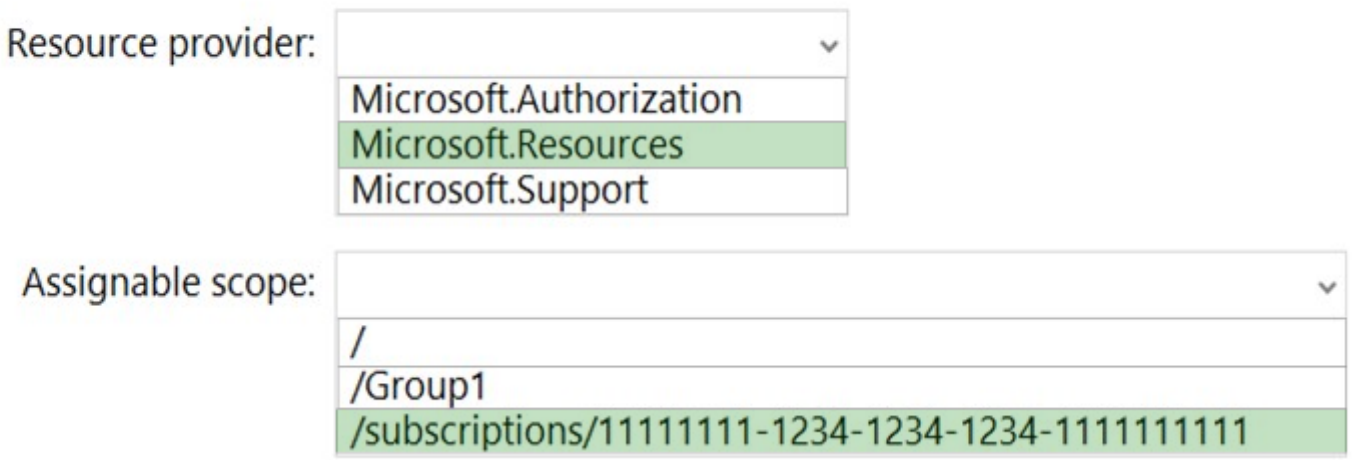
Hot Area:

Answer Area



Correct Answer:

Answer Area



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

thienvupt 2 weeks ago

Correct Answer

Setting assignable scope to root scope ("/") is not supported. Currently, you cannot add a management group as an assignable scope.

upvoted 1 times

https://t.me/learningnets

Question #58 Topic 1

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

Correct 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

stvsting 1 day, 15 hours ago

the answer is correct. test at the lab. you can clone only custome azure ad role or create from scratch.

upvoted 1 times

Topic 2 - Question Set 2

https://t.me/learningnets

Question #1 *Topic 2*

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

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

Sergi0 Highly Voted 11 months, 3 weeks ago
The answer is correct
upvoted 15 times

deegadaze1 Highly Voted 4 months, 2 weeks ago
In Exam
upvoted 6 times

Corpsy Most Recent 1 week ago
In exam 06/07/21
upvoted 1 times

sureshatt 3 months, 3 weeks ago
I could accept the answer, but who needs RBAC for authentication? RBAC is for authorisation. Again, trying to confuse.
upvoted 1 times

Startkabels 3 months, 1 week ago
No that is just you being autistic :D In order to successfully authenticate you need authorization no?
upvoted 1 times

babusartop17 2 weeks, 6 days ago
It's actually the other way around -- first authenticate and then authorize see, this is why you don't get personal...
upvoted 2 times

macco455 3 months, 3 weeks ago
Correct...

https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal#delegate-access-to-other-azure-resources
upvoted 3 times

mayenite 5 months, 2 weeks ago
Correct
upvoted 2 times

tuta 7 months ago
repeated on same page
upvoted 1 times

https://t.me/learningnets

Question #2 *Topic 2*

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

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/automation/update-management/configure-groups

milind8451 Highly Voted 4 months, 3 weeks 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 12 times

dadageer Most Recent 4 months ago
Correct!
upvoted 3 times

https://t.me/learningnets

Question #3 *Topic 2*

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 machine 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

Correct Answer: *C*

References:

https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json

Khumnan Highly Voted 4 months ago

"enable Update Management" is to install agent on the machine. You can install the agent only when the machine is on.

upvoted 12 times

jpons Most Recent 2 weeks ago

Check https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-portal
In the image, the first VM is stopped (deallocated) and still can be selected for enablement
So as far as the VM are in no more then 3 different RG, they can be all enabled

upvoted 2 times

Deepmindx 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 1 times

sureshatt 3 months, 3 weeks 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 3 times

JohnYinToronto 4 months ago

Correct. C
https://docs.microsoft.com/en-us/azure/automation/update-management/overview

upvoted 2 times

dadageer 4 months ago

Correct! Only VMs which are running can have update Management

upvoted 2 times

Pinto 4 months ago

I am not able to find anywhere this condition mentioned, unless the question is more than 2 years old.
This blog does say that there is the functionality available to start VMs before update deployment - https://azure.microsoft.com/en-us/blog/azure-update-management-a-year-of-great-updates/?cdn=disable

upvoted 1 times

jessicamendez10 4 months ago

Is Correct! C

upvoted 4 times

https://t.me/learningnets

Question #4 Topic 2

DRAG DROP -

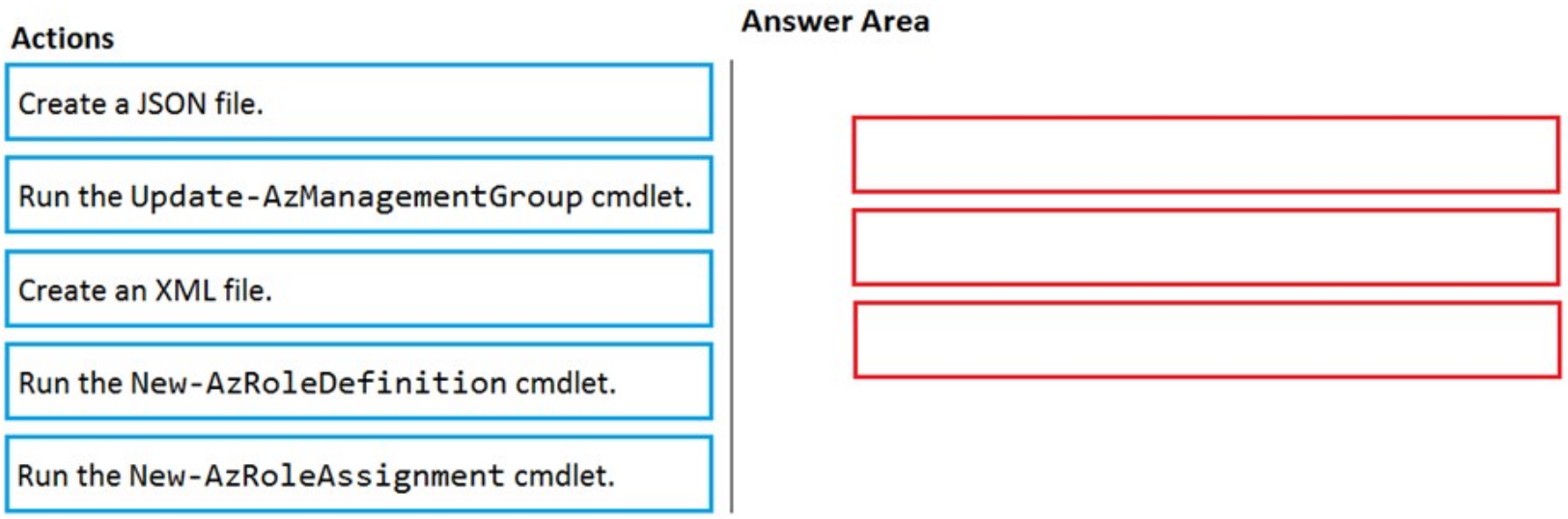
You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

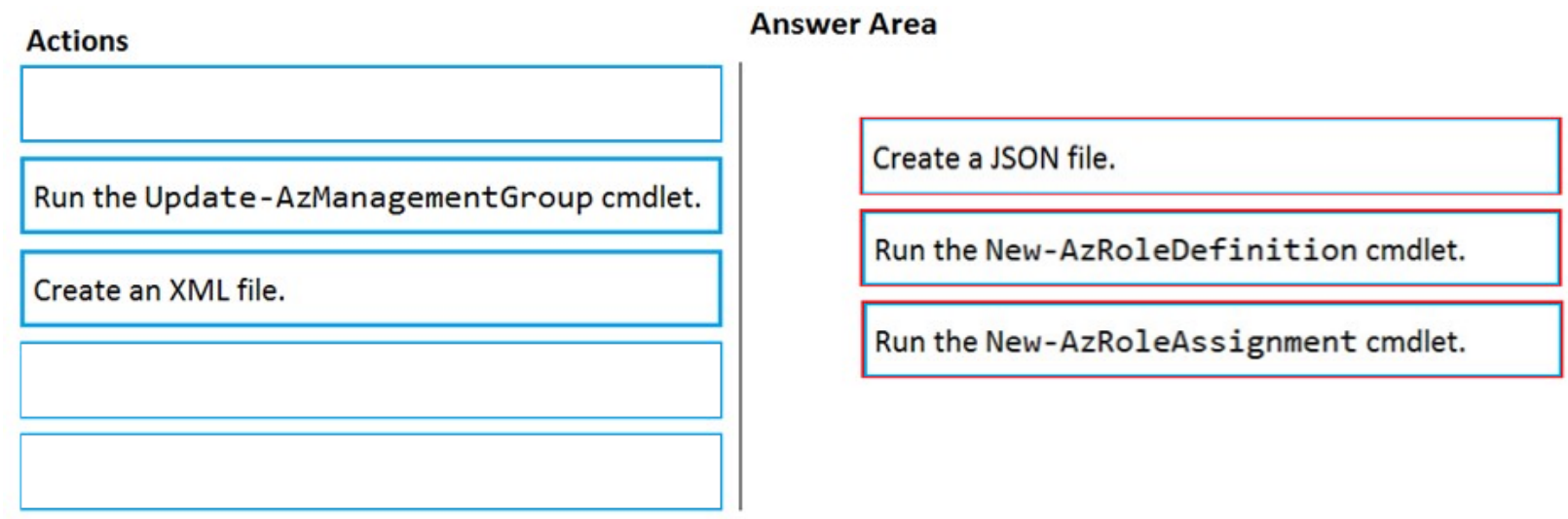
You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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:



Correct Answer:



References:

https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure

LJack Highly Voted 4 months ago

Correct answer

upvoted 11 times

teehex Highly Voted 2 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 7 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 3 times

Fred64 2 months ago

correct answer
we must create a custom role

upvoted 2 times

https://t.me/learningnets

Question #5 *Topic 2*

DRAG DROP -

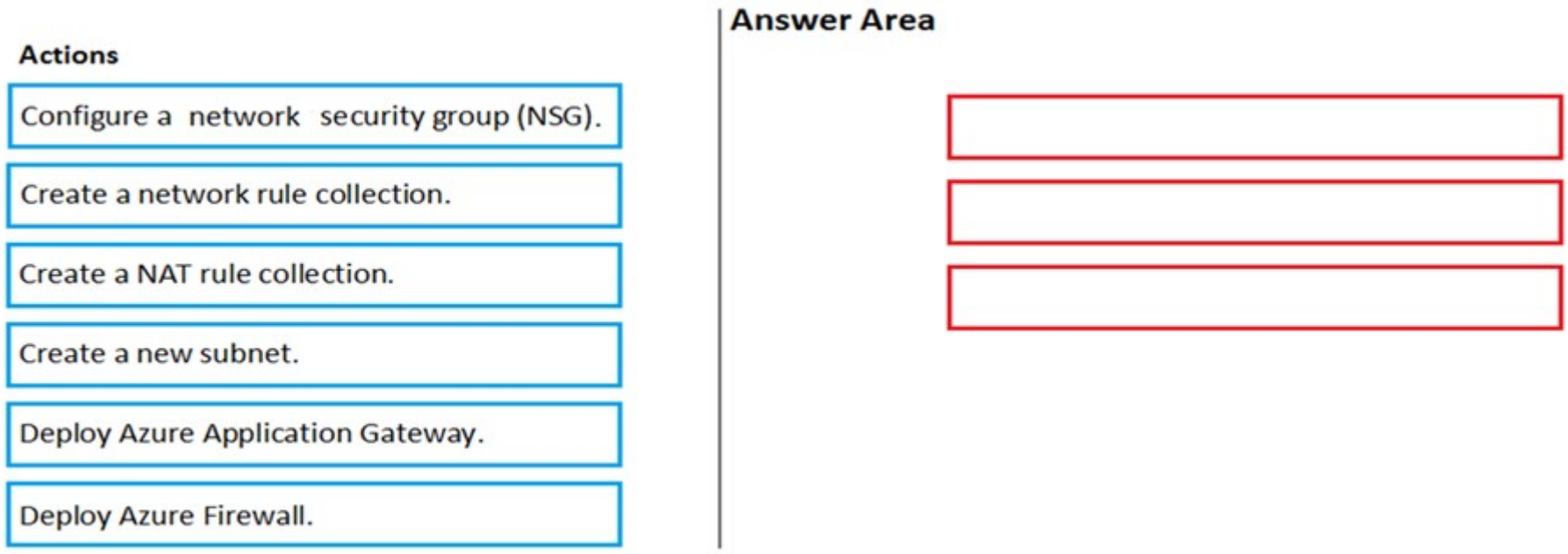
You have an Azure subscription that contains the following resources:

- 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.

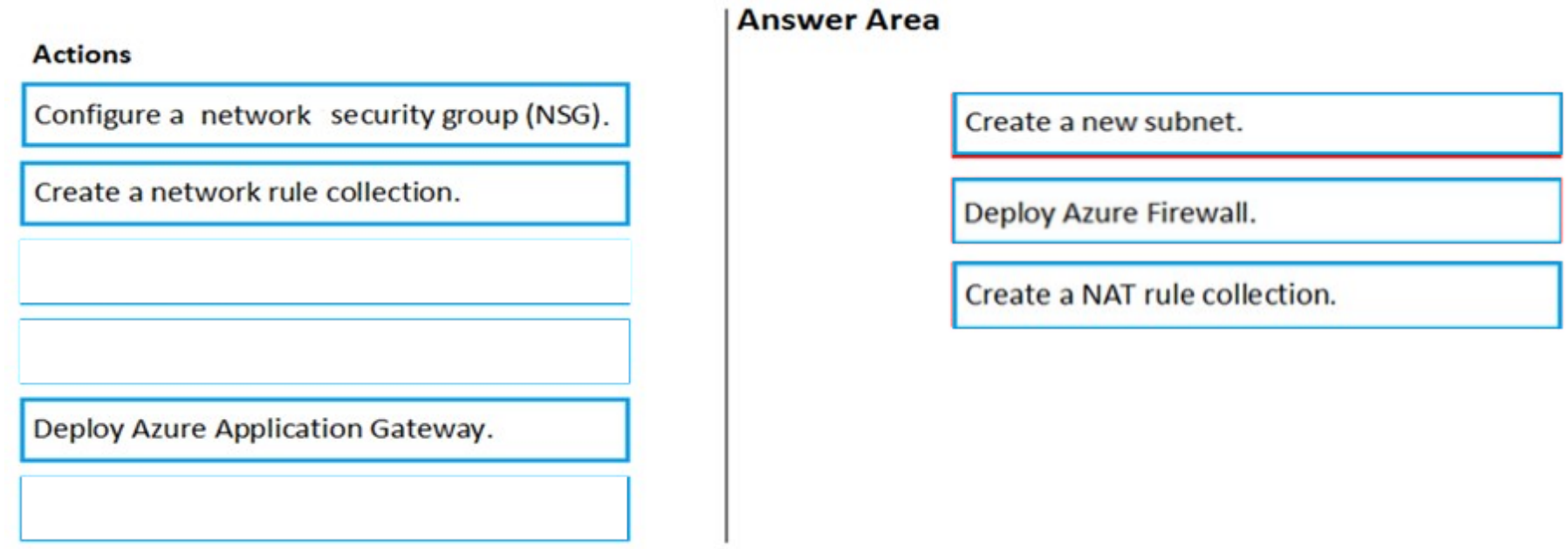
You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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:



Correct Answer:



sukhdeep Highly Voted 3 months, 3 weeks ago

well we can easily connect the VM from internet with Public IP address. Question should need to mention we don't want to use public IP for VM and want to use VM via firewall.

upvoted 6 times

leaderbud 2 months, 2 weeks ago

The thing is that anyway in the list of option you don't have the 'Set VM with a Public IP Address' therefore you need to assume that you only have Private IP enabled - which is by the way better from a Security standpoint not to expose your VM on Internet with an open port. So the idea is to create a new subnet where you can configure the VM to connect outside using Firewall (we are talking here Network level OSI 3 not WAF) and DNAT to have Public IP from FW translated to Private IP address of our backend VM. More info here: https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

upvoted 4 times

Fred64 2 months, 2 weeks ago

"A virtual machine named VM1 that has only a private IP address"

upvoted 2 times

rgullini 2 months, 2 weeks ago

Right. Since the VM has only a private IP, we can´t reach the goal without the proposed solution.

upvoted 1 times

JohnYinToronto Highly Voted 4 months ago

Answers correct.

https://t.me/learningnets

upvoted 5 times

kawsar Most Recent 1 month, 3 weeks ago

No use of subnet 2. Can we deploy Firewall in subnet 2?

upvoted 1 times

3abmula 1 month, 2 weeks ago

To deploy an Azure firewall, subnet name can only be "AzureFirewallSubnet".

upvoted 3 times

teehex 2 months ago

Given answers are correct.
You first need to create a subnet (AzureFirewallSubnet) for Azure Firewall.
Then Create an Azure Firewall
Finally create a NAT rule in order to Nat to internet

upvoted 4 times

Jacquesvz 3 weeks, 1 day ago

100% correct. And best summary and explanation. Thank you teehex

upvoted 1 times

hendry781 3 months, 2 weeks ago

Shouldnt the answer be Create network Collection rules instead of NSG?

upvoted 1 times

Pinto 4 months ago

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat more clarity on this.

upvoted 3 times

dadageer 4 months ago

Correct Answer

upvoted 1 times

gcpbrig01 4 months ago

Correct Answer. The new subnet should be named as AzureFirewallSubnet

upvoted 2 times

Geeky93 4 months ago

why created a new subnet ?

upvoted 1 times

Geeky93 4 months ago

Found the answer in the second message here : https://social.msdn.microsoft.com/Forums/en-US/3cf579e7-7aa0-4c6f-9731-92e0ca73702c/deploy-an-azure-firewall-to-an-already-existing-vnet?forum=WAVirtualMachinesVirtualNetwork

Correct Answer

upvoted 1 times

https://t.me/learningnets

Question #6 *Topic 2*

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

Correct 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

P0d Highly Voted 1 year, 1 month ago
Contributor and AcrPush
upvoted 15 times

rgullini 2 months, 2 weeks ago
Wrong. Correct answer is
AcrPush
AcrImageSigner
upvoted 6 times

temidayo 1 year ago
No, you are wrong,

Correct answer is
AcrPush
AcrImageSigner

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
upvoted 31 times

bluetaurianbull 5 months, 3 weeks 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 "Sign Images" - 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. For details, see Content trust in Azure Container Registry.

But then the confusion is, "Sign Images" seems usually assigned to an automated process, the question talks about assigning 2 roles (Principle of least privilege) to a USER not an automated process. So if it has to be roles assigned to a USER, shouldnt it be AcrPush and Contributor. Ofcource Owner can also push an Image, but it will not follow the Principle of least privilege.
upvoted 1 times

eroms 1 month, 3 weeks ago
its fairly straightforward. No need for any long explanation. Answer is CD. Keyword Least privilege..
upvoted 1 times

gboyega 1 year ago
Correct it should be
ArcPush and AcrImageSigner

Because the question states that we should follow the principle of least priviledge
upvoted 10 times

bluetaurianbull 5 months, 3 weeks 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 "Sign Images" - The ability to sign images, usually assigned to an automated process, which would use a service

https://t.me/learningnets

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 Container Registry.

But then the confusion is, "Sign Images" seems usually assigned to an automated process, the question talks about assigning 2 roles (Principle of least privilege) to a USER not an automated process. So if it has to be roles assigned to a USER, shouldnt it be AcrPush and Contributor. Ofcource Owner can also push an Image, but it will not follow the Principle of least privilege.

upvoted 1 times

gfhbox0083 Highly Voted 1 year ago

C, D, for sure.

upvoted 11 times

FoxDumpz Most Recent 3 weeks, 3 days ago

yes.
AcrPush
AcrImageSigner

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

Contributor is not a Container Role - and The two quarantine role apply to quarantine images only

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

acrimagesigner - Microsoft.ContainerRegistry/registries/sign/write
Push/Pull content trust metadata for a container registry.
Push means write

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

From:https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
" To grant trusted image push permission to a user (or a system using a service principal), grant their Azure Active Directory identities the AcrImageSigner role. This is in addition to the AcrPush (or equivalent) role required for pushing images to the registry."

upvoted 1 times

rgullini 2 months, 2 weeks ago

Correct answer is
AcrPush
AcrImageSigner

upvoted 2 times

aftab7500 2 months, 2 weeks ago

To grant trusted image push permission to a user (or a system using a service principal), grant their Azure Active Directory identities the AcrImageSigner role. This is in addition to the AcrPush (or equivalent) role required for pushing images to the registry. For details, see Azure Container Registry roles and permissions.
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

upvoted 1 times

aftab7500 2 months, 2 weeks ago

To grant trusted image push permission to a user (or a system using a service principal), grant their Azure Active Directory identities the AcrImageSigner role. This is in addition to the AcrPush (or equivalent) role required for pushing images to the registry. For details, see Azure Container Registry roles and permissions.

upvoted 1 times

JAGUDERO 3 months, 2 weeks ago

C y D ars correct
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust#grant-image-signing-permissions

upvoted 1 times

gcpbrig01 4 months ago

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust#grant-image-signing-permissions
C & D is the answer.

upvoted 1 times

fabianotrd 4 months, 2 weeks ago

Answer is correct. It's about content-trust. https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

upvoted 1 times

jbuenoo 10 months, 1 week ago

C and D
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles#sign-images

upvoted 3 times

kratos13 1 year ago

Same as Question7, Topic12

C & D are correct

Here's why ::

https://t.me/learningnets

"Sign images

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. For details, see Content trust in Azure Container Registry."

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

This allows the user to Sign and Push trusted images, using least privilege.

upvoted 4 times

Question #7 *Topic 2*

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
image1	Image was pushed with client content enabled.
image3	Image was pushed with client content disabled.

Which images are trusted images?

A. image1 and image2 only

B. image2 only

C. image1, image2, and image3

Correct 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

Deepmindx 1 week, 6 days ago

IN THE EXAM 29/6/2021

upvoted 1 times

Rume 2 weeks ago

Question is screwed up.... the word "trust" is missing... refer:

https://www.examtopics.com/discussions/microsoft/view/47284-exam-az-500-topic-2-question-7-discussion/

upvoted 2 times

ChinkSantana 1 week, 5 days ago

Why cant it be updated.. Since its same exam vendor

upvoted 2 times

Roger_Smurf 2 weeks ago

The given answer is correct, but the image name should say "image2" in the question, not image1

upvoted 1 times

thienvupt 2 weeks ago

Don't see image2 so answer is incorrect.

upvoted 1 times

https://t.me/learningnets

Question #8 *Topic 2*

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.

Correct 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 11 months, 3 weeks 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 12 times

planb7000 11 months, 2 weeks ago
Perfect! That will surely get you extra points.
upvoted 3 times

Nnanna29 7 months, 3 weeks ago
Definitely! It limits access to only internet instead of 'Any'
upvoted 1 times

am20 Most Recent 2 months ago
why not using bastion?
upvoted 1 times

am20 2 months ago
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview#architecture
upvoted 1 times

ChinkSantana 2 weeks ago
Bsstion is a good way.. But i doubt this is what the question was asking.
upvoted 1 times

Fred64 2 months ago
maybe we can deny all other rules as well?
upvoted 1 times

roy9889 2 months, 1 week ago
I dont understand the meaning of any as a destination, in general. The NSG is assigned to the VM, so the only option should be the localhost/0.0.0.0/ingress .. what other machines could come under ANY ?
upvoted 1 times

https://t.me/learningnets

macco455 3 months, 2 weeks ago

This is created for you when you create the machine in the portal so it is not even necessary anymore. As soon as I create a machine I can RDP to it with no problem

upvoted 1 times

sureshatt 3 months, 3 weeks ago

1. If Azure Defender is available, then use JIT
2. If not, use the Bastian Host.

upvoted 1 times

sukhdeep 3 months, 3 weeks ago

to reduce the attack we can also use Azure firewall with NAT. if public IP get compromised then attacker can only reach firewall not to VM.

upvoted 3 times

sobby 4 months, 2 weeks ago

Source should be slang:Internet

upvoted 2 times

peppycane 5 months, 3 weeks ago

There are steps you have to follow before getting to the pane where you need to input the above stated. The destination address has already been specified. I believe the given answer is correct.

upvoted 1 times

Mahmud1707 8 months, 1 week ago

How about specify the Private IP address of the VM?

upvoted 1 times

Nnanna29 7 months, 3 weeks ago

Working on the NSG of the VM so you do not need to specify the private IP address of the VM

upvoted 1 times

M4gnet1k 12 months ago

It's surprising that they call "reduce the attack surface" to put an ANY rule. Lol!

upvoted 3 times

paulxyz90 6 months, 2 weeks ago

lol ya what's up with that. Destination should be VM1

upvoted 1 times

awssecuritynewbie 9 months, 1 week ago

hahaha so true! haha it would be JIT if it says to allow SSH to a VM for 1 hour ... then it be JIT

upvoted 1 times

rubio83 1 year ago

Should be enable JIT in security center

upvoted 3 times

Nou 11 months, 3 weeks ago

No, its not JIT, this is from the internet you are not requesting access for one user. So need to configure NSG.

upvoted 2 times

xaccan 4 months ago

jit has nothing to do with this question.

upvoted 1 times

https://t.me/learningnets

Question #9 *Topic 2*

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.

Correct 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 10 months, 3 weeks 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 8 times

https://t.me/learningnets

Question #10 *Topic 2*

SIMULATION -

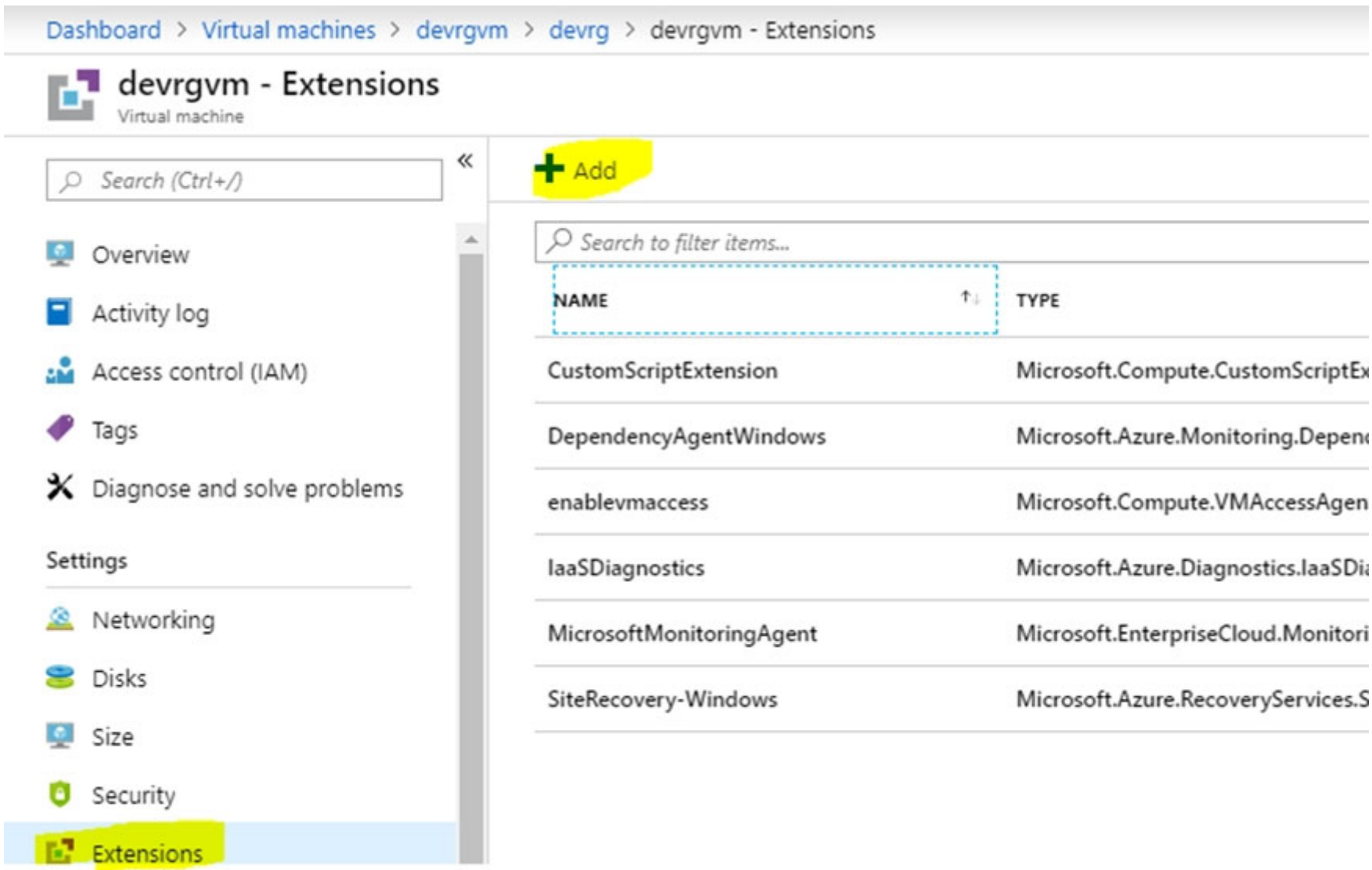
You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

To complete this task, sign in to the Azure portal.

Correct 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 VM1ג€™s blade, navigate to the Extensions section and press Add.



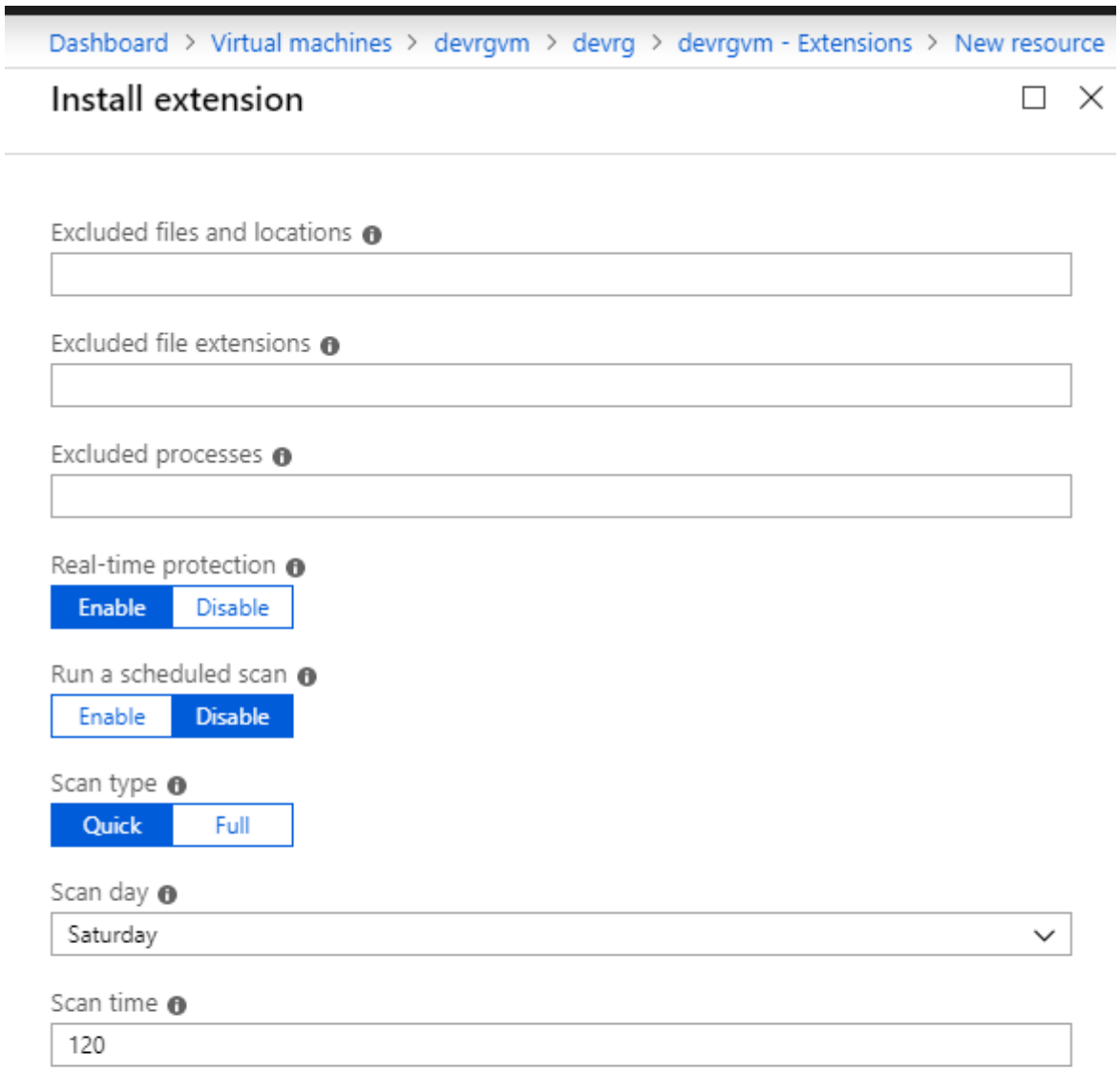
2. Select the Microsoft Antimalware extension and press Create.
3. Fill the ג€Install extensionג€ form as desired and press OK.

Scheduled: Enable -

Scan type: Full -

Scan day: Sunday -

https://t.me/learningnets



Reference:
https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/

awsc 2 months 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 2 times

souvik123 2 months, 2 weeks 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 3 times

ChinkSantana 2 weeks ago
Thanks for the explanation
upvoted 1 times

kimalto452 1 month ago
But why microsoft why ?????
upvoted 1 times

Startkabels 3 months, 1 week ago
What about the time requirement?
upvoted 1 times

https://t.me/learningnets

https://t.me/learningnets

Question #11 *Topic 2*

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.

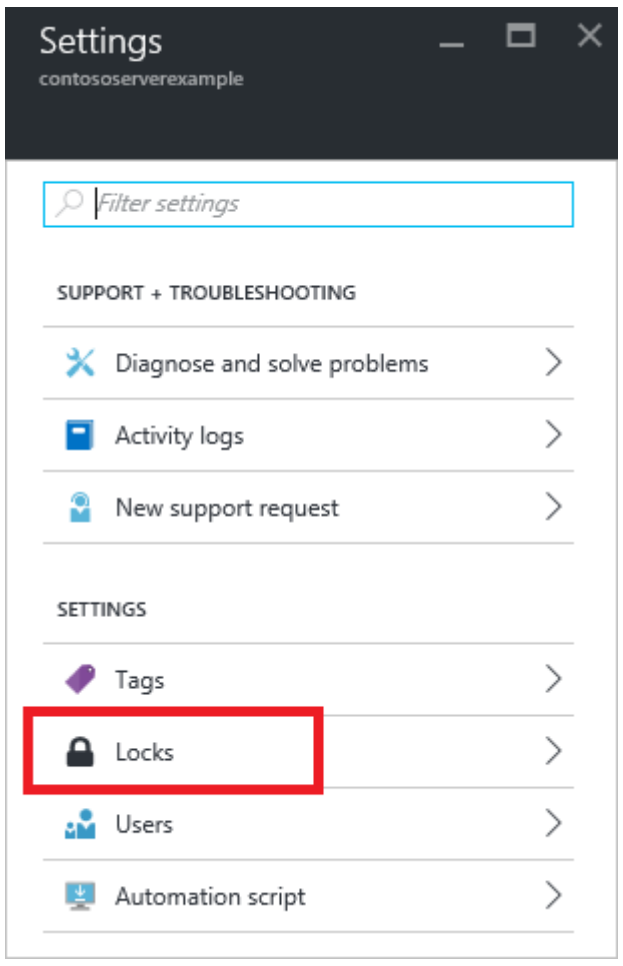
To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

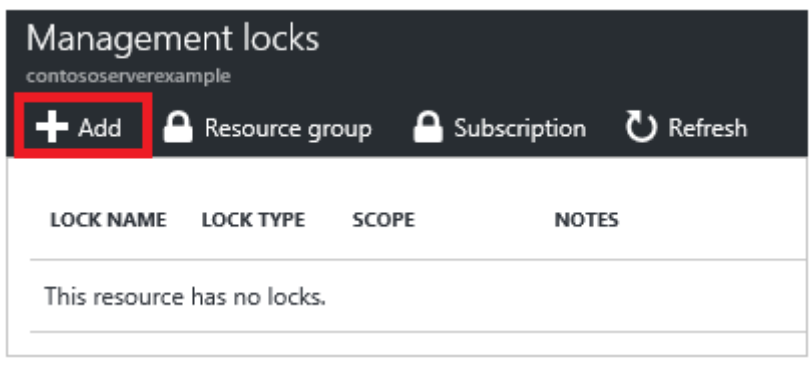
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

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.



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

eroms 1 month, 3 weeks ago

Correct.
Read-only option, as the name implies only allows for read only and not modify.

upvoted 1 times

https://t.me/learningnets

Question #12 *Topic 2*

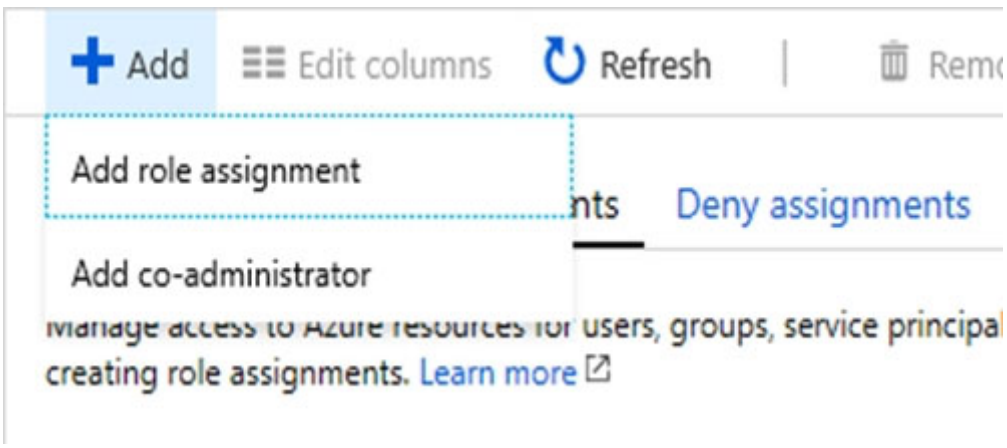
SIMULATION -

You need to grant the required permissions to a user named User211641655 to manage the virtual networks in the RG1lod11641655 resource group. The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

1. In Azure portal, locate and select the RG1lod10598168 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 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 user21059868
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

dadageer Highly Voted 4 months ago

Network Contributor is the answer.
VM Contributor does not have access to VNET

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

upvoted 15 times

ChinkSantana 3 weeks, 1 day ago

I think it does now. The Built-in-Roles no longer has the Network Contributor. Everything is lumped into the VM contributor which can now manage Microsoft.Network

upvoted 1 times

Frosticus 2 weeks, 4 days ago

The new VM contributor role still can't manage virtual networks: https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

upvoted 2 times

ChinkSantana 1 week, 5 days ago

I think i was wrong. There is Network Contributor and Classic Network Contributor

upvoted 1 times

sobby Highly Voted 4 months ago

Role is network contributor

upvoted 6 times

gcpbrig01 4 months ago

yes. virtual machine contributor manages that resource type only

upvoted 1 times

romaso82 Most Recent 2 weeks, 2 days ago

Virtual Machine contributer: Create and manage virtual machines, manage disks and disk snapshots, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions.

upvoted 1 times

3abmula 1 month, 2 weeks ago

https://t.me/learningnets

It's funny that provided answer is "Virtual Machine Contributor", in the same time they mention this in the explanation: "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"

upvoted 1 times

Question #13 *Topic 2*

SIMULATION -

You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod10598168 Azure Storage account.

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

Step 1:

1. In Azure portal go to the storage account you want to secure. Here: rg1lod10598168
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: rg1lod10598168
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

JaggRO Highly Voted 4 months, 2 weeks ago

The description is wrong. The IP range 131.107.0.0/16 isn't allowed on VNET's subnet but it must be set to the Firewall. Go to SA -> Networking -> Firewall & virtual networks -> Firewall section and insert the range into the field Address range and Save.

upvoted 11 times

gcpbrig01 4 months ago

You are right. You can't enter an ip range in the virtual networks section. For that, you need to insert the ip address range in the firewall section.

upvoted 1 times

kimalto452 Most Recent 1 month ago

131.107.0.0/16 subnet... its a subnet range people... read carefully

upvoted 2 times

3abmula 1 month, 2 weeks ago

I'm confused, what exactly is Step1 for?

upvoted 1 times

am20 1 month, 2 weeks ago

I'd go with private link

upvoted 1 times

macco455 3 months, 3 weeks ago

SA-Networking-Firewalls and Virtual Networks- Selected networks and add the virtual network and choose the subnet you want to add. Also should work to just add the IP range under the Firewall section on the same page

upvoted 2 times

Fred64 4 months ago

maybe 131.107.0.0/16 is the subnet IP range. This is unclear

upvoted 3 times

https://t.me/learningnets

Question #14 *Topic 2*

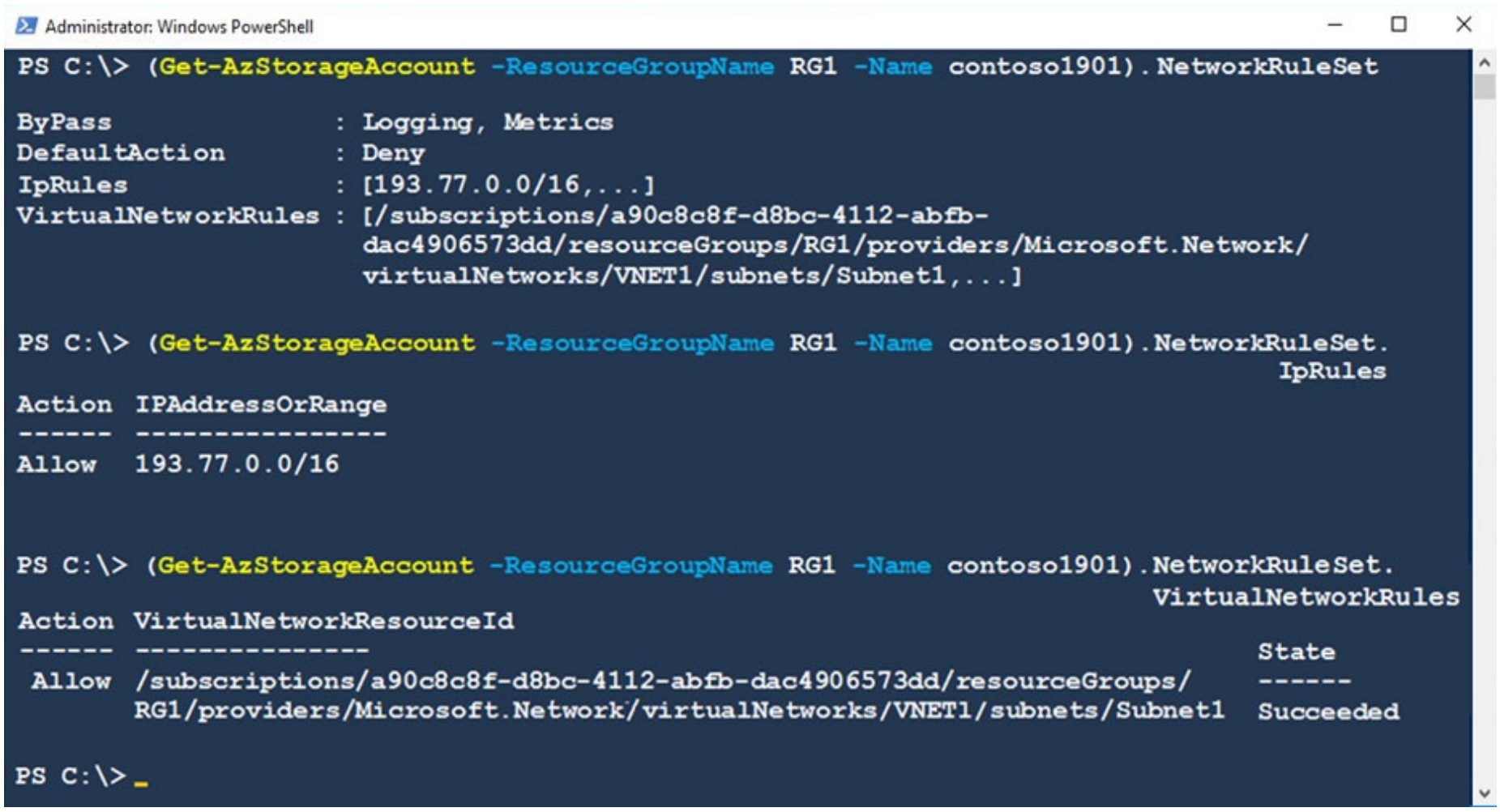
HOTSPOT -

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.)



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.	○	○

https://t.me/learningnets

Correct 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 3 months, 3 weeks ago
answers correct
upvoted 14 times

Triones Most Recent 6 days, 23 hours ago
can someone explain why the first rule deny didn't take effect? is it overwrite?
upvoted 1 times

Jacquesvz 2 days, 17 hours 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 1 times

kubikula 2 months 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 1 times

DCarma 3 weeks, 2 days 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 2 times

Cyberbug2021 2 months, 2 weeks ago
YES - NO - YES
upvoted 3 times

Micronerd 2 months, 2 weeks ago
Address space is /16 therefore 193.77.10.0/24 subnet is allowed. Given answer is correct.
upvoted 2 times

AjitKM 2 months, 2 weeks ago
YES-NO-NO

Given 193.*.*.* IP is not belongs to subnet mask. So when that doesn't belongs to IP then it should be NO
upvoted 1 times

longtech 1 month, 2 weeks ago
The answer is yes bro. Because, the subnet mask is 16 so the network is 192.0.0.0/16 - 192.255.0.0/16 .
upvoted 2 times

rgullini 2 months, 2 weeks ago
It´s Yes, No, Yes. The Ip address range /16 includes the IP address mentioned in the point 3-
upvoted 3 times

dadageer 4 months ago

https://t.me/learningnets

Question #15 *Topic 2*

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

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

Amin_7 2 weeks, 5 days 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. 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. For more information about VNet peering, see About virtual network peering.

https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

upvoted 1 times

bmanu 1 month, 3 weeks ago

Great read https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

upvoted 4 times

glowglow 3 months, 1 week ago

All the virtual networks are peered

upvoted 3 times

JohnYinToronto 3 months, 3 weeks ago

answers correct

upvoted 1 times

dadageer 4 months ago

Correct. If all VNETs are peered then you can access Bastion deployed on the Hub VNET.

upvoted 2 times

gcpbrig01 4 months ago

Suggested answer is correct

upvoted 3 times

https://t.me/learningnets

Question #16 *Topic 2*

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

Correct 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

Thanveer Highly Voted 3 months, 2 weeks ago
Given Answer is correct
upvoted 11 times

rgullini 2 months, 2 weeks ago
Agreed.
upvoted 1 times

teehex Most Recent 2 months ago
B - Azure Automation State Configuration is the only supported way in Azure to meet this requiement.
upvoted 1 times

teehex 2 months 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 1 times

https://t.me/learningnets

Question #17 *Topic 2*

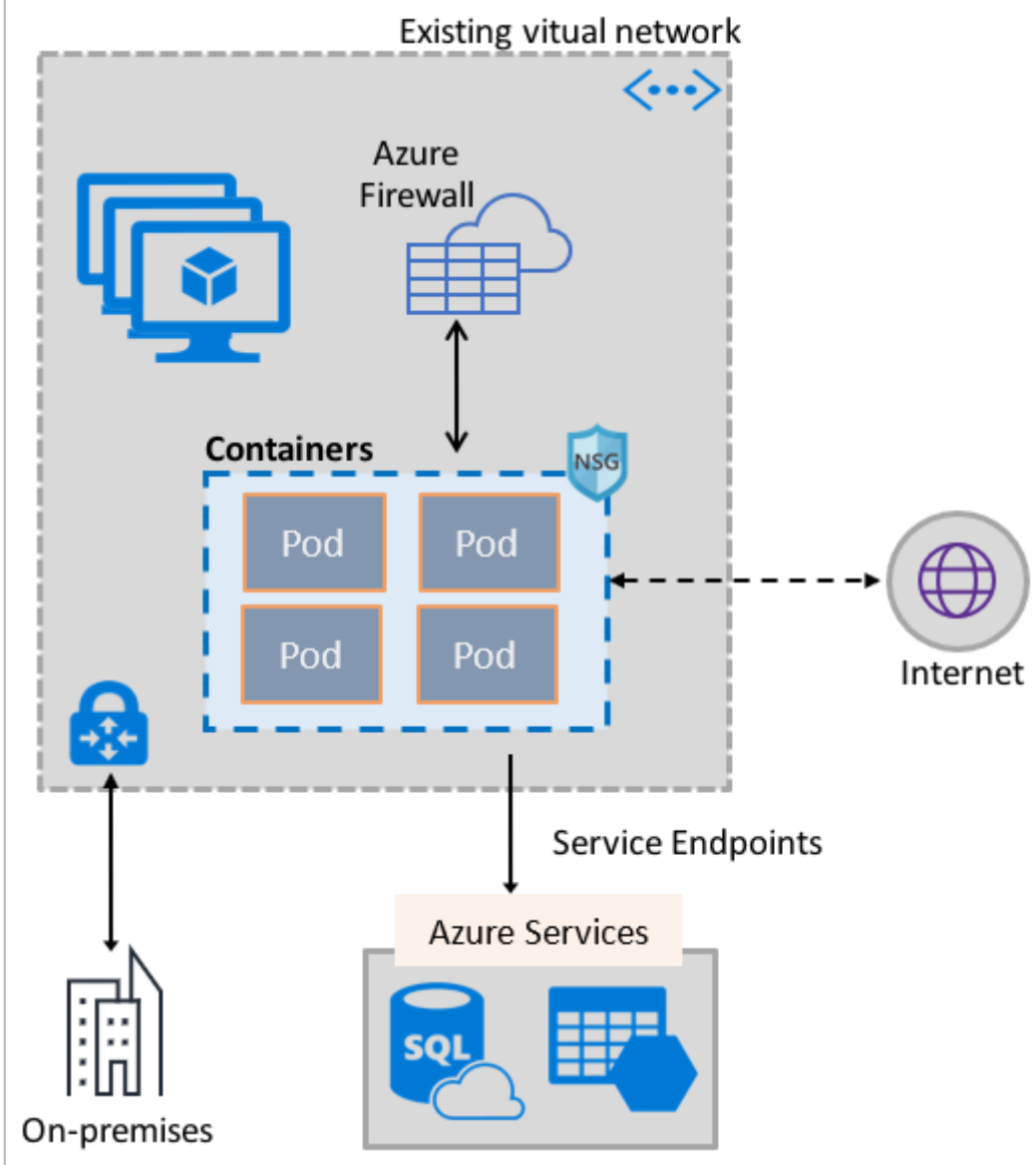
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You create a service endpoint for MicrosoftStorage in Subnet1.
You need to ensure that when 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.

Correct 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 doesnλ€™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

Rave763 Highly Voted 1 year, 2 months ago
C is correct
upvoted 14 times

gfhbox0083 Highly Voted 1 year ago
C, for sure.
Install the container network interface (CNI) plug-in.
upvoted 9 times

Vegazbabz Most Recent 4 months, 2 weeks ago
Had it in an exam this week
upvoted 6 times

https://t.me/learningnets

kdkdk 7 months ago
in the exams
upvoted 2 times

jbuenoo 10 months ago
reference: https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview
upvoted 3 times

DA0410 7 months, 3 weeks 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 2 times

AS007 1 year, 2 months ago
Correct Answer
upvoted 3 times

Question #18

Topic 2

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

Correct 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

Ed2learn 1 month, 3 weeks ago
This is same question as above. The given answer is correct.
upvoted 4 times

https://t.me/learningnets

Question #19 *Topic 2*

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:

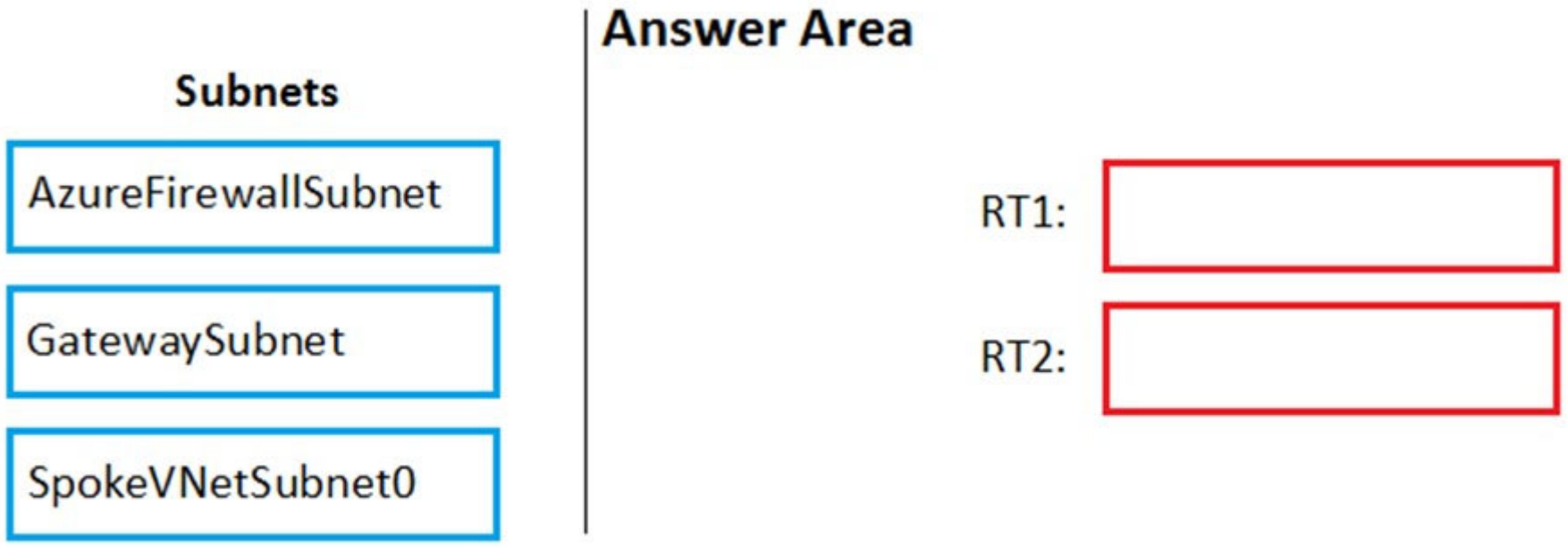
- RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address
- RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

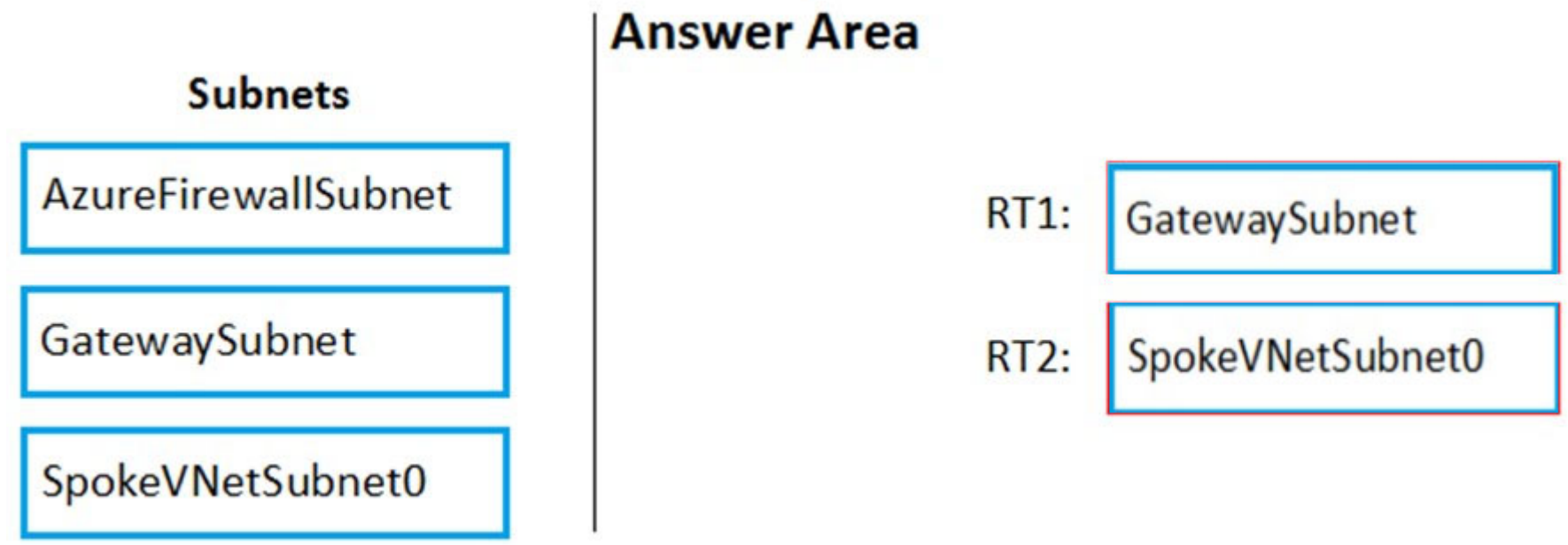
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#create-the-routes

gcpbrig01 Highly Voted 4 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

https://t.me/learningnets

upvoted 9 times

Cisna Highly Voted 2 months, 1 week ago

In exam 02/05/2021

upvoted 8 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 3 times

JohnYinToronto 3 months, 3 weeks ago

answers correct

upvoted 3 times

dadageer 4 months ago

Correct

upvoted 3 times

https://t.me/learningnets

Question #20 *Topic 2*

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" : "                ",
          "details" : {
           "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
           "roleDefinitionsIds" : [
            "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
           ],
           "name" : "customExtension",
           "deployment" : {
                "properties" : {
            "mode": "incremental",
            "parameters" : {
             },
             "                ": {
                }
           }
        }
     }
   }
}
```

Append
Deny
DeployIfNotExists

existenceCondition
resources
template

https://t.me/learningnets

Correct Answer:

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]  ": {
               }
             }
           }
         }
       }
     }
  }
```

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 1 year ago

Answers are correct.
DeployIfNotExist / Template

upvoted 20 times

johnsm Most Recent 1 month, 1 week 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 1 times

teehex 2 months 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 2 times

macco455 3 months, 3 weeks 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 months, 3 weeks ago

answers correct

https://t.me/learningnets

upvoted 2 times

dadageer 4 months, 1 week ago

1. DeployIfNotExists
2. Resources

upvoted 2 times

Pinto 4 months ago

template not resources
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists

upvoted 2 times

ham56141 5 months ago

DeployIfNotExists
resources

upvoted 2 times

Pinto 4 months ago

template not resources
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists

upvoted 2 times

sureshatt 3 months, 3 weeks ago

should be a template "this property should include the full template deployment as it would be passed to the Microsoft.Resources/deployments PUT API"

upvoted 1 times

deegadaze1 6 months ago

Why not Resources instead of Template???
--->"DeployIfNotExists" policy definition executes a {template} deployment when the condition is met!!

upvoted 3 times

gboyega 1 year ago

Correct

upvoted 3 times

deegadaze1 6 months ago

Why not Resources?
Why the template was the correct answer?

upvoted 1 times

lnn_az 1 year, 1 month ago

Correct Answer. Refer https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists-example

upvoted 4 times

dumpmaster 1 year, 3 months ago

There is a default Azure police for that:
"Deploy default Microsoft IaaSAntimalware extension for Windows Server"

upvoted 3 times

Beitran 4 months, 2 weeks ago

Thank you!

upvoted 1 times

Sizz 1 year, 2 months ago

Sources:

https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#compute

https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Compute/VMAntimalwareExtension_Deploy.json

upvoted 1 times

barchetta 1 year, 5 months ago

If I am not mistaken this policy is not completed? "template" is simply the last command in the script and it has not been identified but will need to be? Im so going to get this one wrong if it isnt identical.

upvoted 1 times

https://t.me/learningnets

Question #21 *Topic 2*

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

Correct 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

DeepMoon Highly Voted 9 months, 1 week 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 36 times

kiketxu 7 months, 3 weeks ago
Perfectly explained. Thanks!
upvoted 5 times

gfhbox0083 Highly Voted 1 year ago
B for sure.
(Azure AD) role assignment
upvoted 25 times

amanp Most Recent 5 months, 2 weeks ago
Given Answer is correct.
Service principal must be assigned atleast Reader role to the ACR for deploying to ACI or AKS
upvoted 1 times

DeepMoon 9 months, 1 week 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 8 times

shaheer1991 1 year, 1 month ago
the given answer is the most reasonable between the choices.
upvoted 3 times

barchetta 1 year, 5 months ago
Im not sure this is right. When you auto create a service principle it defaults the role to contributor. Before running the script, update the ACR_NAME variable with the name of your container registry. The SERVICE_PRINCIPAL_NAME value must be unique within your Azure Active Directory tenant. If you receive an "'http://acr-service-principal' already exists." error, specify a different name for the service principal.

You can optionally modify the --role value in the az ad sp create-for-rbac command if you want to grant different permissions. For a complete list of roles, see ACR roles and permissions.
upvoted 1 times

PDR 1 year, 4 months ago
but would that service principal contributor role be only assigned to the cluster and not to the registry, therefore you need to assign it to the registry itself?
upvoted 1 times

https://t.me/learningnets

Question #22 *Topic 2*

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

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

gcpbrig01 Highly Voted 4 months ago

correct answer. intunes enrollment works with windows 10 version 1809 or later

upvoted 15 times

Kumar1983 Highly Voted 2 months, 2 weeks ago

Correct. Verified on link on 4/26/21.

upvoted 5 times

Amin_7 Most Recent 2 weeks, 5 days 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 1 month ago

servers are not mobile devices

upvoted 2 times

Rajesh123 1 month, 1 week ago

MDM is user Devices with Window 10 OS

upvoted 2 times

https://t.me/learningnets

Question #23 *Topic 2*

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.

Correct 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.

JAGUDERO 3 months, 1 week ago
something is missing, This does not restrict the currently deployed resources
upvoted 1 times

Ed2learn 1 month, 3 weeks 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 1 times

eroms 1 month, 3 weeks ago
Maybe restrict destination field to the Subnet of the connected Vnet1.
upvoted 1 times

CarlosBarrero 5 months, 1 week ago
the answer is correct
upvoted 4 times

https://t.me/learningnets

Question #24 *Topic 2*

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.

Correct Answer: *See the explanation below.*

You need to configure a λ€˜lockλ€™ 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 doesnλ€™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 1 month, 3 weeks ago

This is correct.

upvoted 1 times

https://t.me/learningnets

Question #25 *Topic 2*

SIMULATION -
You need to ensure that a user named Danny11597200 can sign in to any SQL database on a Microsoft SQL server named web11597200 by using SQL Server
Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.
To complete this task, sign in to the Azure portal.

Correct 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 web11597200.
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 Danny11597200.
5. Click the Select button to add Danny11597200.
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

saszowy 2 months, 1 week ago
solution is correct - you have to do this in AZURE PORTAL not in SSMS
the other way is to use Query editor which is in preview and you wolud need to know admin password. so...
upvoted 1 times

dadageer 4 months ago
The solution is correct! If you create Danny11597200 as a contained user then user can only login to that DB using SSMS! The requirements are that Danny11597200 can login to any DB under that SQL Server so you must set Danny11597200 as Active Directory Admin so he can login on current DB or any DB further created under this Server.
upvoted 2 times

sureshatt 4 months, 1 week ago
Wrong solution. This makes Danny11597200 an Admin which is too much privileges, he just need to be able to login, for this he needs to be a contained user: use
CREATE USER <Azure_AD_principal_name> FROM EXTERNAL PROVIDER;
upvoted 2 times

gcpbrig01 4 months ago
thanks for explaining this
upvoted 1 times

Pinto 4 months, 1 week ago
Q says user should be able to sign in on any DB on the DB server. Isn't contained user just for a DB and the account would need to be set on every DB on that server?
upvoted 4 times

gcpbrig01 4 months ago
Contained user is set on master DB which then allows that user to go ahead and create the Danny11597200 user using the command CREATE USER <Azure_AD_principal_name> FROM EXTERNAL PROVIDER;
upvoted 1 times

gcpbrig01 4 months ago
The newly created user can login via Sql Management Studio
upvoted 1 times

https://t.me/learningnets

Question #26 *Topic 2*

SIMULATION -
You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.
To complete this task, sign in to the Azure portal.

Correct 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 web11597200. 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 doesnλ€™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.

am20 2 months ago
I'd use private endpoint instead
upvoted 2 times

sureshatt 3 months, 2 weeks ago
why do we need the last step?
"8. Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On." ??
upvoted 1 times

sureshatt 3 months, 2 weeks ago
This is dangerous and too open. I think the last step SHOULD NOT BE done.

"This option configures the firewall to allow all connections from Azure, including connections from the subscriptions of other customers. If you select this option, make sure that your login and user permissions limit access to authorized users only."

https://docs.microsoft.com/en-us/azure/azure-sql/database/firewall-configure#connections-from-inside-azure
upvoted 1 times

LJack 4 months ago
This is correct, I do it quite often in Prod env. Adding service endpoint to firewall, communication then occurs over Microsoft's backbone.
upvoted 1 times

Pinto 4 months, 1 week ago
Haven't tested in lab but looks correct as per https://azure.microsoft.com/en-au/blog/vnet-service-endpoints-for-azure-sql-database-now-generally-available/?cdn=disable
upvoted 2 times

https://t.me/learningnets

Question #27 *Topic 2*

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

Correct 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

LJack Highly Voted 4 months ago
Correct answer
upvoted 7 times

Ed2learn Most Recent 1 month, 3 weeks ago
third time this question has appeared in this question set but the answer is still correct.
upvoted 1 times

https://t.me/learningnets

Question #28 *Topic 2*

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

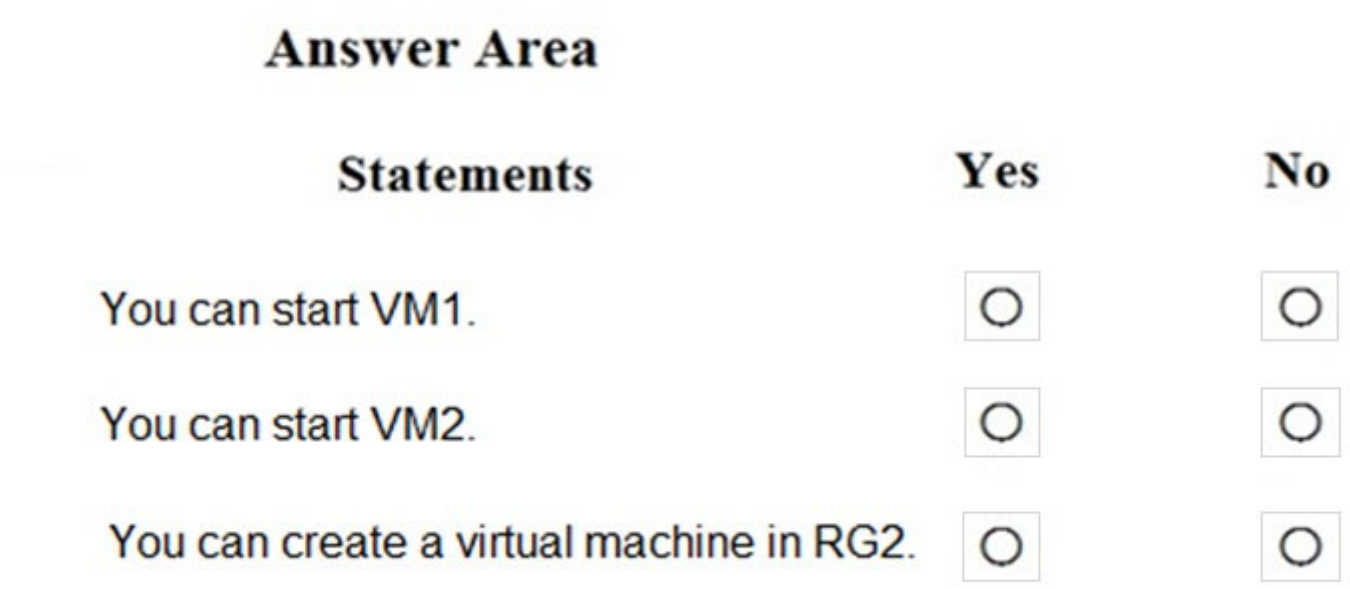
You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

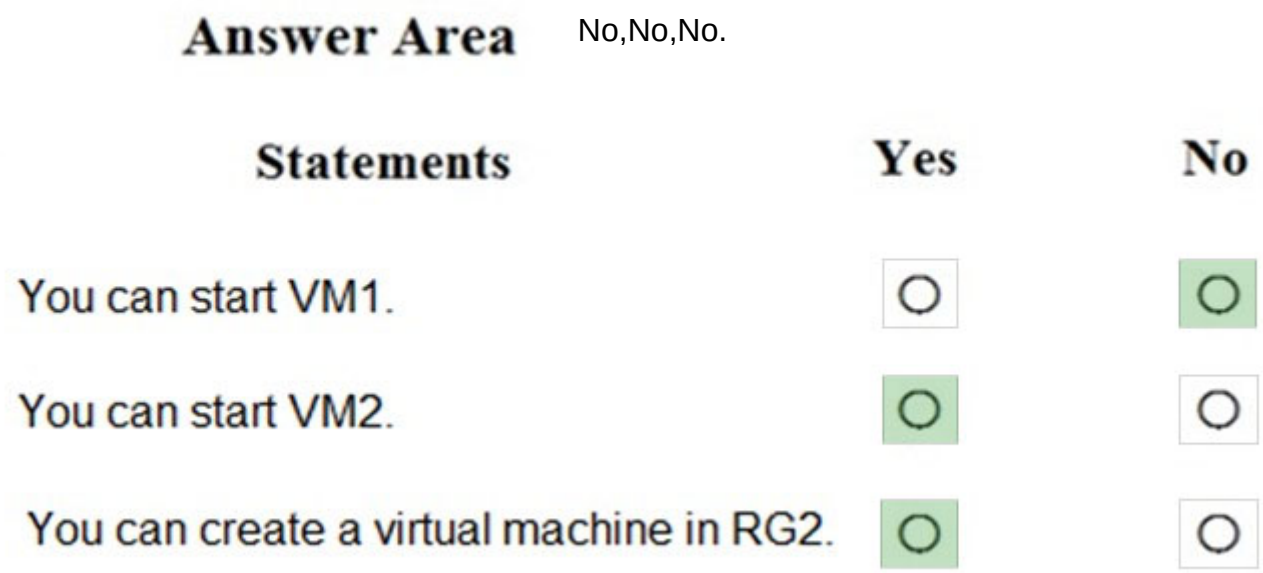
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



References:

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

snelkoppeling Highly Voted 1 year, 7 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 189 times

rgullini 2 months, 3 weeks ago

https://t.me/learningnets

This is correct. Also tested.
upvoted 3 times

prd0202 3 months ago
No doubt - it is No, No, No
upvoted 3 times

sureshatt 3 months, 2 weeks ago
this is the correct answer.
upvoted 2 times

xBoy 3 months, 3 weeks ago
No/No/No. Tested on LAB
upvoted 5 times

jbarszcz Highly Voted 1 year, 3 months ago
just tested it. No/No/No
upvoted 49 times

MarioMK Most Recent 1 month, 1 week ago
NNN it is so obvious.
A read-only lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request.

If you want to create a lock at a parent level, select the parent. The currently selected resource inherits the lock from the parent. For example, you could lock the resource group to apply a lock to all its resources.

ExamTopics please correct the false answer
upvoted 2 times

teehex 2 months ago
what is on earth with given answer? It is completely wrong.

Correct answers must be triple NO.
upvoted 4 times

Cyberbug2021 2 months, 1 week ago
A read-only lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
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 lock from the parent. The most restrictive lock in the inheritance takes precedence.
upvoted 1 times

Ayman79 4 months ago
A read-only lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request.
N
N
N
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources
upvoted 1 times

brpjp 4 months, 1 week ago
I think we need to read this like carefully as lock is applied to Resource Group and not Resources.

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.

If you read correctly alogwith Policy VM1 - Not allowed and VM2 allowed.

So answer given is correct.
upvoted 1 times

macco455 3 months, 2 weeks ago
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 lock from the parent. The most restrictive lock in the inheritance takes precedence
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources#how-locks-are-applied
Answer is : N,N,N
upvoted 2 times

DeepCyber 4 months, 2 weeks ago
No,No,No
Confirmed in the lab.
upvoted 4 times

https://t.me/learningnets

mak791 4 months, 2 weeks ago

Answer is No, No, NO

upvoted 1 times

DeepCyber 4 months, 2 weeks ago

Confirmed in the lab.
Answers:
No
No
No

upvoted 1 times

SnehaNaik 4 months, 2 weeks ago

All 3 should be NO

upvoted 1 times

JaggRO 4 months, 3 weeks ago

This answer should be tagged as wrong. You cannot create VM in RG2 which is ReadOnly. Just tested in Azure.

upvoted 1 times

milind8451 4 months, 3 weeks ago

NO - A read-only lock on a VM prevents all users from starting or restarting the VMs in it.
NO - A read-only lock on a RG prevents all users from starting or restarting the VMs in it.
NO - You can create new resources in RG if Delete Lock is applied but not when ReadOnly lock is applied.
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

upvoted 3 times

Xtian_ar 4 months, 4 weeks ago

No, No, and No!

upvoted 1 times

Thi 5 months, 2 weeks ago

Tested:
No
No
No

upvoted 2 times

AshTac 5 months, 3 weeks ago

Thank god I check all your comments. Agreed No, No and No!!!

upvoted 2 times

https://t.me/learningnets

Question #29 *Topic 2*

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

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

Correct Answer:

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 3 months, 3 weeks ago

answers correct

upvoted 11 times

dadageer Highly Voted 4 months ago

Correct!

https://t.me/learningnets

upvoted 5 times

little_h0rse Most Recent 1 month, 2 weeks 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 1 times

gcpbrig01 4 months ago

Security Admin - View and update permissions for Security Center.
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-admin
Service Administrator - Equivalent to Owner role. But only relevant in classic deployment model.
https://docs.microsoft.com/en-us/azure/role-based-access-control/classic-administrators
Hence the answer is correct

upvoted 2 times

https://t.me/learningnets

Question #30 *Topic 2*

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.

Correct 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 doesnג€™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 1 month, 3 weeks 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 5 times

Zorag 1 month, 3 weeks ago
Awesome this does the trick
upvoted 1 times

Zorag Most Recent 1 month, 3 weeks 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 1 times

Fred64 2 months, 2 weeks ago
why in step 6 it is said to not activate bi directional communication?
upvoted 1 times

sureshatt 4 months, 1 week 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 4 times

eroms 1 month, 3 weeks ago
tested it and it failed. You need an NSG rule for this to work
upvoted 1 times

https://t.me/learningnets

AZRA068 5 months, 2 weeks 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 1 times

AZRA068 5 months, 2 weeks 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 2 times

gcpbrig01 4 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 7 months, 3 weeks ago

The provided answer is correct as VMs in Vnet 1 can communicate with VMs in Vnet 2 and not bi-directional communication

upvoted 1 times

realname007 8 months ago

anyone knows the updated answer for this using the current interface ?

upvoted 2 times

https://t.me/learningnets

Question #31 *Topic 2*

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.

Correct 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 doesnλ€™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. Weλ€™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

vishg 8 months, 1 week ago

Also Required to add routing rule.

upvoted 2 times

Fred64 4 months ago

yes but we don't have enough informations to define the route. What is the next hop?

upvoted 1 times

https://t.me/learningnets

Question #32 *Topic 2*

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.

Correct Answer: *See the explanation below.*

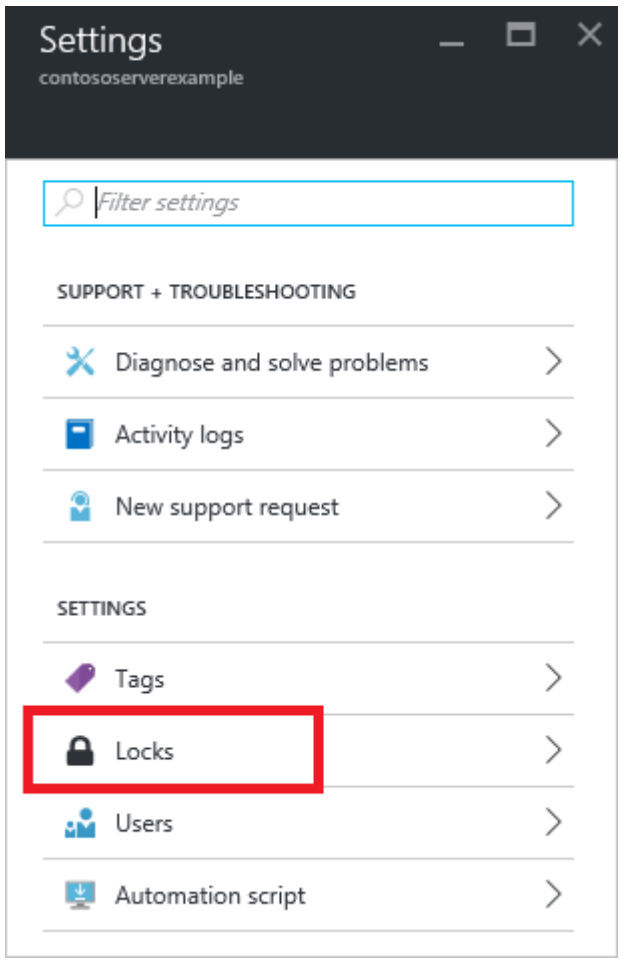
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

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.

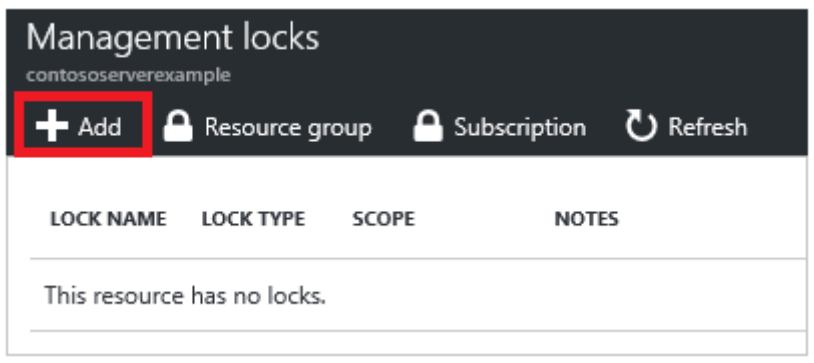
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET2. Alternatively, browse to

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.



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 4 months ago

This is the correct procedure for requirements outlined.

upvoted 2 times

https://t.me/learningnets

Question #33 *Topic 2*

You have an Azure virtual machine named VM1.

From Azure Security Center, you get the following high-severity recommendation: ג€Install endpoint protection solutions on virtual machineג€.

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 Advanced Threat Protection (Microsoft Defender ATP).

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection

peluca Highly Voted 11 months, 1 week ago

A is correct

upvoted 18 times

MrMozz Highly Voted 10 months, 2 weeks ago

levo017 - please do your homework before start confusing everybody here.
Microsoft clearly stated that you need to use the extension.

upvoted 5 times

macco455 3 months, 3 weeks ago

@mrmozz It made perfect sense to me, you are the one that needs to learn how to read!

upvoted 1 times

levo017 9 months, 4 weeks ago

Maybe my words are not exactly clear, but I AM saying option B is not making sense as it's a service pack download. So Answer is A.

upvoted 2 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 2 times

Azuriste 2 months, 3 weeks ago

Correct

upvoted 1 times

sukhdeep 3 months, 2 weeks ago

Answer is A as tested.

upvoted 2 times

glowglow 3 months, 2 weeks ago

Should be A, correct? B is Installing Microsoft System Center Security Management Pack on VM. should extensions for azure, correct?

upvoted 1 times

macco455 3 months, 3 weeks ago

https://docs.microsoft.com/en-us/azure/security-center/security-center-services?tabs=features-windows#supported-endpoint-protection-solutions-
In reading this, IF the server was 2012R2 and earlier, B would be the right answer, but if its 2016 or above than A would be. But since we don't have that info, we are unable to determine if the correct answer is A or B.

upvoted 1 times

milind8451 4 months, 3 weeks ago

A is right ans. Microsoft Endpoint protection is Malware extension. Done it lot of times in real life.

upvoted 4 times

reha 6 months ago

A is correct!
https://docs.microsoft.com/en-us/azure/security-center/security-center-services?tabs=features-windows , "Supported endpoint protection solutions "

upvoted 1 times

bluetaurianbull 6 months, 2 weeks ago

https://t.me/learningnets

Is it clear from https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

"Microsoft Antimalware can also be deployed using Azure Security Center. Read Install Endpoint Protection in Azure Security Center for more information."

To me also it seems A is the correct answer.

upvoted 2 times

bluetaurianbull 6 months, 2 weeks ago

Also the table in the URL is very clear and precise
https://docs.microsoft.com/en-us/azure/security-center/security-center-services?tabs=features-windows#supported-endpoint-protection-solutions-
System Center Endpoint Protection (Microsoft Antimalware) Windows Server 2012 R2, 2012, 2008 R2 (see note below) Via Extension Yes

upvoted 1 times

skng010 7 months, 3 weeks ago

Answer is A,

upvoted 4 times

ipindado2020 9 months, 1 week ago

I go for A

upvoted 1 times

Vinz_ 10 months ago

I think the provided link is incorrect. Here it is the one I believe is more relevant to the correct answer.
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

upvoted 1 times

Nou 11 months, 3 weeks ago

I think it is A, https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/iaas-antimalware-windows

upvoted 4 times

lalithasms 11 months, 3 weeks ago

Correct Answer is B

upvoted 1 times

levo017 10 months, 3 weeks ago

Endpoint protection in VM sense means protection against malware. Answer B's option is download pack for Windows Servers.

upvoted 1 times

levo017 9 months, 4 weeks ago

Just to be clear, Answer is A.

upvoted 6 times

https://t.me/learningnets

Question #34 Topic 2

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

Answer Area

Correct Answer:

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

https://t.me/learningnets

gcpbrig01 Highly Voted 4 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 8 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 4 times

Cyberbug2021 2 months, 2 weeks ago

Because - Secret

upvoted 2 times

rpm1234567 3 weeks, 4 days 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 1 times

Jacquesvz 2 days, 16 hours ago

Hi rpm1234567. given answers correct; see gcpbrig01's explanation.

upvoted 1 times

JohnYinToronto 3 months, 3 weeks ago

answers correct

upvoted 3 times

https://t.me/learningnets

Question #35 *Topic 2*

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

Correct 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

A365 Highly Voted 3 months, 2 weeks 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 9 times

dadageer Highly Voted 4 months ago

correct answer

upvoted 5 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago

A NSG required for JIT

upvoted 1 times

sureshatt 3 months, 2 weeks ago

wrong. Only vm4 has an attached NSG. The NSG should be attached to the VM, not to the network.

upvoted 2 times

macco455 3 months, 2 weeks ago

The given answer is correct as it doens't matter where the NSG is attached to for it to work

upvoted 3 times

https://t.me/learningnets

Question #36 *Topic 2*

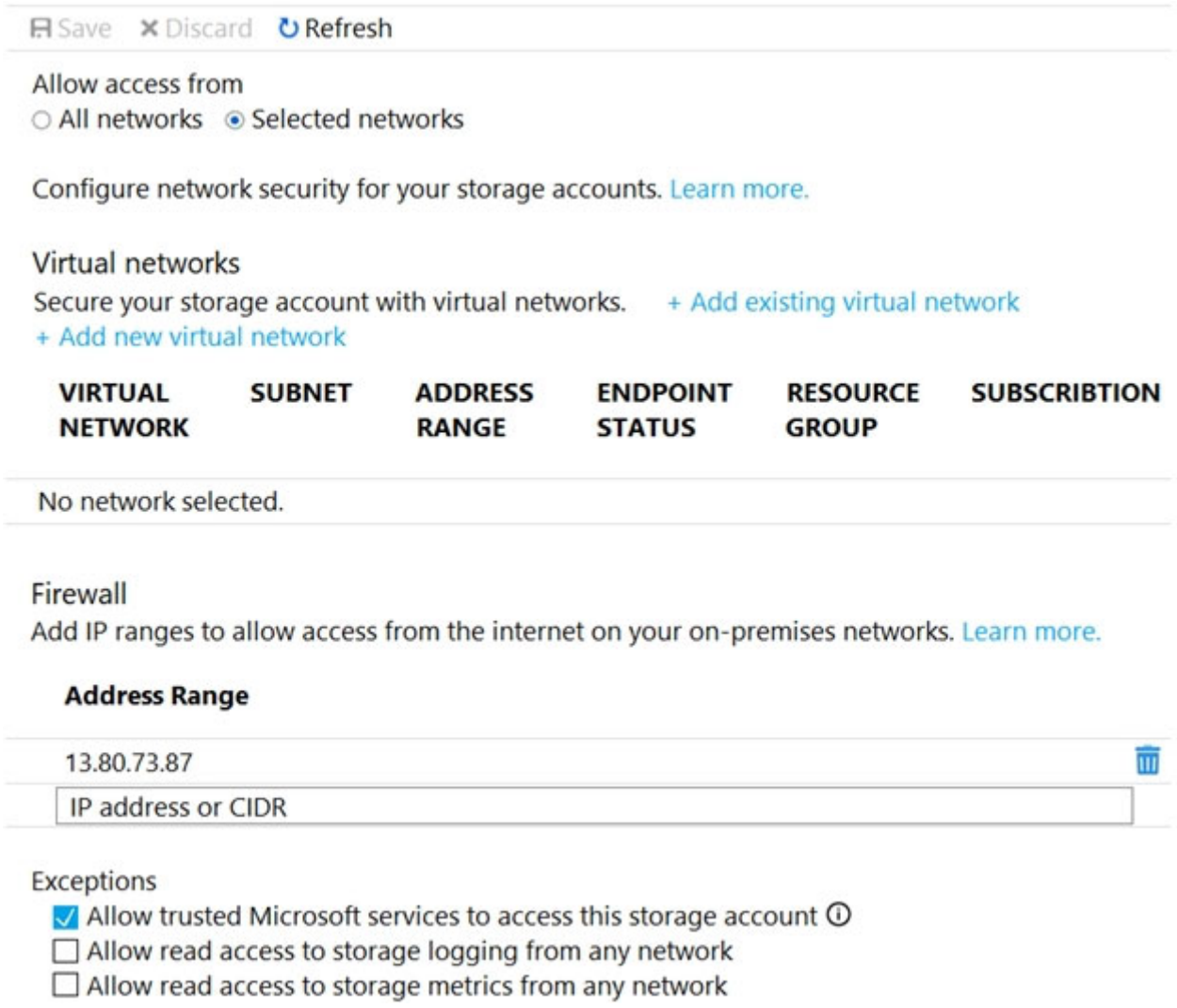
HOTSPOT -

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.



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.	○	○

Answer Area No,No,No

Correct Answer:

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

https://t.me/learningnets

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 3 months, 2 weeks 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 23 times

kimalto452 1 month 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 2 times

ChinkSantana 3 weeks ago
Correct. NO, NO, NO
upvoted 1 times

hang10z Highly Voted 3 months, 3 weeks 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 6 times

sureshatt 3 months, 2 weeks 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 2 times

Dineshvishe Most Recent 1 week, 1 day ago
As per my observation, the answers are correct. The service endpoint mentioned in only to confuse people. It has nothing to do with real question as it is not allowed to access the storage. Rest VM will be accessing storage with public IP which is allowed for VM1 and rest VM will not be able to access the storage as they are not allowed to.
upvoted 1 times

Shiningsoundar 3 weeks, 5 days ago
Storage accounts have a public endpoint that is accessible through the internet. You can also create Private Endpoints for your storage account, which assigns a private IP address from your VNet to the storage account, and secures all traffic between your VNet and the storage account over a private link. The Azure storage firewall provides access control for the public endpoint of your storage account. You can also use the firewall to block all access through the public endpoint when using private endpoints. Your storage firewall configuration also enables select trusted Azure platform services to access the storage account securely.
upvoted 2 times

rpm1234567 3 weeks, 3 days ago
Hi Shinigsoundar,
thanks in advance,
Can you have the correct answer for this question and confirm me in the exam there is no simulation.And also share the list of question.
upvoted 2 times

Cyberbug2021 2 months, 1 week ago
Azure Private Endpoint is a network interface that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet.

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.

https://docs.microsoft.com/en-us/azure/data-explorer/vnet-endpoint-storage-event-hub?tabs=storage-account
upvoted 1 times

Firedragon 2 months, 3 weeks ago
Given answer is correct.
if the condition changed to: Subnet1 and Subnet2 have a Microsoft.Storage private endpoint configured, then the answer will be Y Y Y
https://www.youtube.com/watch?v=HbVCi2NcKyU
upvoted 4 times

https://t.me/learningnets

Cyberbug2021 2 months, 1 week ago

Agree - Y - Y - Y

upvoted 1 times

rgullini 2 months, 1 week ago

To access from the private IP addresses you need both: A private endpoint and the firewall rule in the storage account

upvoted 5 times

JAGUDERO 2 months, 3 weeks ago

They are confusing "Services endpoints" uses public addressing and "Private Endpoint" uses private addressing on your Vnet.

The scenario talks about "Services endpoints"

upvoted 1 times

DilipJain 2 months, 4 weeks ago

The answer should be Yes, Yes, Yes
Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 3 times

rgullini 2 months, 2 weeks ago

Even it that case, the private vnets are not configure to access the storage.

upvoted 1 times

Firedragon 2 months, 3 weeks ago

If the Private endpoint is use, the answer will be Y Y Y. Given it's Service endpoint, Y N N.
https://www.youtube.com/watch?v=HbVCi2NcKyU

upvoted 2 times

teamaws 3 months, 1 week ago

Answer is correct, don't believe the naysayers

upvoted 2 times

milad123 3 months, 2 weeks ago

No, No, No
Endpoints allow you to secure your critical Azure service resources to "only" your virtual networks.
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#secure-azure-services-to-virtual-networks

upvoted 1 times

macco455 3 months, 3 weeks ago

Given that in the question it states that service endpoints are set up from subnet1 and 2 to the storage account, I think the answer are Yes,Yes,Yes As all servers can use the private IPs to route traffic over the service endpoints directly to the storage account. Thats my thought process, but I might be missing something. Feel free to correct and explain why.

upvoted 1 times

ChinkSantana 2 weeks ago

Yes we have Service end point at VNET side. On Storage side you also need to allow those Network. Dont Forget Principle of Least privilege.

upvoted 1 times

canonigo 3 months, 3 weeks ago

To support 1 is no as well.
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.
https://docs.microsoft.com/es-es/azure/storage/common/storage-network-security?tabs=azure-portal

upvoted 1 times

Pinchi 4 months ago

No,No,No
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 4 times

nihao381 3 months, 4 weeks ago

I could see arguments for Yes on 1 though, as publishing a private endpoint in the subnet does not block the VM from making a connection to the public endpoint for the storage service. This can be done via DNS overriding: https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns

upvoted 3 times

BalderkVeit 1 month, 3 weeks ago

agree with nihao - service endpoints are nice, but they don't change anything in this config. No vnets selected, and public access on firewall allowed on public IP of VM one. so Y - N - N

upvoted 1 times

dadageer 4 months ago

Answers are correct!

upvoted 4 times

https://t.me/learningnets

gcpbrig01 4 months ago

Answer is correct- service endpoint configuration in vnet must be followed by configuring the vnet under the firewall and network section of storage account.

upvoted 4 times

https://t.me/learningnets

Question #37 Topic 2

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

Answer Area

Correct Answer:

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 -

https://t.me/learningnets

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 1 year, 4 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 52 times

Rave763 Highly Voted 1 year, 2 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 10 times

gboyega 1 year ago

Correct. Answer is correct

upvoted 7 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 3 times

kumax 3 weeks, 4 days ago

On exam, May 2021.

upvoted 5 times

Cisna 2 months, 1 week ago

in exam 02/05/2021

upvoted 6 times

rpm1234567 3 weeks, 4 days ago

Hi Cisna,
Can you confirm the correct answer .

upvoted 1 times

milind8451 4 months, 3 weeks 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 3 times

milad123 5 months ago

correct

upvoted 2 times

JeanTremblay 5 months, 3 weeks ago

This is a question for the az-104 not the az-500 !!

upvoted 2 times

KaiserdomTW 1 month ago

Also seen on az - 304

upvoted 1 times

zic04 5 months, 3 weeks ago

Correct

upvoted 2 times

B1T3X 6 months, 1 week ago

Answer is correct. Location doesn't matter but when you create an update deployment you have to choose either Linux or Windows. (There are also older versions of both OS families that aren't supported, but in this case, all mentioned OS versions are supported)

upvoted 2 times

Surs 6 months, 3 weeks ago

Answer is correct. In update management, when you create a schedule you can either choose windows or linux.

upvoted 2 times

hamshoo 6 months, 4 weeks ago

You can connect all virtual machines onto an existing Update management solution

upvoted 1 times

Chrisinternet 7 months ago

Tested in Azure. When you add Azure VMs to Update Management, you can choose only 1 Location (East US OR West US) , Windows and Linux VM types..
SO answers, for me, should be:

https://t.me/learningnets

Update 1 : VM2 and VM4 (WestUS)
Update 2 : VM1 and VM5 (EastUS)

upvoted 1 times

nothankyouspankyou 2 weeks, 6 days ago

"Azure VMs can exist in any region, no matter the location of your Automation account."

from:
https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-portal#enable-update-management

upvoted 1 times

deepu1982 7 months, 3 weeks ago

Update Management can be used to natively deploy to machines in multiple subscriptions in the same tenant, its a tenant level . Answer is correct

upvoted 1 times

Stuudent 8 months ago

I don't know, look at point 4 here:

The list of virtual machines is filtered to show only the virtual machines that are in the same subscription and location. If your virtual machines are in more than three resource groups, the first three resource groups are selected.

https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-portal

upvoted 1 times

macco455 3 months, 3 weeks ago

Thats just showing you how tis set up not what can and cannot be added to the group. It also states if you need to show more just select them but it cant be more than 3

upvoted 1 times

btxy4 9 months, 1 week ago

https://docs.microsoft.com/en-us/azure/automation/update-management/update-mgmt-groups
Choose either Windows or Linux.

upvoted 2 times

TauruSH 10 months ago

How can this answer be correct,neither their resource group are same nor their region!!!!
i Think for 1st one it should be "For VM4 only" and for second one "For VM1,VM2 and VM5 Only"

upvoted 3 times

tms2020 9 months, 3 weeks ago

Update Management assesses and applies security updates to all connected Windows Server and Linux servers in a workspace as per https://docs.microsoft.com/en-us/azure/automation/update-management/update-mgmt-overview

Hence both update management solutions applicable to all the machines provided they should not be in stopped state

upvoted 5 times

mlourh 7 months, 1 week ago

I agree, update management solutions is applicable to all VMs even they are differents OS and different locations,

upvoted 1 times

https://t.me/learningnets

Question #38 *Topic 2*

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:

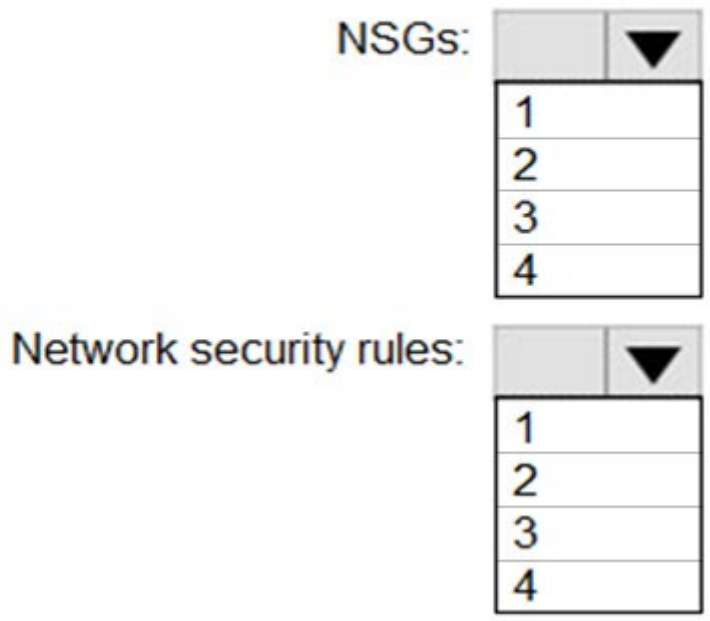
- Allow traffic to VM4 from VM3 only.
- Allow traffic from the Internet to VM1 and VM2 only.
- Minimize the number of NSGs and network security rules.

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



Answer Area NSG -1

Correct Answer:

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

https://t.me/learningnets

Oz Highly Voted 1 year, 7 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 80 times

Roy_Batty 10 months, 2 weeks 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

abrahamtek 3 weeks, 1 day 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

rgullini 2 months, 1 week ago

This is correct.

upvoted 2 times

sambsamb 6 months, 2 weeks ago

You don't need the 3rd deny rule.
We have the default rules 65500 to deny all inbound/outbound at the end of the default rule set
So Answer remains:
NSG ⇒ 1
Rules ⇒ 2
VM4 => VM3 Rule: Source AppGroup4, Destination AppGroup3
Internet => VM1,2 Rule: Source Internet, Destination AppGroup12
not counting the default rules that end up denying all

upvoted 9 times

Xtian_ar 4 months, 4 weeks ago

Yes, a 3rd deny rule is needed. You mentioned that there is a defualt deny rule, yes, but there is a defualt allow rule that allow any traffic between VMs of the same VNet, so that is the reason a 3rd deny rule is needed

upvoted 12 times

Fred64 2 months, 2 weeks ago

yes but we can remove it so it is still 3 rules

upvoted 2 times

nicksu 1 month, 3 weeks ago

one cannot remove default 65000+ rules

upvoted 6 times

Oz Highly Voted 1 year, 7 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 22 times

gills 8 months, 2 weeks 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 6 times

Arejay 5 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

bhbh2020 Most Recent 2 weeks, 5 days ago

check URL https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VM's within it. For example, if a rule is added to NSG1 which denies all inbound and outbound traffic, VM1 and VM2 will no longer be able to communicate with each other. Another rule

https://t.me/learningnets

would have to be added specifically to allow this.

AllowVNetInBound - default rule
This rule permits all the hosts inside the virtual network (including subnets) to communicate between them without any blocks.

Required NSG = 1 -> to block traffic on VM4 you can use the same NSG -> remmber NSG on subnet affect connectivity between VMs within it
Required Rules= 3

A rule to allow traffic to VM4 from VM3
A rule to allow traffic from internet to AppGRoup12 (VM1+VM2)
A rule to block to override AllowVNetInBound

upvoted 1 times

bhbh2020 2 weeks, 5 days ago

check URL https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VM's within it. For example, if a rule is added to NSG1 which denies all inbound and outbound traffic, VM1 and VM2 will no longer be able to communicate with each other. Another rule would have to be added specifically to allow this.

AllowVNetInBound - default rule
This rule permits all the hosts inside the virtual network (including subnets) to communicate between them without any blocks.

Required NSG = 1
to block traffic on VM4 you can use the same NSG -> remmber NSG on subnet affect connectivity between VMs within it.

Required Rules= 3

A rule to allow traffic to VM4 from VM3
A rule to allow traffic from internet to AppGRoup12 (VM1+VM2)
A rule to block to override AllowVNetInBound

upvoted 1 times

Cyberbug2021 2 months, 1 week ago

Since we are dealing with 1 subnet - 1 NSG on that subnet is sufficient.
So box 1 is 1

Now the don't forget the default rules when you apply the NSG
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules

Inbound and outbound - from vnet to vnet is all allowed, so you need a rule to block all vnet to vnet traffic (above 65000) - thats 1, then you need a rule to allow VM4 to VM3 only - thats 2.
All internet outbound is allowed, all internet inbound is denied - so you only need 1 more rule to allow the internet inbound traffic.

So box 2 would be 3 rules

upvoted 1 times

esatu 2 months ago

How about this? Inbound and outbound - from vnet to vnet is all allowed. We just need one rule to block AppGroup12 to VM4. So 2 rules, one for the internet inbound and one to block traffic from AppGroup12 to VM4 (which in other word allows communication between VM3 and VM4 only). And 1 NSG at subnet level.

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

1 NSG and 2 Rules - VM1 and VM2 are both in the same ASG so you can use ASG in destination don't have to use specific ips
Deny rule is already in by default - don't have to add that.

upvoted 1 times

JOKERO 2 months, 1 week ago

you need to put a inbound Deny All rule, it will impact the communication between the VMs in the same subnet.

upvoted 1 times

cannibalcorpse 3 months ago

1 and 1
1 NSG
1 NSG rule for incoming traffic from the internet. We dont need to create for traffic between VM4 and VM3

upvoted 4 times

macco455 3 months, 3 weeks ago

SInce vnet traffic is effected by the NSG on the subnet, you can deny vnet traffic by putting a deny all rule on the NSG.
Therefore, 1NSG
3 Rules is the answer as stated by many others.

upvoted 1 times

sureshatt 4 months, 3 weeks ago

According to https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups
We need 1 NSG since one Subnet
We need 3 Rules.
1. allow internet to appgroup12

https://t.me/learningnets

2. allow iappgroup3 to appgroup4
3. Deny all to appgroup4.

upvoted 1 times

milind8451 4 months, 3 weeks ago

Ans is 1 and 3. Since there is 1 subnet so you can create 1 NSG for the subnet, you can assign NSG to each VM as well but then you need 4 NSGs which is not optimum solution as they need minimum NSGs so 1 NSG for first ques. Here are the 3 NSG rules to be created -
1) Allow Inbound traffic from Internet for VM1 and VM2 (App Group 12)
2) Deny all traffic to VM4
3) Allow traffic from VM3 to VM4

By default, all inbound traffic from internet is denied Because it is denied by the DenyAllInbound default security rule.

upvoted 1 times

Shades 4 months, 4 weeks ago

This is the exact example used in below articled, read the diagram well:

https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

upvoted 3 times

JeanTremblay 5 months, 1 week ago

The question is bout allowing traffic from a VM to another or from internet to 2 VM. Nothings mentions to allows traffic to The question talks ONLY about allowing internet traffic to 2 VMs; and traffic from one VM to another. The question doesn't talk about traffic involving ASGs
1 NSG & 2 rules
Source Port Destination Port, Protocol
Internet 0-65535 10.0.0.10, 10.0.011 0-65535 any
10.0.0.100 0-65535 10.0.0.100, 10.0.011 0-65535 any
an ASG

upvoted 1 times

Thi 5 months, 2 weeks ago

NSG1: 1, Network security rules:1
NSG1: All VM are in the same subnet with different NIC. As soon as we deploy any default or custom NSG, it adds the default rule which can not be either deleted or modified, to communicate within all resources in the same VNet.
NSG Rules: Here all VMs are in the same subnet, and you know the three default rules are automatically deployed by Microsoft which can neither deleted nor modified. Means there is no control of user on these rules. So ideally, without any adding rule, VM can communicate with each other inside a VNet whose member it is.Hence No. of Rule added by user is Zero. This fulfills our 1st requirement "Allow traffic to VM3 from VM4" for 2nd requirement "Allow traffic from the Internet to VM1 and VM2 only" we need to add a rule in the same NSG. So minimum number of rules in NSG is 1.

upvoted 1 times

Thi 5 months, 2 weeks ago

NSG1: 1, Network security rules:1
NSG1: All VM are in the same subnet with different NIC. As soon as we deploy any default or custom NSG, it adds the default rule which can not be either deleted or modified, to communicate within all resources in the same VNet.
NSG Rules: Here all VMs are in the same subnet, and you know the three default rules are automatically deployed by Microsoft which can neither deleted nor modified. Means there is no control of user on these rules. So ideally, without any adding rule, VM can communicate with each other inside a VNet whose member it is.Hence No. of Rule added by user is Zero. This fulfills our 1st requirement "Allow traffic to VM3 from VM4" for 2nd requirement "Allow traffic from the Internet to VM1 and VM2 only" we need to add a rule in the same NSG. So minimum number of rules in NSG is 1.

upvoted 1 times

inf 5 months, 4 weeks ago

Answer: 1 NSG, 3 Rules
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups
Article is very close to the requirements (as indicated by canbe)

No requirement for any VM to communicate with another VM except from VM4->VM3. Thus all other intra-vnet traffic could be denied, however ignored is much simpler.

1 x NSG assigned to subnet
3 x Rules assigned to NSG
1 - 100 - Allow traffic from VM4 (AppGroup4) to VM3 (AppGroup3)
2 - 200 - Allow traffic from Internet to VM1,VM2 (AppGroup12)
3 - 500 - Deny all traffic to VM3 (AppGroup3)

(3 x default rules, NOT created thus don't increase rule count, are:
1 - 65000 - Allow VirtualNetwork<-->VirtualNetwork
2 - 65001 - Allow AzureLoadBalancer->Any
3 - 65002 - Deny Any<-->Any
)

upvoted 3 times

canbe20 5 months, 4 weeks ago

In the docs very similar scenario is described: https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups
Then 1 NSG and 3 rules looks enough. Initially, I also thought 2 NSGs and 3 rules, however I haven't taken into account the app security groups

upvoted 1 times

lateralus 6 months ago

https://t.me/learningnets

Tested this in a lab: you can go with 1 NSG group with 2x DENY rules:
Rule 1: Inbound rule: deny any traffic from AppGroup12 to AppGroup4. You don't need to deny internet as this is a default inbound rule. Also you don't need to allow Vm3 to VM4 traffic as they are in the same vnet and traffic is allowed by a default rule.
Rule 2: Inbound rule: Allow Internet from Any to AppGroup12.

upvoted 3 times

https://t.me/learningnets

Question #39 *Topic 2*

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

Answer Area

Correct Answer:

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

Rume 2 weeks ago

Answer is correct.

upvoted 1 times

https://t.me/learningnets

Question #40 *Topic 2*

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

Correct 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.

gfhbox0083 Highly Voted 1 year 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 14 times

besha Most Recent 2 weeks, 4 days ago
This question definitely will be in the exam! 4th time here
upvoted 1 times

kimalto452 1 month ago
same question wtff
upvoted 1 times

Rupain 1 month, 1 week ago
4th time repeating
upvoted 1 times

cmong2005 1 month, 3 weeks ago
repeated question
upvoted 1 times

zic04 5 months, 3 weeks ago
Correct
upvoted 3 times

kristiann21 1 year, 1 month ago
correct answer
upvoted 4 times

ogbeufi1 1 year, 1 month ago
Correct
upvoted 4 times

https://t.me/learningnets

Question #41 *Topic 2*

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

Correct 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

Rume 2 weeks ago

given answer is correct

upvoted 1 times

https://t.me/learningnets

Question #42 Topic 2

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

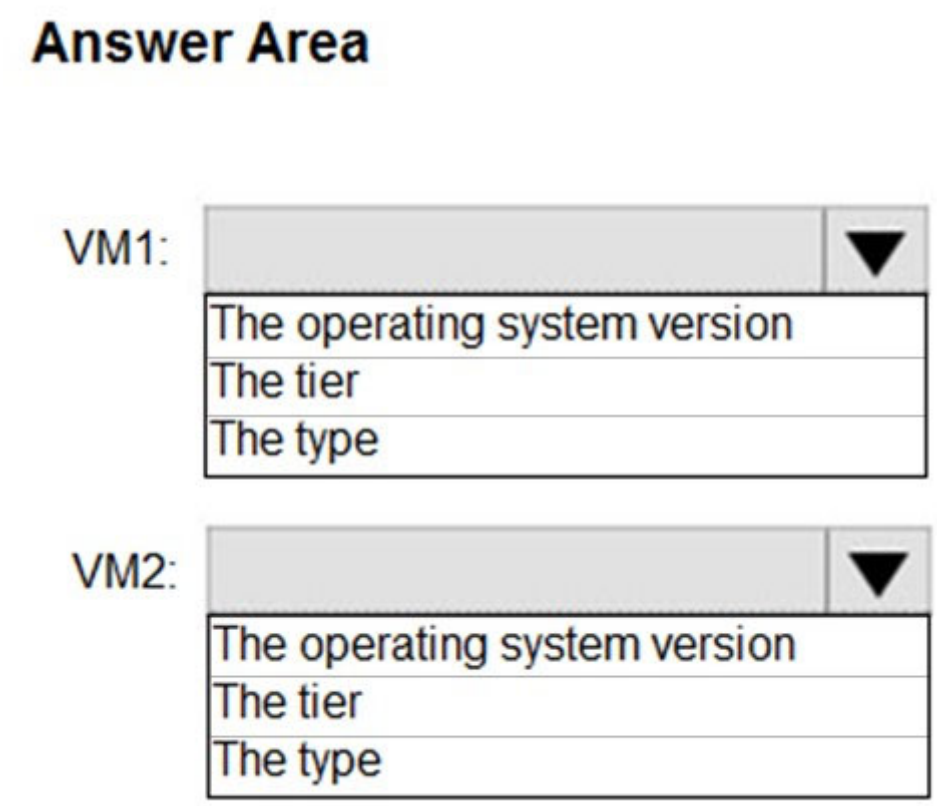
You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

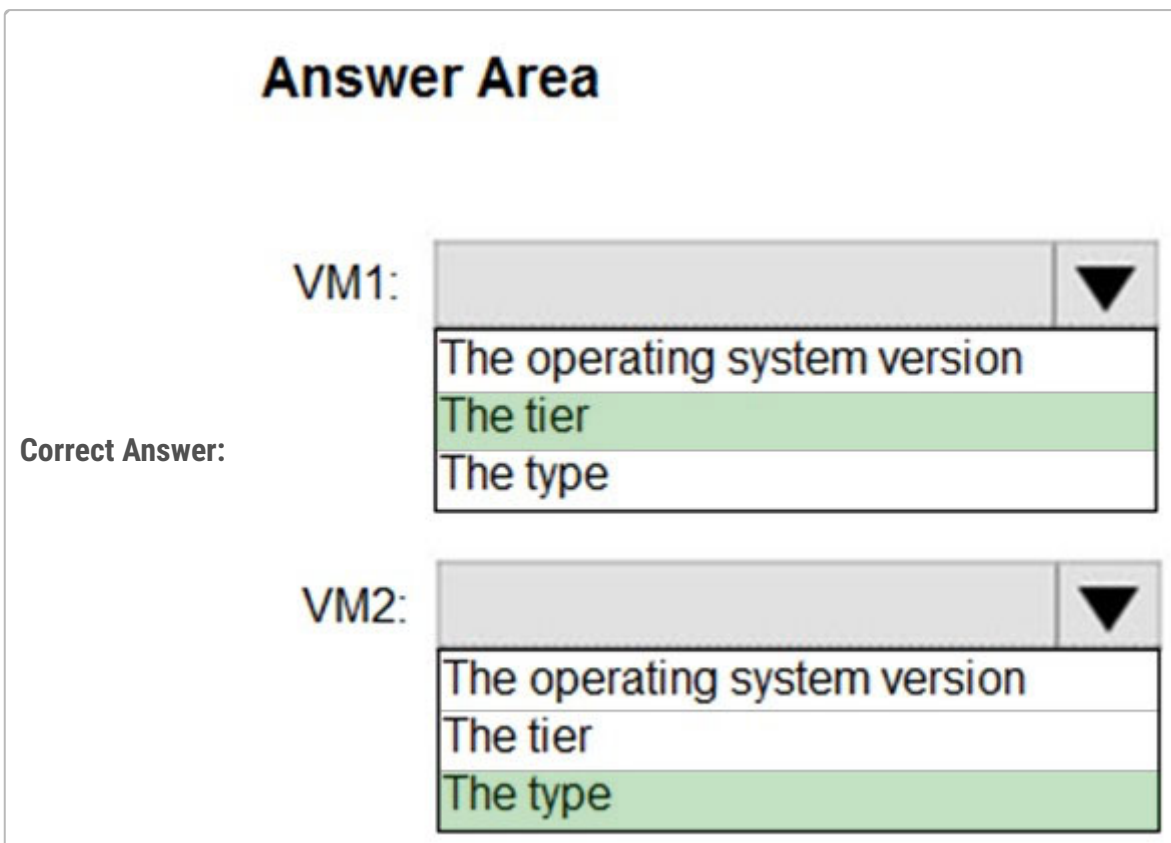
What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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

https://t.me/learningnets

dirgiklis Highly Voted 1 year, 4 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 30 times

AZGregor 6 months, 1 week 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 6 times

levo017 10 months, 3 weeks ago

very thorough, thanks !

upvoted 2 times

gboyega 1 year ago

this is CORRECT

upvoted 1 times

dumpmaster 1 year, 3 months ago

But you can have a VM L4s using Generation 1. Maye this is a wrong question or incomplete.

upvoted 2 times

Solanki Highly Voted 1 year, 2 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 12 times

aythan09 1 year, 1 month ago

A L4s is not a LsV2.
https://azure.microsoft.com/en-us/pricing/details/virtual-machines/linux/#lsv2-series

upvoted 3 times

SandroAndrade Most Recent 1 month, 3 weeks 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 1 times

gcpbrig01 4 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 4 months, 3 weeks 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 5 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 5 months, 1 week ago

the answer is correct

upvoted 1 times

Thi 5 months, 2 weeks 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 1 month, 3 weeks ago

L4S is there
https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-previous-gen

https://t.me/learningnets

4 x vCPU & 32Gb RAM, but it is "of previous generation". This could be the key
upvoted 1 times

B1T3X 6 months, 1 week 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

bluetaurianbull 6 months, 3 weeks ago
VM1 is clearly TIER - no doubt.
For VM2 "The Operating system version" which is Ubuntu 16.04-DAILY-LS doesn't look like is a supported version for Encryption.

Azure Disk Encryption for Linux VMs - https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#supported-vms-and-operating-systems
Endorsed Linux distributions on Azure - https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros

Ubuntu by Canonical Ubuntu Server and Pro. 16.x, 18.x, 20.x
Information about extended support for Ubuntu 12.04 and 14.04 can be found here: Ubuntu Extended Security Maintenance.
upvoted 1 times

tarq 5 months, 4 weeks ago
its 16.04-DAILY-LTS (not LS) OS which is clearly supported in link you provided.
upvoted 1 times

inf 5 months, 4 weeks ago
Incorrect. ADE is supported for this flavour of OS
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview
Canonical Ubuntu 16.04 16.04-DAILY-LTS Canonical:UbuntuServer:16.04-DAILY-LTS:latest OS and data disk
upvoted 1 times

ufuomaolori 6 months, 3 weeks ago
Given Answer seems correct.
These links will help clarify the argument:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux#unsupported-scenarios
upvoted 1 times

Danish12 7 months ago
Answers are correct, see the link for details https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview#supported-vms-and-operating-systems
upvoted 1 times

GayanWK 7 months, 1 week ago
Standard_L4s - is part of
https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-previous-gen#ls-series
This may not support encryption since it's Newer size recommendation: Lsv2-series is not supporting.
upvoted 1 times

Respar 7 months, 3 weeks ago
I think the answer for VM2 is correct.
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview
upvoted 1 times

kiketxu 7 months, 3 weeks ago
1. Type A is not supported, as same than Basic.
2. The question is wrong. It's OS because is valid, it isn't Gen2 and its a valid Tier.

Those who prepared this question, should correct it. I saw similiar question in other sites and the statement is different. Don't believe this wrong question will be in the exam.

GL all!
upvoted 2 times

Stuudent 8 months ago
Are we seriously expected to know the level of detail which machine is which generation BY HEART?! A a SECURITY ENGINEER? I must say I am getting frustrated with the level of the questions, this is not something one needs to know by heart, it can be looked up.
upvoted 9 times

paulxyz90 6 months, 2 weeks ago
Agree - test writers are losing their marbles. Anyone who does not have access to this site's material is toast.
upvoted 1 times

awssecuritynewbie 7 months, 4 weeks ago
i agree dude
upvoted 1 times

Kampo 10 months ago
I guess 2nd is Server OS. Ubuntu 16.04 is not supported for Azure disk encryption. See this.
https://docs.microsoft.com/en-us/azure/virtual-machines/generation-2#generation-2-vm-sizes

https://t.me/learningnets

upvoted 1 times

Stuudent 8 months ago

Ubuntu 16.04-DAILY-LTS is specifically mentioned as supported.

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

upvoted 3 times

https://t.me/learningnets

Question #43 Topic 2

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

Correct Answer: *A* C

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

Oz Highly Voted 1 year, 7 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 134 times

Kinanke 5 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

AZGregor 6 months, 2 weeks 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 2 times

D0yle 1 year, 5 months ago

Yes, you can deploy Log Analythics to certain regions but the you can add VMs from anywere, including from your local network.

upvoted 5 times

onlyfunmails 1 year, 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

https://t.me/learningnets

junkz Highly Voted 1 year, 9 months ago

vm1 and 4 can, analytics integration is bound by region, not RG

upvoted 57 times

SandroAndrade 1 month, 3 weeks 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 1 times

samankaluarach Most Recent 1 week ago

C is a correct answer. VMs aren't limited to the regions supported by the Log Analytics workspace.
https://docs.microsoft.com/en-us/azure/automation/how-to/region-mappings

upvoted 1 times

MarioMK 2 months ago

the correct answer is C. Tested in the portal.

upvoted 3 times

roy9889 2 months, 1 week ago

You may deploy NEW VMs from any region within the USA geography, but here they want to know which existing VM can connect.
If you create a workspace, there is only a single option to select Resource Group and then the VMs within that RG populate. So in this case, only VM1 is in RG1 that you have already selected for the workspace.

The question doesnt want to know what all possibilities are there IN GENERAL, in which case your answer would have been absolutely correct.
The question instead wants to know what the possibilites are after the current selection that has ALREADY been made.

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

C is the answer - all VMs
"You can monitor Azure VMs in any region. The VMs themselves aren't limited to the regions supported by the Log Analytics workspace."

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

just checked log analytics is available in all regions (almost) - but there is cost when transferring between geographical regions, since the the cost does not mention anything to do with cost, the answer will be all. VM1, VM2, VM3 and VM4

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

I also think log analytics is not available in west europe

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

its geographically bound I think - The two regions listed are in different geographical regions. one in US and other in Europe. so all US regions would be allowed

upvoted 1 times

Fred64 4 months, 1 week ago

Log analytics is not region bound. Just try!
So all VM can be bound

upvoted 5 times

JaggRO 4 months, 2 weeks ago

C is correct answer. Just tested to connect VM in one region to LAW in different region. It works fine.

upvoted 3 times

PM2 4 months, 3 weeks ago

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 regulatory requirements, or your company's compliance requirements. Having VMs in a a different region could also introduce data bandwidth charges. -- Answer is C.

upvoted 2 times

JaggRO 4 months, 3 weeks ago

I have just tested it and I was able to add ALW to VM in RG1 and ALW is in RG2. And it's working fine. The answer is wrong and ALW is bound by region only.

upvoted 1 times

milind8451 4 months, 3 weeks ago

All Vms can be connected to LA workspace, Log Analytics is not restricted by region or resource group.

upvoted 3 times

sukhdeep 5 months, 1 week ago

Given answer is incorrect. I did test in azure portal. Log analytics workplace connect to any VM irrespective of Region and resource groups. So answer will be all VMs.

upvoted 2 times

https://t.me/learningnets

Falkreath 6 months ago

Answer is C. Tested this in my lab environment with a bunch of VMs and Resource Groups in different regions and they all connected to the LAW.

upvoted 1 times

RSSRAO 6 months, 1 week ago

correct answer should be: VM1, VM2, VM3 and VM4

upvoted 2 times

https://t.me/learningnets

Question #44 *Topic 2*

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.

Correct 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

JohnYinToronto Highly Voted 3 months, 3 weeks ago

answer correct

upvoted 9 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 2 times

https://t.me/learningnets

Question #45 *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. 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

Correct 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

lnn_az Highly Voted 1 year, 1 month 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 12 times

GayanWK 7 months, 1 week ago
or you can use ARM template deployment.
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/iaas-antimalware-windows#template-deployment
upvoted 2 times

Solanki Highly Voted 1 year, 2 months ago
answer is right,

https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware#antimalware-deployment-scenarios
upvoted 11 times

glowglow Most Recent 3 months, 2 weeks 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 1 times

Super_Pun 4 months ago
It's correct, Microsoft Antimalware is the extension attached to the Windows Server
upvoted 1 times

sureshatt 4 months, 3 weeks ago
We do this for our VMs. So the answer is correct.
upvoted 2 times

sukhdeep 5 months, 1 week 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 5 months, 3 weeks ago
Correct A
upvoted 2 times

kiketxu 7 months, 3 weeks ago
right answer. DSC extension is the way

https://t.me/learningnets

upvoted 3 times

gboyega 1 year ago
ANSWER IS CORRECT
upvoted 5 times

jakobaszek 1 year, 1 month ago
The answer is A
upvoted 1 times

Otto_Aulicino 1 year, 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 1 year, 4 months ago
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware
upvoted 2 times

Question #46 *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. 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

Correct Answer: *B*
Microsoft Antimalware is deployed as an extension and not a feature.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

kiketxu Highly Voted 7 months, 3 weeks ago
Windows feature is not for DSC extensions. NO is the correct answer.
upvoted 6 times

gboyega Most Recent 1 year ago
B IS CORRECT
upvoted 3 times

gfhbox0083 1 year ago
B, for sure
upvoted 3 times

rajatw 1 year, 2 months ago
Correct Answer. It's B
upvoted 4 times

https://t.me/learningnets

Question #47 *Topic 2*

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.

D. From Azure AD, configure the User settings.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

SteroidalRED Highly Voted 6 months, 3 weeks 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 11 times

tuta Highly Voted 6 months, 4 weeks ago
A is correct - though question has been repeated
upvoted 11 times

aftab7500 Most Recent 2 months, 2 weeks ago
Azure AD can only be enabled on Kubernetes RBAC-enabled cluster.
Azure AD legacy integration can only be enabled during cluster creation.
upvoted 1 times

g2d2 4 months, 1 week 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 4 times

HardcodedCloud 4 months, 2 weeks ago
Answer is A.
upvoted 4 times

mayenite 5 months, 2 weeks ago
I believe the answer should be D
upvoted 1 times

v078 4 months, 2 weeks ago
"D. From Azure AD, configure the User settings."? I am not an AKS expert, but I doubt it is so - there is nothing that could solve the stated problem, I will go with A.
upvoted 1 times

xaccan 3 months, 2 weeks ago
You just believe but you are not sure?
You should give justification why D is correct?
Answer is A
upvoted 1 times

https://t.me/learningnets

Question #48 *Topic 2*

You have an Azure subscription that contains an Azure Container Registry named Registry1. Azure Defender is enabled in the subscription.
You upload several container images to Register1.
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

Correct Answer: *A*
Reference:
https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/

Rahulbard 4 days, 17 hours ago
The question is a bit tricky. It says that Azure defender is enabled, which means images are being scanned using Qualys. So how is it he answer "A"
upvoted 1 times

romaso82 1 week, 6 days ago
Answer C:
upvoted 1 times

Rume 2 weeks ago
Given answer is correct
upvoted 1 times

https://t.me/learningnets

Question #49 *Topic 2*

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.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

dumpmaster Highly Voted 1 year, 3 months ago
Right, I use Azure monitor for some of my clients.
upvoted 12 times

cunlu Highly Voted 6 months, 3 weeks 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 5 times

MarioMK Most Recent 1 month, 3 weeks 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

Cyberbug2021 2 months, 2 weeks 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 5 months, 3 weeks 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 3 times

inf 5 months, 3 weeks 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 11 months, 2 weeks 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 10 months ago
That is very very wrong. Best solution is definately to define an action group
upvoted 4 times

https://t.me/learningnets

joilec435 1 year, 2 months ago

sentinel

upvoted 3 times

JohnCrawford 1 year, 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

https://t.me/learningnets

Question #50 *Topic 2*

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

Correct 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

Jhonsteve83 Highly Voted 1 year, 2 months ago
answer is correct
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview
upvoted 17 times

kdkdk Highly Voted 7 months ago
in the exams
upvoted 14 times

zic04 Most Recent 5 months, 3 weeks ago
C correct
upvoted 4 times

deegadaze1 6 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 2 times

gboyega 1 year ago
C IS CORRECT
upvoted 2 times

gfhbox0083 1 year ago
C, for sure.
User-defined route
upvoted 3 times

kristiann21 1 year, 1 month ago
correct answer
upvoted 6 times

https://t.me/learningnets

Question #51

Topic 2

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

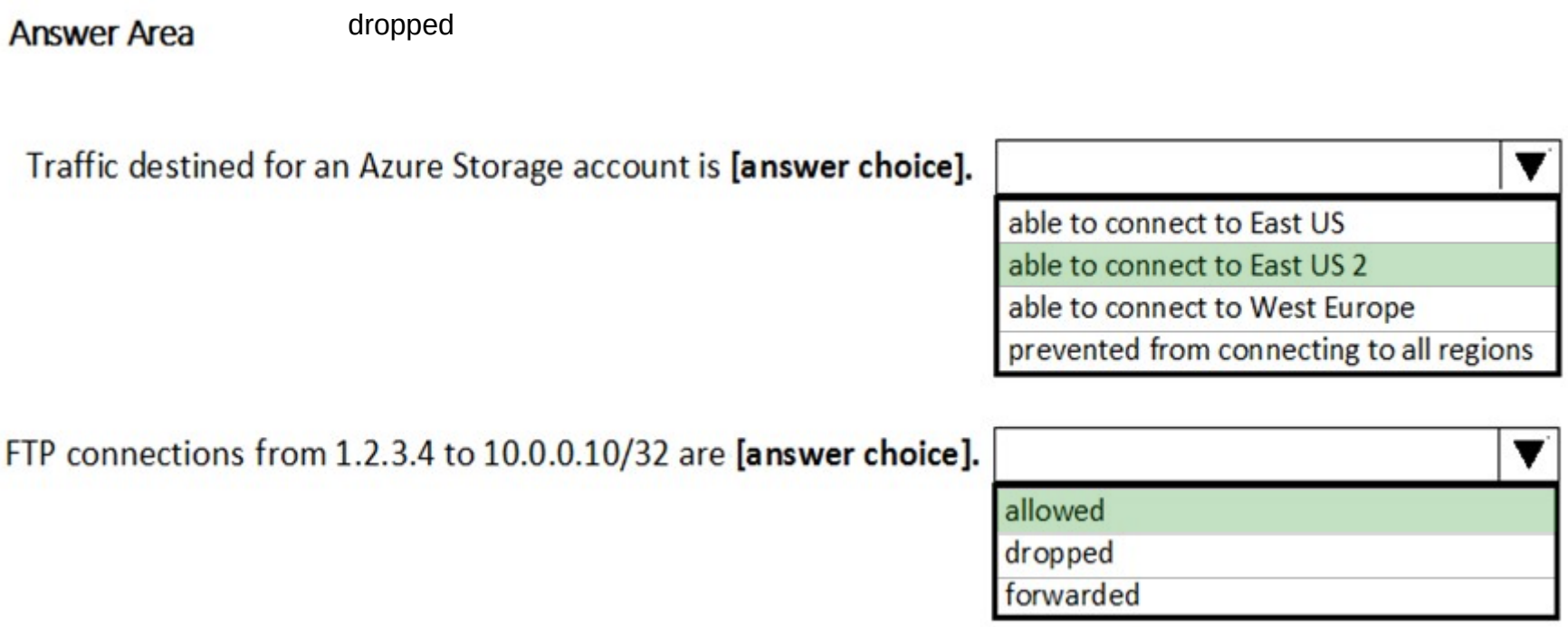
FTP connections from 1.2.3.4 to 10.0.0.10/32 are **[answer choice].**

- allowed
- dropped
- forwarded

https://t.me/learningnets

Correct Answer:

Answer Area



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 1 year, 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 113 times

rgullini 2 months, 2 weeks 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 1 times

GraceCyborg 5 months ago

i believe its a typo..

upvoted 3 times

gboyega Highly Voted 1 year 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 27 times

Rahulbard Most Recent 4 days, 16 hours ago

Agree. The answer for the second part is "Dropped". THe other reason i thought was because the priority on the first rule is lower, which means it will deny all

upvoted 1 times

Deepmindx 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 3 times

longtech 1 month, 2 weeks ago

the answer is wrong in the second box. Because, it allows for specify address which is 10.10.10.5/32. However, in this question, the address is 10.10.10.10/32, so the traffic will be dropped.

upvoted 2 times

alryazvrn 2 months ago

As far as I remember, port 21 is not enough for ftp. 20 should be opened as well. And in some cases dynamic ports are used as well

upvoted 1 times

https://t.me/learningnets

Fred64 2 months, 2 weeks ago

box 1: east 2
box 2: dropped

because rule 104 applies before 504 and deny everything

upvoted 3 times

russ0 2 months, 2 weeks ago

I meant denied by 105..

upvoted 1 times

russ0 2 months, 2 weeks ago

What about the priority? Would 504 (FTP) already be denied by 104? Not considering even a typo or if it is really wrong (would be dropped), just based on priority. Or am I messing up the priotities?

upvoted 3 times

AnupAnup 4 months, 1 week ago

Tried and Tested: 1st answer is correct. 2nd answer is also correct. here is the explanation. A VNet can have two IP ranges 1.0.0.0/8 and 10.0.0.0/8 together to make it part of same VNet. Additionally, the top most default rule of NSG is Allow all within same VNet. Hence, FTP traffic on port 21 from 1.2.3.4/32 to 10.0.0.10/32 is also allowed due to default allow all rule within same VNet.

upvoted 2 times

gcpbrig01 4 months ago

wrong. 10.0.0.10/32 is equivalent to 10.0.0.10. It is not mentioned in the FTP rule. Also not allowed by the default "DenyAllInbound" rule.

upvoted 2 times

xaccan 3 months, 2 weeks ago

AnupAnup, with your result seems you dont know how to work with Azure NSG.

upvoted 3 times

Fred64 4 months, 1 week ago

Be carefull to order of precedence

upvoted 1 times

sureshatt 4 months, 3 weeks ago

Answers:
1. East US 2 able to connect
2. packed is dropped. only 10.0.0.5/32 is allowed (NOT 100.0.0.10/32)

upvoted 2 times

v078 4 months, 2 weeks ago

Probably also worth mentioning, that the cmdlet does only show additional rules on the NSG, which means, that there is a rule, denying all inbound traffic, which we do not see in the ouput.

upvoted 1 times

milind8451 4 months, 3 weeks ago

1) Able to connect to East US2 (because storage allow rule priority is 104 and deny is 105, so allow will be enforced over deny)
2) Allowed (Assuming that it is a typo and destination is 10.0.0.5/32) else dropped

upvoted 4 times

Pinto 5 months, 1 week ago

NSG is bound to the subnet. From the subnet outbound connection is allowed only to East US 2 storage account as the priority of StorageEA2Allow rule is higher.
The ftp rule is for incoming traffic. The rule states traffic allowed from 1.2.3.4 to 10.0.0.5:21 will be allowed. But in the choice the destination IP is mentioned as 10.0.0.10. Hence, will be dropped by the deny all rule.

upvoted 1 times

Thi 5 months, 1 week ago

I dont agree please understand about direction of NSG it's outside direction not inside direction

upvoted 1 times

xaccan 3 months, 2 weeks ago

The Question does not state if the traffic is egress or ingress.

upvoted 1 times

AshTac 5 months, 3 weeks ago

I may be wrong but here is my feeling. For the first question, we are being thrown off by the two outbound rules. As far as I can tell, this question is talking about inbound connectivity for both questions. (feel free to correct me If you think I am wrong)

Q1 - the answer is "prevented from connecting to all regions"
Q2 - The answer is "dropped" since the IP added for the /32 is not the same one listed in the question

upvoted 5 times

pittaya_r 3 months, 3 weeks ago

I think the question mean that if we attached this NSG to VM then outbound from VM to StorageAccount is allow/deny

upvoted 1 times

https://t.me/learningnets

seconazure 4 months, 1 week ago

I agree

upvoted 1 times

Thi 5 months, 2 weeks ago

AshTac: Agree with you. I feel the same....

upvoted 2 times

JeanTremblay 5 months, 3 weeks ago

For the storage: No connection at all. The direction is Outbound ; not Inbound

upvoted 2 times

zic04 5 months, 3 weeks ago

East US2 and dropped sure

upvoted 5 times

https://t.me/learningnets

Question #52 *Topic 2*

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

Correct 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/

HarryD Highly Voted 1 year, 3 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 21 times

maj79 1 year ago

hence answer A is correct

upvoted 6 times

rgullini 2 months, 2 weeks ago

You corrected yourself below. So, just for the ones reading, correct answer is C

upvoted 4 times

maj79 1 year ago

Correction : hence answer C is correct

upvoted 11 times

David_986969 1 year, 1 month ago

Application ecurity group is assign at the resource group level

upvoted 1 times

Anamak2 1 year 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 17 times

gboyega Highly Voted 1 year ago

C is Correct
They are part of the Same VNET
Confirmed in the Lab

https://t.me/learningnets

upvoted 18 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 2 times

MarioMK 1 month, 4 weeks 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 months, 2 weeks ago

C is correct. Vnet1 has subnet11 and 12

upvoted 4 times

scarw7 6 months, 1 week ago

same typo in explanation at vcpguide. who is copying from whom? :-)

upvoted 1 times

AzureGurl 6 months, 1 week ago

ASG is only applicable on VNet Level. Hence Answer is correct.

upvoted 4 times

azsblearner 6 months, 2 weeks ago

In the exam

upvoted 6 times

Danish12 7 months ago

Answer is correct!

upvoted 2 times

Bluediamond 10 months, 1 week ago

C 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

eug45 11 months, 2 weeks ago

correct C

Application Security Groups are a region-specific resource. It can only be associated with NICs in the same region as the application security group. And once you associate an application security group with one network interface in an Azure virtual network, the application security group can only be associated with network interfaces in the same Azure virtual network.

upvoted 2 times

gfhbox0083 1 year ago

C for sure,
Part of the same Vnet

upvoted 6 times

lnn_az 1 year, 1 month ago

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 NIC1 assigned to an application security group named ASG1 is in the virtual network named VNET1, then all subsequent network interfaces assigned to ASG1 must exist in VNET1. so NIC2 and NIC3 (which is associated with Subnet11 and Subnet12 under VNET1) is the correct answer.

You cannot add network interfaces from different virtual networks to the same application security group

upvoted 6 times

farslayer9 1 year, 1 month ago

C is correct, ASGs exist in the same VNET, not subnet.
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

upvoted 5 times

SadioMane 1 year, 1 month ago

Yup. Answer is C.

upvoted 3 times

Borris69 1 year, 2 months ago

C. is correct answer

upvoted 11 times

https://t.me/learningnets

Prash85 1 year, 2 months ago
A is the correct answer.
upvoted 2 times

xaccan 3 months, 2 weeks ago
go study, cert won't help you
upvoted 1 times

AS007 1 year, 2 months ago
Same subnet - correct is A
upvoted 1 times

vlq 1 year, 2 months ago
Same VNET, not Subnet - so C. is correct answer
upvoted 19 times

levo017 10 months, 3 weeks ago
ASG operates within the boundary of NSG, which operates on Subnet.
upvoted 1 times

levo017 10 months ago
Ignore my previous comment. ASG has be in boundary of VNet, not Subnet.
upvoted 1 times

https://t.me/learningnets

Question #53 *Topic 2*

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.

Correct 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

kristiann21 Highly Voted 1 year, 1 month ago
correct answer
upvoted 23 times

gboyega Highly Voted 1 year ago
B is Correct
upvoted 9 times

AndreasF Most Recent 3 months, 1 week ago
https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application
"No enforcement options are currently available".
This feature cannot therefore be used to prevent
upvoted 1 times

zic04 5 months, 3 weeks ago
B correct
upvoted 3 times

tuta 7 months ago
Correct ans = B
upvoted 4 times

SadioMane 1 year, 1 month ago
Answer B is the answer
upvoted 7 times

https://t.me/learningnets

Question #54 *Topic 2*

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.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements

Coldriver Highly Voted 5 months, 1 week 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 20 times

deegadaze1 Highly Voted 4 months, 2 weeks ago
It was in Exam
upvoted 11 times

Deepmindx Most Recent 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 3 times

DCarma 3 weeks, 1 day ago
Triple-DES? Bloody hell what year is this? Haven't used that since it was claimed to be 'legacy' almost 10 years ago. Still, it's the correct answer for this one.
upvoted 3 times

kumax 3 weeks, 4 days ago
On exam, May 2021.
upvoted 2 times

Priv09 3 weeks, 5 days ago
correct answer. option B.
Private certificate requirements:
Azure Web Apps does not support AES256 and all pfx files should be encrypted with TripleDES.
upvoted 2 times

bpank 2 months, 2 weeks ago
why would it not be option D?
upvoted 1 times

bpank 2 months, 2 weeks ago
web app does not support AES256. thank you
upvoted 5 times

Kinanke 4 months, 3 weeks ago
correct. https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements
upvoted 3 times

https://t.me/learningnets

Question #55 *Topic 2*

You plan to deploy Azure container instances.
You have a containerized application that validates credit cards. The application 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

Correct 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

gfhbox0083 Highly Voted 1 year ago
D, for sure.
Using Container Group
upvoted 24 times

msftman Highly Voted 6 months, 3 weeks ago
on test
upvoted 15 times

Fred64 Most Recent 2 months, 3 weeks ago
D
all the other one are Azure concepts
upvoted 2 times

milad123 5 months ago
correct
upvoted 5 times

kristiann21 1 year, 1 month ago
correct answer.
upvoted 10 times

https://t.me/learningnets

Question #56 *Topic 2*

DRAG DROP -

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

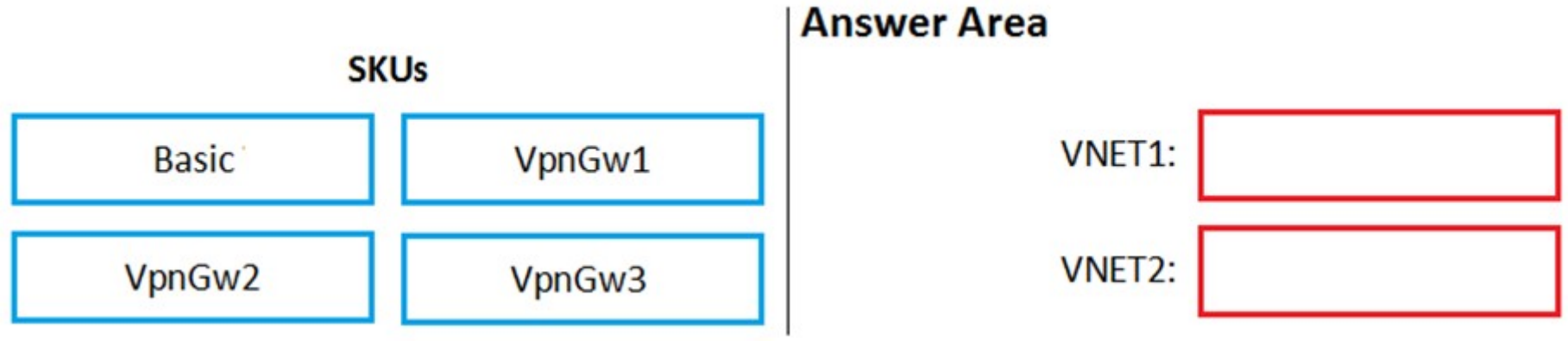
You need to implement VPN gateways for the virtual networks to meet the following requirements:

- 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.

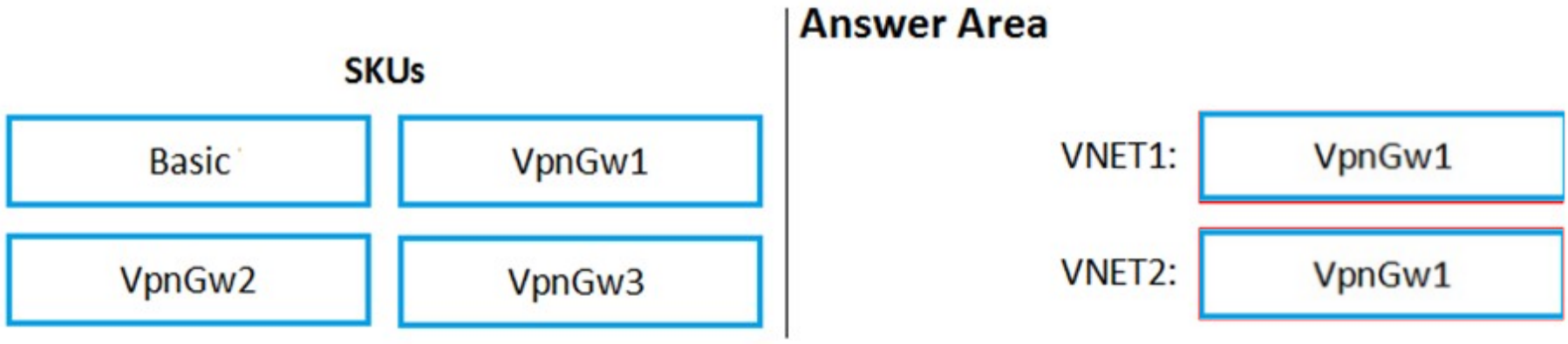
Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



References:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

nihao381 Highly Voted 4 months ago

Correct, as BGP is not supported in the Basic SKU.

upvoted 12 times

souvik123 2 months, 2 weeks ago

Any reference for BGP not supported in Basic SKU?

upvoted 1 times

SandroAndrade 1 month, 3 weeks ago

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

upvoted 2 times

nicksu 1 month, 3 weeks 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 1 times

Fred64 Highly Voted 2 months, 2 weeks ago

in real life, do you kno someone learning things like that for every sazure service?

upvoted 10 times

whysohardwhy 2 weeks ago

"remember they are just exams, don't argue with them"

upvoted 1 times

kimalto452 4 weeks ago

yes, you for example :D

upvoted 1 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago

https://t.me/learningnets

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways
upvoted 1 times

JohnYinToronto 3 months, 3 weeks ago
Answers correct
upvoted 3 times

Question #57

Topic 2

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

Correct Answer: *B*

JohnYinToronto Highly Voted 3 months, 3 weeks ago
answer correct
upvoted 15 times

https://t.me/learningnets

Question #58 *Topic 2*

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 â€" 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.	○	○

Answer Area No,No,Yes

Statements	Yes	No
Correct Answer: 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.

gcpbrig01 Highly Voted 4 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

https://t.me/learningnets

account in the firewall section of the storage account.

upvoted 12 times

rgullini 2 months, 2 weeks 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 3 times

rgullini 2 months, 2 weeks ago

Agree with you. Answers are correct

upvoted 1 times

hmghmg 2 months, 3 weeks ago

Yes, but not on the same Azure region.
The answer is: NO,NO,NO

upvoted 2 times

canonigo Highly Voted 3 months, 3 weeks ago

For me it's NO, NO, NO.

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.
Services deployed in the same region as the storage account use private Azure IP addresses for communication. Thus, you cannot restrict access to specific Azure services based on their public outbound IP address range.
https://docs.microsoft.com/es-es/azure/storage/common/storage-network-security?tabs=azure-portal

upvoted 8 times

Madball Most Recent 6 days, 13 hours ago

I am rather confused by this one, I have created a test environment to match the settings. The one thing to point out is that when you attempt to add VNET3/Subnet3 to the selected networks for the storage account it will ask you to enable the service endpoint Microsoft.Storage.

I then created a file share on the storage account for testing purposes.

Results
VM1 = Unable to access the file share from the Azure Portal.
VM2 = Unable to access the file share from the Azure Portal.
VM3 = I am able to access the file share from the Azure Portal (Only if I enable service endpoint Microsoft.Storage on subnet3, otherwise I cannot access it).

If I am doing something wrong then please say, otherwise I feel the answer would be either No, No, No or No, No, Yes depending on what you do with VNET3/Subnet3.

upvoted 1 times

MarioMK 1 month, 3 weeks ago

NYY
Q1: No. IP for VM1 is excluded from the firewall settings. Hence, no access will be allowed from this VM.
Q2: No endpoint present on the subnet. However, access from the VM public IP address is allowed.
Q3:Even though the service endpoint is not enabled for the subnet, once you try to add the selected subnet to the firewall settings, a little pop up will be shown saying the following: "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." Therefore, answer should be Yes.

upvoted 1 times

nicksu 1 month, 3 weeks ago

I think it should be N Y Y

When enabling access from VNET3/Subnet3 the service endpoint is to be automatically created

"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."

upvoted 2 times

Lb83 2 months, 1 week ago

Just be aware that when the firewall rule gets added to the storage account to enable the access for vnet3 it automatically enables the service endpoint on the network.

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

you need a service endpoint with a vnet

upvoted 2 times

glowglow 3 months, 2 weeks ago

https://t.me/learningnets

should be No, Yes, Yes, correct?

⇨ Allow access from: Selected networks
⇨ Virtual networks: VNET3\Subnet3
Firewall ג€" Address range: 52.233.129.0/24

upvoted 2 times

Firedragon 2 months, 3 weeks ago

Agree. When adding VNET3\Subnet3, it'll ask you to Enable the Storage service endpoints or you can't even add the subnet. so, it's Yes.
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.

upvoted 2 times

cannibalcorpse 3 months, 1 week ago

Subnet3 does not have service endpoint for storage. So it should be NO

upvoted 2 times

macco455 3 months, 3 weeks ago

Yes VM is in same region and has a service endpoint to access the storage account
Yes, VM is in same region and allowed thru the public IP based on network rule
Yes, VM is in same region and allowed based on subnet 3 being allowed

This is my $.02, feel free to correct if wrong

upvoted 2 times

3abmula 1 month, 2 weeks ago

I have tested on Lab, wasn't expecting this result, but you're right.
Answer Yes, Yes, Yes

upvoted 1 times

3abmula 1 month, 2 weeks ago

Sorry, please ignore, I think macco455 has done the same mistake I have done. I was able to connect successfully but I didn't test do any tasks, but did later and wasn't able to list blob containers except from VM3. IP rules doesn't seem to work, only service end points.
It's No, No, Yes.

upvoted 1 times

macco455 3 months, 3 weeks ago

Also, the logic on the answers seems off. It says on one line that no endpoint is configured but traffic is allowed from public IP, but on next like it says traffic is allowed from vnet but no service endpoint is configured. Seems a bit contradictory to me, unless u need service endpoints configured from inside the vnet but not outside??? Just doesn't seem logical

upvoted 1 times

rgullini 2 months, 2 weeks 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 1 times

dadageer 4 months ago

answers correct

upvoted 3 times

https://t.me/learningnets

Question #59 *Topic 2*

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.

Save Discard Upload Download

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

Correct 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

Deepmindx Highly Voted 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 7 times

JohnYinToronto Most Recent 3 months, 3 weeks ago

answer correct

upvoted 4 times

dadageer 4 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)

https://t.me/learningnets

```
# Update the application group membership claims
az ad app update --id $serverApplicationId --set groupMembershipClaims=All
```

upvoted 4 times

gcpbrig01 4 months ago

groupMembershipClaims should be set to "All"

upvoted 4 times

https://t.me/learningnets

Question #60 Topic 2

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.	○	○

https://t.me/learningnets

Correct 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 λ€˜anyλ€™ traffic on λ€˜anyλ€™ 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 donλ€™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 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 11 times

Cyberbug2021 2 months, 1 week ago
Peered yes but what about rule 160 - any any deny
upvoted 1 times

BalderkVeit 1 month, 3 weeks 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 1 times

rgullini 2 months, 3 weeks ago
Agree with your comments and the answers.
upvoted 1 times

hydrillo Most Recent 3 weeks, 3 days 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 1 times

kumax 3 weeks, 4 days ago
On exam, May 2021.
upvoted 3 times

AMMANANA 2 months 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 3 times

nicksu 1 month, 3 weeks ago
There is no peering between VNET2 & VNET4. The VM4 does have the PIP, but the ICMP from Internet is not allowed
upvoted 1 times

Fred64 2 months ago
the technique is always the same:
1) Check feasability:
if VNET are peared they can communicate with private IP
if not one must use public IP, that mean both side should have one

If feasability is OK on check permission with NSG
upvoted 2 times

https://t.me/learningnets

cybul7 2 months, 1 week ago

B should be Yes.
VM4 has public IP, and there is no outboud rule to block ping from VM2 (we don't need to have public IP addess for VM2 to make a ping command to public ip)

upvoted 2 times

Fred64 2 months, 2 weeks ago

Whatever the question its easy to see that NSG never block. So it is now a question of connectivity.
We access either from public IP if there is public IP either from private IP if same vnet or peered vnet.

box 1: vm1 and vm3 are peered, so its Y
box 2: vm2 and vm4 not peered. So check public IP. VM4 has a public IP but not VM2. So NSG
box 3: the question is focussed by public acces, so public IP. VM3 has a public IP. So Y

upvoted 1 times

macco455 3 months, 3 weeks ago

Agree with answers

upvoted 3 times

JohnYinToronto 3 months, 3 weeks ago

answers correct

upvoted 3 times

Topic 3 - Question Set 3

https://t.me/learningnets

Question #1 *Topic 3*

SIMULATION -

A user named Debbie has the Azure app installed on her mobile device.

You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

You need to configure an alert rule in Azure Monitor.

1. Type Monitor into the search box and select Monitor from the search results.
2. Click on Alerts.
3. Click on +New Alert Rule.
4. In the Scope section, click on the Select resource link.
5. In the Filter by resource type box, type locks and select Management locks (locks) from the filtered results.
6. Select the subscription then click the Done button.
7. In the Condition section, click on the Select condition link.
8. Select the Delete management locks condition the click the Done button.
9. In the Action group section, click on the Select action group link.
10. Click the Create action group button to create a new action group.
11. Give the group a name such as Debbie Mobile App (it doesnג€™t matter what name you enter for the exam) then click the Next: Notifications > button.
12. In the Notification type box, select the Email/SMS message/Push/Voice option.
13. In the Email/SMS message/Push/Voice window, tick the Azure app Push Notifications checkbox and enter debbie@contoso.com in the Azure account email field.
14. Click the OK button to close the window.
15. Enter a name such as Debbie Mobile App in the notification name box.
16. Click the Review & Create button then click the Create button to create the action group.
17. Back in the Create alert rule window, in the Alert rule details section, enter a name such as Management lock deletion in the Alert rule name field.
18. Click the Create alert rule button to create the alert rule.

Banzaaai 2 months, 3 weeks ago

how does Simulations look on exam ?

upvoted 3 times

3abmula 1 month, 2 weeks ago

It's more like a real lab, a browser that's allowed only to access portal.azure.com. But as exam takers, no labs appeared in AZ-500 for over a year.

upvoted 1 times

JohnYinToronto 3 months, 3 weeks ago

answer correct

upvoted 1 times

https://t.me/learningnets

Question #2 *Topic 3*

You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?

A. Azure Storage Explorer

B. SQL query editor in Azure

C. File Explorer in Windows

D. Azure Security Center

Correct Answer: *A*
If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables.
You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name.
Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).
Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

Note:
There are several versions of this question in the exam. The questions in the exam have two different correct answers:
1. Azure Storage Explorer
2. AZCopy
Other incorrect answer options you may see on the exam include the following:
1. Azure Monitor
2. The Security & Compliance admin center
3. Azure Cosmos DB explorer
4. Azure Monitor
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json
https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers

Deepmindx 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 1 times

Fred64 2 months, 2 weeks ago
answer correct : A
upvoted 4 times

Pinto 3 months, 4 weeks ago
https://docs.microsoft.com/en-us/azure/storage/common/manage-storage-analytics-logs?tabs=azure-portal#enable-logs
upvoted 3 times

eroms 1 month, 2 weeks ago
Not relevant!
upvoted 1 times

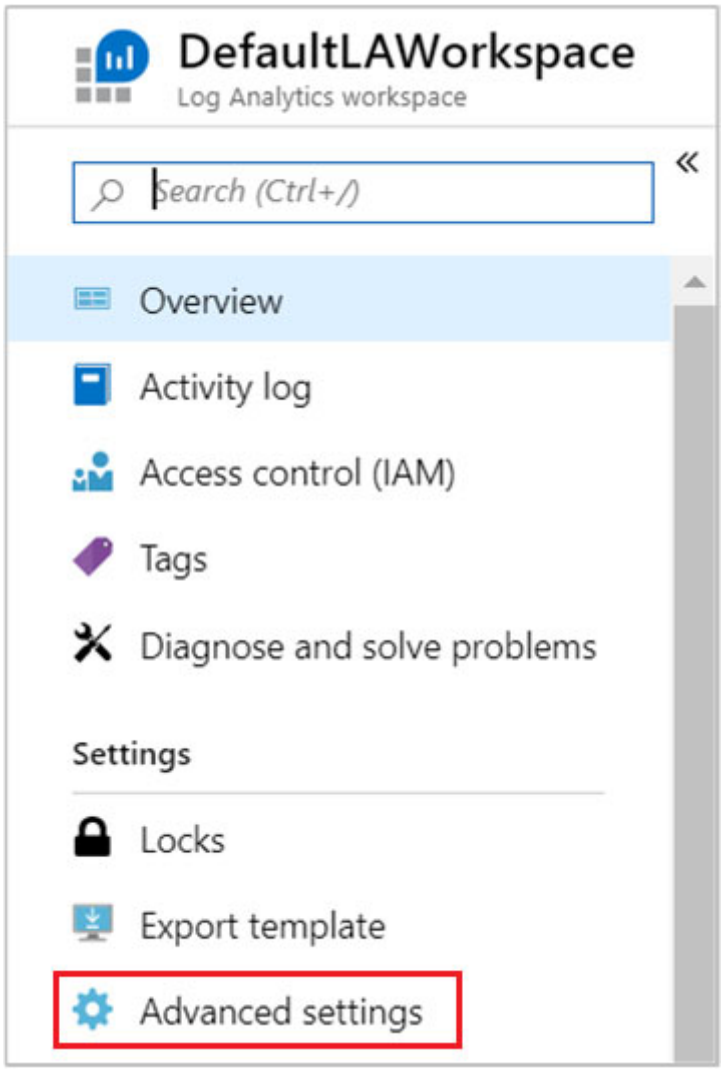
https://t.me/learningnets

Question #3 *Topic 3*

SIMULATION -
You plan to connect several Windows servers to the WS11641655 Azure Log Analytics workspace.
You need to ensure that the events in the System event logs are collected automatically to the workspace after you connect the Windows servers.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Correct Answer: *See the explanation below.*
Azure Monitor can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.

Data collection from Windows VM -
1. In the Azure portal, locate the WS11641655 Azure Log Analytics workspace then select Advanced settings.



2. Select Data, and then select Windows Event Logs.
3. You add an event log by typing in the name of the log. Type System and then select the plus sign +.
4. In the table, check the severities Error and Warning. (for this question, select all severities to ensure that ALL logs are collected).
5. Select Save at the top of the page to save the configuration.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

Fred64 2 months, 3 weeks ago
https://docs.microsoft.com/en-us/azure/azure-monitor/vm/quick-collect-azurevm#enable-the-log-analytics-vm-extension

Don't forget to connect vm to log analytics
upvoted 1 times

dadageer 4 months ago
No longer under advanced settings. You need to configure it from 'Agents configuration'
upvoted 3 times

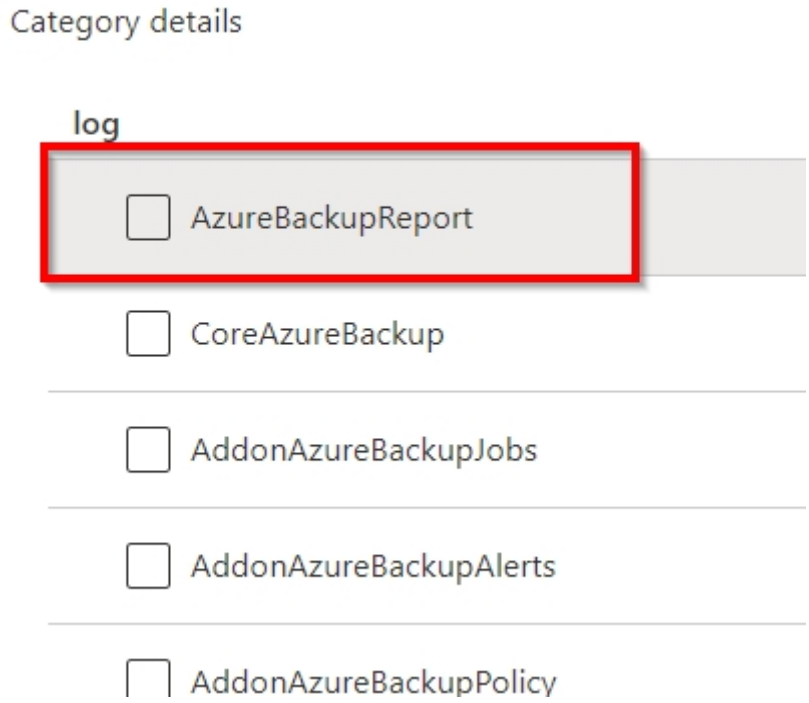
OhBee 3 months, 1 week ago
Correct ^^
upvoted 1 times

https://t.me/learningnets

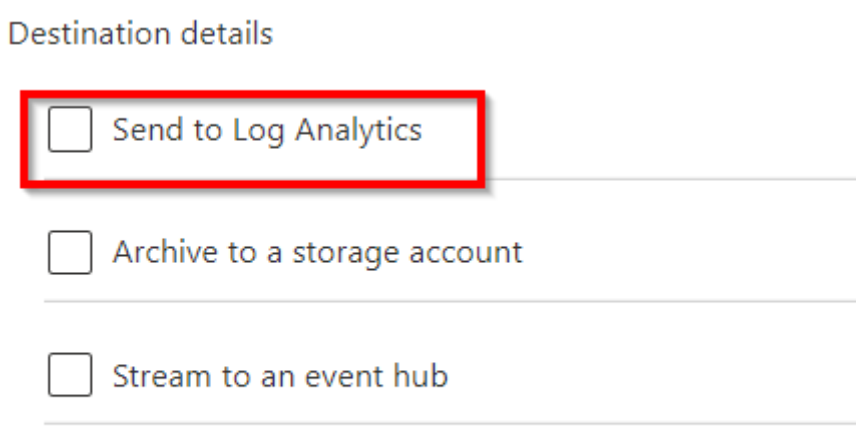
Question #4 *Topic 3*

SIMULATION -
You need to ensure that the AzureBackupReport log for the Vault1 Recovery Services vault is stored in the WS11641655 Azure Log Analytics workspace.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Correct Answer: *See the explanation below.*
1. In the Azure portal, type Recovery Services Vaults in the search box, select Recovery Services Vaults from the search results then select Vault1.
Alternatively, browse to Recovery Services Vaults in the left navigation pane.
2. In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.
3. Click the Add a diagnostic setting link.
4. Enter a name in the Diagnostic settings name box.
5. In the Log section, select AzureBackupReport.



6. In the Destination details section, select Send to log analytics



7. Select the WS11641655 Azure Log Analytics workspace.
8. Click the Save button to save the changes.
Reference:
https://docs.microsoft.com/en-us/azure/backup/backup-azure-diagnostic-events

dadageer 4 months ago
This has now changed and you no longer get an option to select 'type' of logs.
upvoted 1 times

OhBee 3 months, 1 week ago
I can still see this though...are you sure about that ?
upvoted 2 times

https://t.me/learningnets

Question #5 *Topic 3*

SIMULATION -

You need to ensure that the audit logs from the SQLdb1 Azure SQL database are stored in the WS11641655 Azure Log Analytics workspace.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Correct Answer: *See explanation below.*

1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the Security section and select Auditing.
3. Turn auditing on if it isnλ€™t already, tick the Log Analytics checkbox then click on Configure.

4. Select the WS11641655 Azure Log Analytics workspace.
5. Click Save to save the changes.

https://t.me/learningnets

Question #6 *Topic 3*

HOTSPOT -

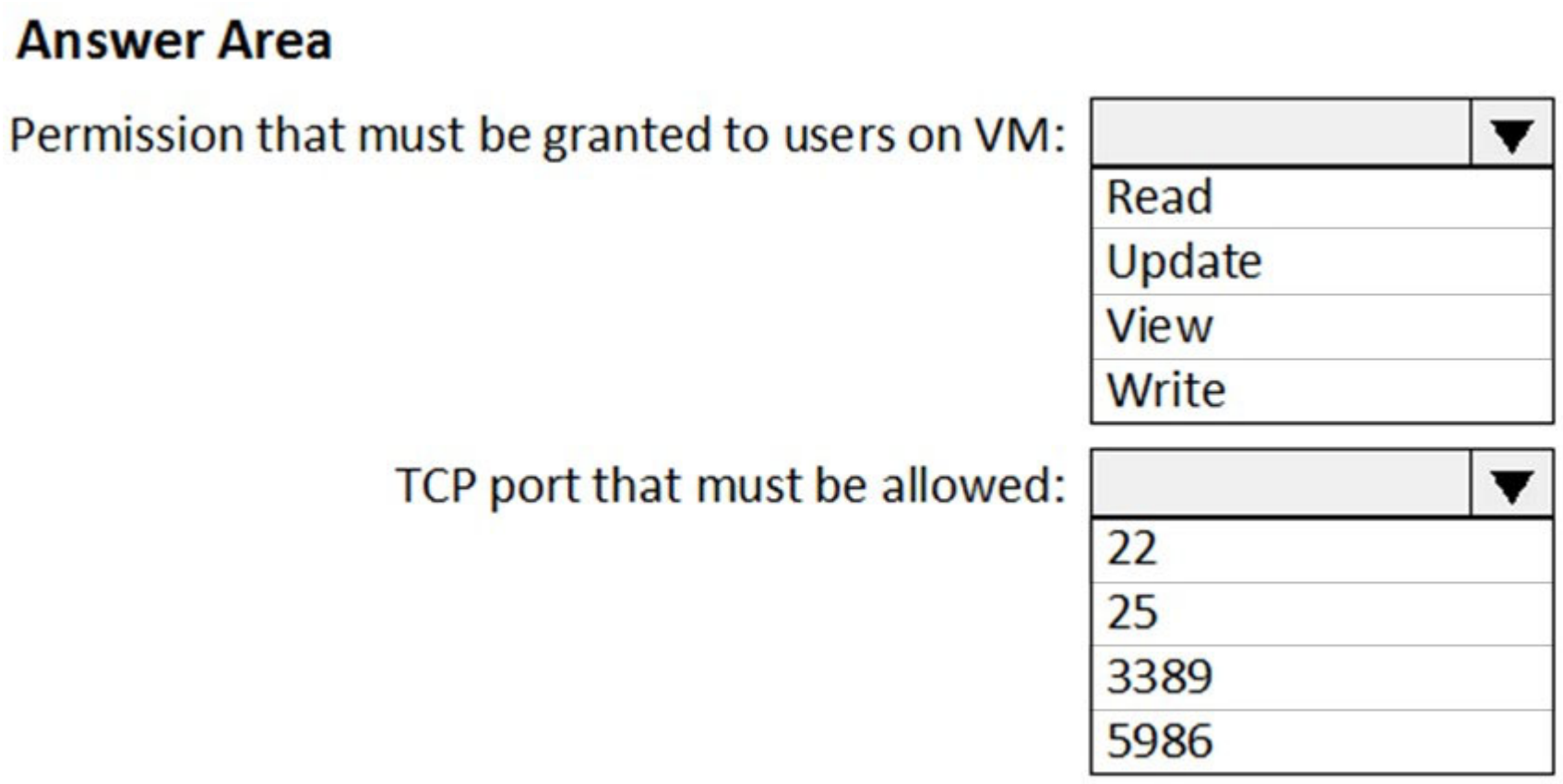
You are configuring just in time (JIT) VM access to a Windows Server 2019 Azure virtual machine.

You need to grant users PowerShell access to the virtual machine by using JIT VM access.

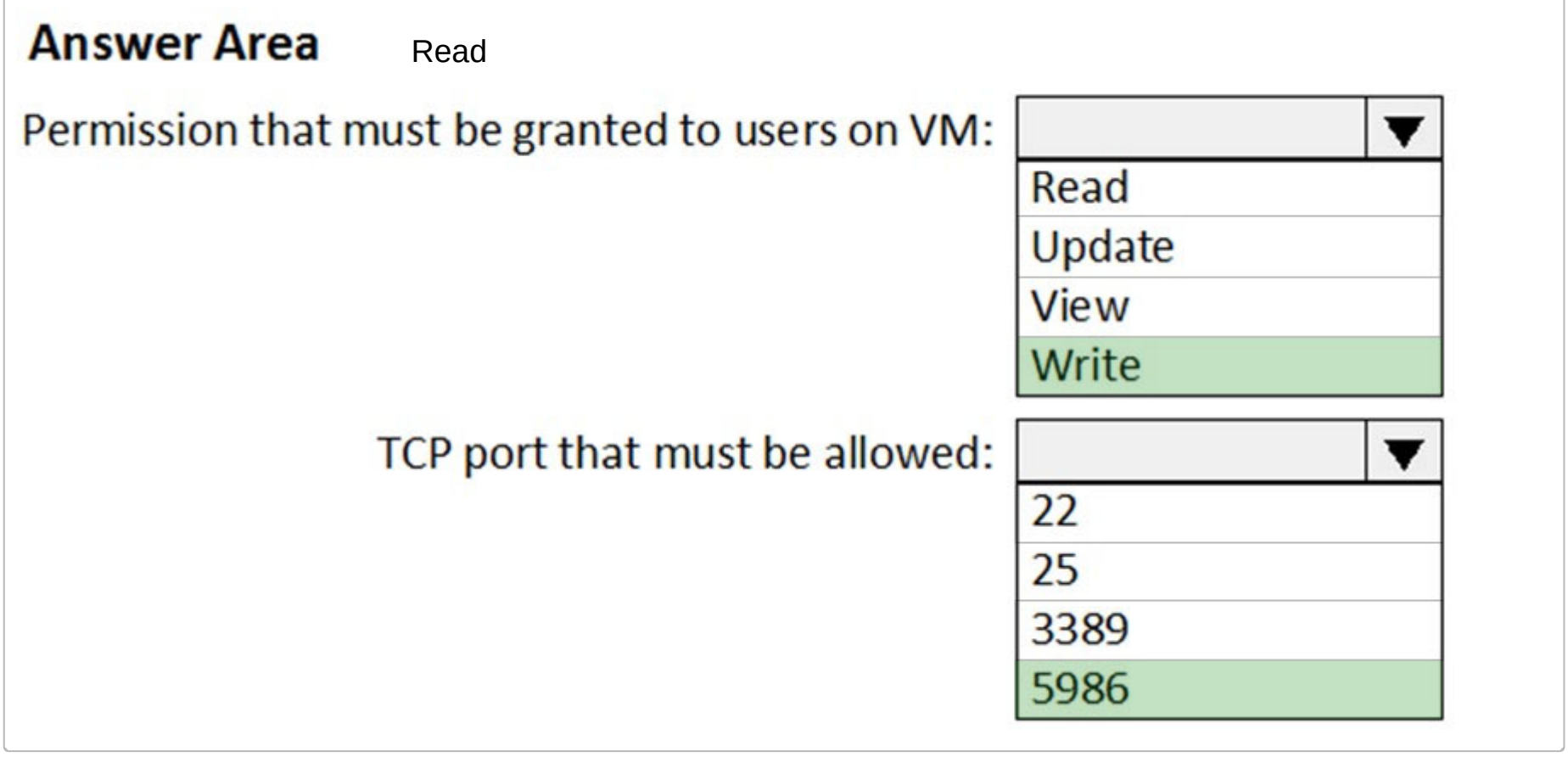
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



jpons 2 weeks ago

Port is ok, but access is Read
https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained#what-permissions-are-needed-to-configure-and-use-jit

upvoted 2 times

Joillane 2 weeks ago

First one should be Read

upvoted 2 times

https://t.me/learningnets

Question #7 *Topic 3*

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Region	Resource group
SQL1	Azure SQL database	East US	RG1
Analytics1	Azure Log Analytics workspace	East US	RG1
Analytics2	Azure Log Analytics workspace	East US	RG2
Analytics3	Azure Log Analytics workspace	West Europe	RG1

You create the Azure Storage accounts shown in the following table.

Name	Region	Resource group	Storage account type	Access tier (default)
Storage1	East US	RG1	Blob	Cool
Storage2	East US	RG2	General purpose V1	*Not applicable*
Storage3	West Europe	RG1	General purpose V2	Hot

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Storage accounts that can be used as the audit log destination:
- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:
- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Correct Answer:

Answer Area Storage1 and Storage2 only

Storage accounts that can be used as the audit log destination:
- Storage1 only
- **Storage2 only**
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:
- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- **Analytics1, Analytics2, and Analytics3**

pravinjin Highly Voted 4 months ago

Storage 1 and 2
https://docs.microsoft.com/en-us/azure/azure-sql/database/audit-log-

https://t.me/learningnets

format#:~:text=Blob%20audit,in%20the%20Azure%20storage%20account.
Log analytics 1,2 and 3

upvoted 19 times

rraviska 2 months, 3 weeks ago

Storage needs to be in same region (East US). Hence Storage - Storage1 and Storage2 only.
Log Analytics can be in any region. Hence it can be Storage1, Storage2 or Storage3

upvoted 6 times

dadageer 4 months ago

agreed tested

upvoted 3 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 3 times

JagannathChellappa 1 month, 1 week ago

Box 1 - Storage 1 and Storage 2 [as SQL is in EAST US Region - the storage must be on the same region]
Box 2 - Analytics 1, 2 and 3 [Log Analytics Workspace can be at any location]

upvoted 2 times

3abmula 1 month, 2 weeks ago

Tested, works with both Storage 1 (Blob, Cool Tier) and Storage 2 (GPv1).
Answer for box1: Storage1 and Storage2 only.

upvoted 2 times

Keem 1 month, 2 weeks ago

impliedly, the storage for log Analytics will be frequently accessed. as such storage 1 "cool tie" is out of it. even though it is in the same region (East US) correct answer =storage 2 only

upvoted 2 times

dfernandes 4 days, 6 hours ago

i agree with it.
the same question appeared in Az-301 past year

upvoted 1 times

roy9889 2 months, 1 week ago

I d have to disagree with "pravinjin"
I believe the original solution given is CORRECT
Storage 1 is of COOL TIER (so it cannot store audit logs as audit logs need to seen regularly)

upvoted 2 times

Neonlight8 1 month, 3 weeks ago

Box 1: Storage 1 and Storage 2 only. Audit log destination has to be the same Region as SQL1. East US has Blob and GPv1, both works.

Blob - Allows writing to log files https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-overview

GPv1 - supports Blob, Queue, and Table storage, Azure Files
https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview

Cool Tier - Optimized for storing data that is infrequently accessed and stored for at least 30 days. Question did not mention how often the audit logs are accessed so this is usable https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

Box 2: Analytics1, 2 ,3 - Log analytics workspace can be in any region

upvoted 3 times

MiAZBA 2 months, 2 weeks ago

I Think it's Storage 1 only ,
Storage2 is a General Purpose v1 (GPv1) and it don't support tiering.
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#storage-accounts-that-support-tiering

upvoted 1 times

glowglow 3 months, 2 weeks ago

It's because of the storage2 version "GPV1"
General Purpose v1 (GPv1) accounts don't support tiering.

upvoted 1 times

Pinto 3 months, 4 weeks ago

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

upvoted 2 times

gcpbrig01 4 months ago

I get the log analytics part- it is subscription/resource-group/location agnostic. I dont get the part where storage 1 and 2 are chosen.

upvoted 2 times

gcpbrig01 4 months ago

ok. since both storage accounts are in same region as the sql database maybe?

https://t.me/learningnets

upvoted 2 times

https://t.me/learningnets

Question #8 *Topic 3*

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.

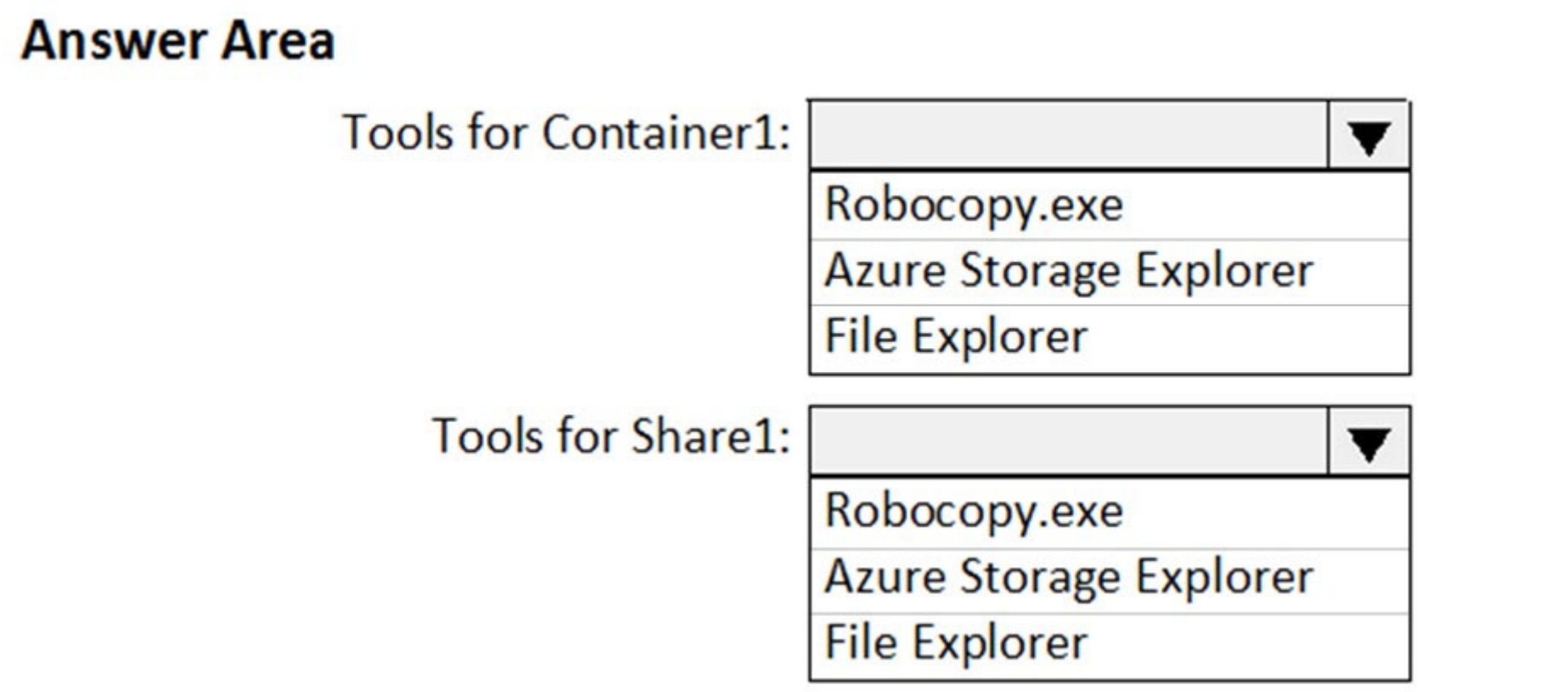
Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

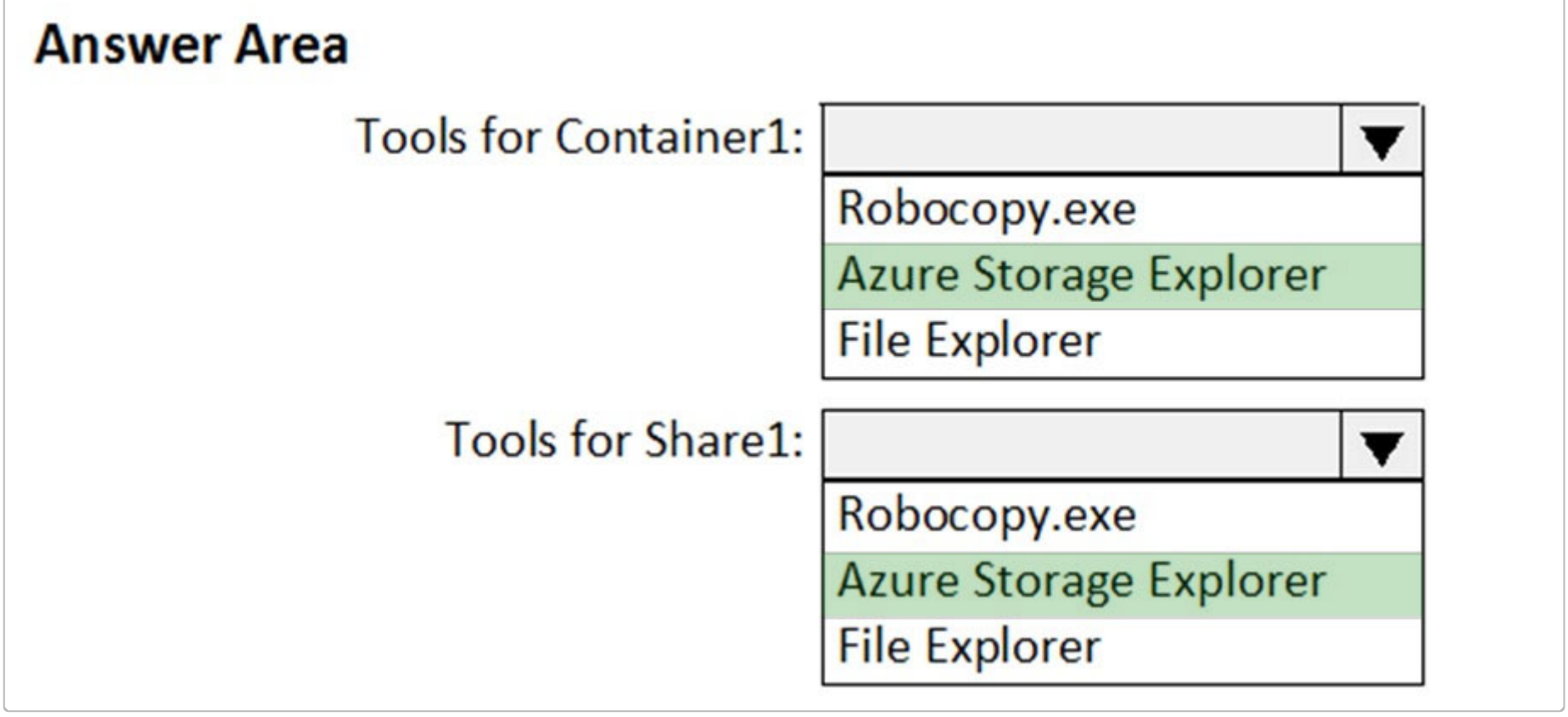
Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Cisna Highly Voted 2 months, 1 week ago
in exam 02/05/2021
upvoted 8 times

Rajesh123 Most Recent 1 month, 1 week ago
Azure Storage Explorer = Which tool using the SAS
upvoted 1 times

JerryGolais 2 months, 3 weeks ago

https://t.me/learningnets

- Azure Storage Explorer
This one is simple enough.
- Azure Storage Explorer
You do not map a file share from azure with SAS. You can use SAS with storage explorer though.
https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows#mount-the-azure-file-share

upvoted 3 times

sukhdeep 3 months, 2 weeks ago

why we can't use File explorer for share1 ? I have share on Azure which I access from file explorer as network drive.

upvoted 2 times

Sitender 2 months, 4 weeks ago

Windows file explore can't authenticate with Azure. you can only access normal share on same NW

upvoted 2 times

JAGUDERO 3 months, 1 week ago

the question says "Which tool can you use"

upvoted 3 times

JohnYinToronto 3 months, 3 weeks ago

answers correct
https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows

upvoted 4 times

Sethoo 3 months, 3 weeks ago

Azure storage explorer lets you Upload, download, and manage Azure blobs, files, queues, and tables, as well as Azure Cosmos DB and Azure Data Lake Storage entities. Easily access virtual machine disks, and work with either Azure Resource Manager or classic storage accounts. Manage and configure cross-origin resource sharing rules.
Given answer appear correct

upvoted 3 times

https://t.me/learningnets

Question #9 *Topic 3*

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.

Correct Answer: *B*
References:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal

romanaa Highly Voted 11 months ago
so many repetitions
upvoted 13 times

kiketxu 9 months, 3 weeks ago
agree!
upvoted 5 times

kumax Highly Voted 3 weeks, 3 days ago
On exam, May 2021.
upvoted 5 times

arytech Most Recent 2 weeks, 4 days 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 1 times

mayenite 5 months, 2 weeks ago
Given answer is correct
upvoted 4 times

https://t.me/learningnets

Question #10 *Topic 3*

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

Correct Answer: *B*

fpspam Highly Voted 11 months, 3 weeks ago
I think this is correct. Source: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview
upvoted 11 times

Rajesh123 Most Recent 1 month ago
ALA can store logs from 30 to 730 days (2 years)
upvoted 1 times

JohnYinToronto 3 months, 3 weeks ago
answer correct
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace
upvoted 3 times

deegadaze1 4 months, 2 weeks ago
in Exam
upvoted 4 times

tuta 7 months ago
this page has too many repeatitions
upvoted 3 times

https://t.me/learningnets

Question #11 *Topic 3*

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.

Correct Answer: *B*

Elpresidento27 Highly Voted 4 months, 2 weeks 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 12 times

sureshatt 3 months, 2 weeks 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 3 times

111ssy Highly Voted 11 months ago
Correct answer: B
upvoted 11 times

James79 Most Recent 1 month ago
Another example of a microsoft question where you can make solid arguments for 3 of the 4 answers....
upvoted 1 times

kra96 2 months ago
Given answer is right. https://github.com/uglide/azure-content/blob/master/articles/application-insights/app-insights-monitor-web-app-availability.md
upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago
https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
I think the answer is A - you do need to use visual studio before uploading the file to insights
upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago
"Developers at the company PLAN to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1."

The plan is to create - not created yet, what do you do first. you cannot register something that has not been created yet
upvoted 1 times

teamaws 3 months, 1 week ago
Going with C, this is a security test, not development. The Developer Associate test would have a different perspective related to what's in the code!
upvoted 2 times

juandiegope 3 months, 3 weeks ago
Right Ans.. This is the documentation:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep

1 Step: Upload the web test
upvoted 1 times

nothankyouspankyou 6 days, 17 hours ago

https://t.me/learningnets

Unbelievable they would have a question like this. At the bottom of that doc:
If 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....
So you dont get the token from AAD.
A has to be the right answer.

upvoted 1 times

deegadaze1 4 months, 2 weeks ago

in Exam

upvoted 9 times

seconazure 4 months, 2 weeks ago

if we think as a security guy C should be the correct ans !

upvoted 2 times

milind8451 4 months, 2 weeks ago

Right ans.

upvoted 2 times

kiranmai 5 months ago

Repeated. The answer is correct

upvoted 3 times

Question #12 *Topic 3*

You have an Azure subscription named Subscription1.
You deploy a Linux virtual machine named VM1 to Subscription1.
You need to monitor the metrics and the logs of VM1.
What should you use?

A. the AzurePerformanceDiagnostics extension

B. Azure HDInsight

C. Linux Diagnostic Extension (LAD) 3.0

D. Azure Analysis Services

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-linux

M4gnet1k Highly Voted 10 months, 2 weeks ago

Given answer is correct.

upvoted 14 times

ipindado2020 Highly Voted 9 months, 1 week ago

Agree with C

upvoted 5 times

adsdadasdad Most Recent 1 week, 2 days ago

has to be A, got the question in the az-204 exam and now again .its A

upvoted 1 times

nothankyouspankyou 6 days, 17 hours ago

A isn't for Linux, only Windows.

upvoted 1 times

https://t.me/learningnets

Question #13 *Topic 3*

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.
You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.
What should you create?

A. an alert rule

B. a playbook

C. a function app

D. a runbook

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Teesmd Highly Voted 10 months, 2 weeks ago
Provided answer (Playbook) is correct
upvoted 18 times

mayenite Highly Voted 5 months ago
In exam
upvoted 9 times

Deepmindx Most Recent 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 3 times

strawberries 6 months, 3 weeks ago
correct
upvoted 2 times

KitiMan 10 months, 2 weeks ago
Correct answer
upvoted 6 times

https://t.me/learningnets

Question #14 *Topic 3*

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:

- Retain logs for two years.
- Query logs by using the Kusto query language.
- Minimize administrative effort.

Where should you store the logs?

A. an Azure event hub

B. an Azure Log Analytics workspace

C. an Azure Storage account

Correct Answer: *B*

jbuenoo Highly Voted 10 months ago

I agree with answer:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries

upvoted 16 times

deegadaze1 Highly Voted 4 months, 2 weeks ago

in Exam

upvoted 9 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 4 times

HardcodedCloud 4 months, 2 weeks ago

B is the correct answer.
Data retention at the workspace level can be configured from 30 to 730 days (2 years) for all workspaces unless they are using the legacy Free pricing tier.

upvoted 4 times

v078 4 months, 2 weeks ago

B - correct. Worth mentioning, that you can also store logs in Storage Account and configure retention as well, but the keyword here is Kusto, you cannot use Kusto to query logs stored in storage account, I believe.

upvoted 6 times

Loga 7 months, 3 weeks ago

Agreed. B is the correct ans!

upvoted 2 times

awssecuritynewbie 9 months ago

basically sentinel

upvoted 1 times

https://t.me/learningnets

Question #15 *Topic 3*

You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?

A. the Security & Compliance admin center

B. Azure Security Center

C. Azure Cosmos DB explorer

D. AzCopy

Correct Answer: *D*
If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables.
You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name.
Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).
Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

Note:
There are several versions of this question in the exam. The questions in the exam have two different correct answers:
1. Azure Storage Explorer
2. AZCopy
Other incorrect answer options you may see on the exam include the following:
1. SQL query editor in Azure
2. File Explorer in Windows
3. Azure Monitor
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json
https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers

macco455 Highly Voted 3 months, 3 weeks ago
Answer is correct
https://docs.microsoft.com/en-us/azure/storage/common/manage-storage-analytics-logs?tabs=azure-portal#view-log-data
upvoted 5 times

GAP77 Most Recent 1 week, 3 days ago
Many storage-browsing tools enable you to download blobs from your storage account; you can also use the Azure Storage team provided command-line Azure Copy Tool AzCopy to download your log data.
upvoted 1 times

https://t.me/learningnets

Question #16 *Topic 3*

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Microsoft Monitoring Agent installed?

A. VM3 only

B. VM1 and VM3 only

C. VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

Correct Answer: *D*

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2,

2016, version 1709 and 1803.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-faq

Neonlight8 1 month, 3 weeks ago

https://docs.microsoft.com/en-us/azure/security-center/faq-data-collection-agents

Windows or Linux IaaS VMs qualify if:

The Log Analytics agent extension is not currently installed on the VM.
The VM is in running state.
The Windows or Linux Azure Virtual Machine Agent is installed.
The VM is not used as an appliance such as web application firewall or next generation firewall

upvoted 1 times

pal40sg 2 months ago

Right Answer:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

However, auto provisioning reduces management overhead by installing all required agents and extensions on existing - and new - machines

upvoted 2 times

Great1 3 months, 2 weeks ago

correct

upvoted 2 times

https://t.me/learningnets

Question #17 *Topic 3*

SIMULATION -
You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.
To complete this task, sign in to the Azure portal.

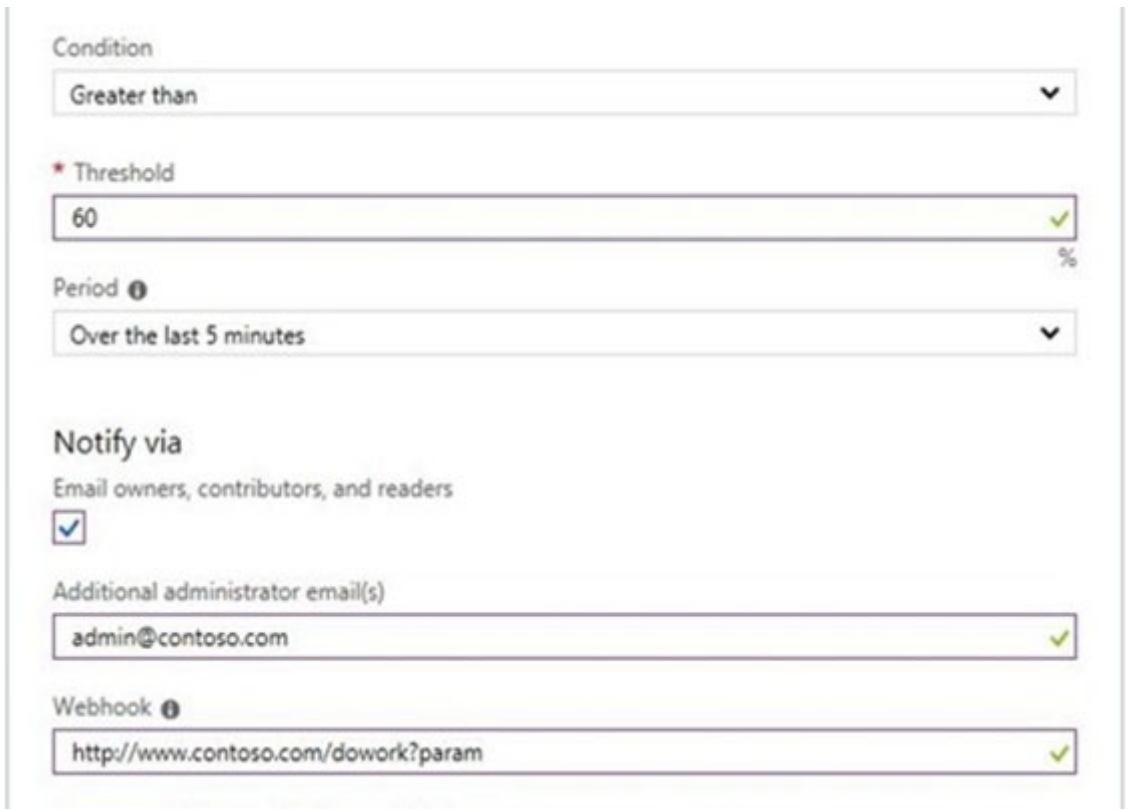
Correct Answer: *See the explanation below.*
Create an alert rule on a metric with the Azure portal
1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.
2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.

Metric: CPU Percentage -

Condition: Greater than -

Period: Over last 15 minutes -

Notify via: email -
Additional administrator email(s): admin1@contoso.com



Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal

kimalto452 3 weeks, 5 days ago
no that thing "alert classic" xD
upvoted 1 times

JhonyTrujillo 3 months, 3 weeks ago
az 500 ?
upvoted 3 times

https://t.me/learningnets

Question #18 *Topic 3*

SIMULATION -

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

To complete this task, sign in to the Azure portal.

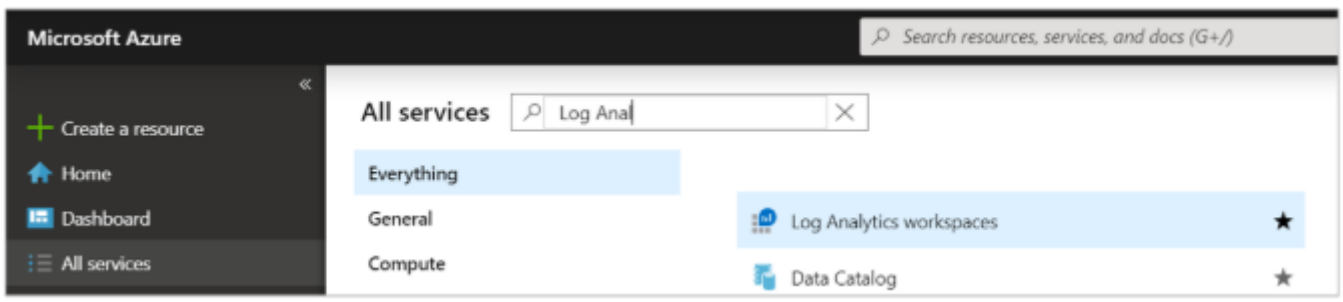
This task might take several minutes to complete You can perform other tasks while the task completes.

Correct Answer: *See the explanation below.*

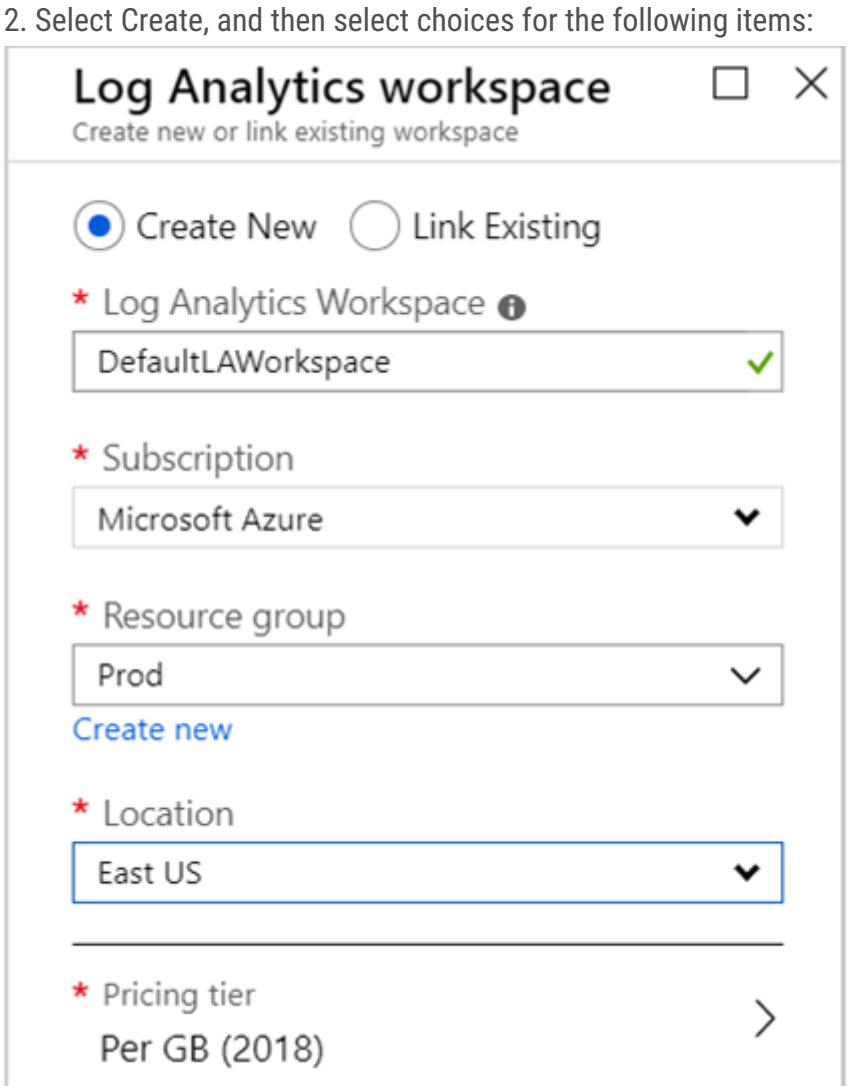
Step 1: Create a workspace -

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

1. In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.



2. Select Create, and then select choices for the following items:



3. After providing the required information on the Log Analytics workspace pane, select OK.

While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.

Step 2: Enable the Log Analytics VM Extension

Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.

1. In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.

2. In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).

3. On the left-hand menu, under Workspace Data Sources, select Virtual machines.

4. In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.

5. In the details for your virtual machine, select Connect. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the Status shows Connecting.

After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

dadageer Highly Voted 4 months ago

https://t.me/learningnets

Completely wrong solution.
Go to VM > Diagnostic Settings > Enable it > point to storage account
Under Logs check (Security > Audit Failure) is ticked

upvoted 35 times

macco455 3 months, 3 weeks ago

Agree, answer is wrong but dadageer is right.

upvoted 1 times

Laxreasoning 3 months, 3 weeks ago

that's the answer I was thinking off.. then to see Azure monitor, happy to see your answer and 6 upvotes

upvoted 1 times

sheva370 Most Recent 1 month ago

The given answer is wrong.

1. Open the menu for a virtual machine in the Azure portal.
2. Click on Diagnostic settings in the Monitoring section of the VM menu.
3. Click Enable guest-level monitoring if the diagnostics extension hasn't already been enabled.
4. A new Azure Storage account will be created for the VM with the name will be based on the name of the resource group for the VM, and a default set of guest performance counters and logs will be selected.
5. In the Logs tab, select the Audit Failure log to collect from the virtual machine.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/diagnostics-extension-windows-install#install-with-azure-portal

upvoted 2 times

MarioMK 1 month, 2 weeks ago

Wrong Solution. You should go to the VM > Diagnostic Settings > Enable it if it hasnt been already enabled > Logs > Check if the desired log is selected >Agent > Select the desired Storage account, Log Level etc

upvoted 1 times

DeepCyber 3 months ago

Agree with dadageer.. Thanks
Tested in lab!

upvoted 2 times

https://t.me/learningnets

Question #19 *Topic 3*

You have 10 virtual machines on a single subnet that has a single network security group (NSG).
You need to log the network traffic to an Azure Storage account.
What should you do?

A. Install the Network Performance Monitor solution.

B. Create an Azure Log Analytics workspace.

C. Enable diagnostic logging for the NSG.

D. Enable NSG flow logs.

Correct Answer: *D*
A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:
- Create a VM with a network security group
- Enable Network Watcher and register the Microsoft.Insights provider
- Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
- Download logged data

View logged data -
▪
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

Super_Pun Highly Voted 4 months ago
Given answer is correct because the requirement is logging network traffic
upvoted 7 times

kumax Highly Voted 2 months, 1 week ago
From the material I have, there is additional line below as following:
Which 2 actions should you perform? Each answer presents part of the solution.
ANS: B & D
B: Enable Azure Network Watcher
D: Enable NSG flow logs.
There is a E selection, which is not the correct answer anyway.
E: Create an Azure Log Analytics workspace
Just watch out for the real question.
upvoted 5 times

dadageer Most Recent 4 months ago
Answer is correct : D
upvoted 4 times

dadageer 4 months ago
Answer is correct : D
upvoted 3 times

pravinjin 4 months ago
Answer: B
upvoted 1 times

macco455 3 months, 3 weeks ago
Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG. Flow data is sent to Azure Storage accounts from where you can access it as well as export it to any visualization tool, SIEM, or IDS of your choice.
upvoted 1 times

macco455 3 months, 3 weeks ago
Wrong, correct answer is D
upvoted 2 times

https://t.me/learningnets

Question #20 *Topic 3*

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics Agent installed?

A. VM3 only

B. VM1 and VM3 only

C. VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

Correct Answer: *D*

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2,

2016, version 1709 and 1803

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Raghav935 Highly Voted 2 months, 2 weeks ago

correct answer

upvoted 5 times

https://t.me/learningnets

Question #21 *Topic 3*

HOTSPOT -

You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{
    "type" : "Microsoft.Compute/virtualMachines/extensions",
    "name" : "[concat(parameter('vmname'), /OMSExtension]",
    "apiVersion" : "[variables('apiVersion')]",
    "location" : "[resourceGroup().location]",
    "dependsOn" : [
        "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
    ],
    "properties" : {
        "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
        "type" :  "MicrosoftMonitoringAgent",
        "typeHandlerVersion" : "1.0",
        "autoUpgradeMinorVersion" : true,
        "settings" : {
            [                          ▼] : "[variable('var1')]"
              "AzureADApplicationID"
              "WorkspaceID"
              "WorkspaceName"
              "WorkspaceURL"
    },
        "protectedSettings" : {
            [                          ▼] : "[variable ('var2')]"
              "AzureADApplicationSecret"
              "StorageAccountKey"
              "WorkspaceID"
              "WorkspaceKey"
    }
  }
}
```

https://t.me/learningnets

Correct Answer:

Answer Area

```
{
    "type" : "Microsoft.Compute/virtualMachines/extensions",
    "name" : "[concat(parameter('vmname'), /OMSExtension]",
    "apiVersion" : "[variables('apiVersion')]",
    "location" : "[resourceGroup().location]",
    "dependsOn" : [
        "[concat('Microsoft.Compute/virtualMachines/", parameters('vmName'))]"
    ],
    "properties" : {
        "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
        "type" :  "MicrosoftMonitoringAgent",
        "typeHandlerVersion" : "1.0",
        "autoUpgradeMinorVersion" : true,
        "settings" : {
            [ ▼ ] : "[variable('var1')]"
                "AzureADApplicationID"
                "WorkspaceID"
                "WorkspaceName"
                "WorkspaceURL"
    },
        "protectedSettings" : {
            [ ▼ ] : "[variable ('var2')]"
                "AzureADApplicationSecret"
                "StorageAccountKey"
                "WorkspaceID"
                "WorkspaceKey"
        }
    }
}
```

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

gcpbrig01 Highly Voted 4 months ago

Answer is correct.

"properties": {

"publisher": "Microsoft.EnterpriseCloud.Monitoring",

"type": "MicrosoftMonitoringAgent",

"typeHandlerVersion": "1.0",

"settings": {

"workspaceId": "[parameters('monitoringAgentWorkspaceID')]"

},

"protectedSettings": {

"workspaceKey": "[parameters('monitoringAgentWorkspaceKey')]"

}

}

}

upvoted 5 times

Pinto 3 months, 4 weeks ago

https://docs.microsoft.com/en-us/services-hub/health/mma-setup

upvoted 1 times

JaBe Most Recent 2 months, 1 week ago

Help me understand I don't get it. See previous question " You have an Azure subscription that contains the virtual machines shown in the following table. [...] From Azure Security Center, you turn on Auto Provisioning. You deploy the virtual machines shown in the following table. [...] On which virtual machines is the Log Analytics Agent installed?" Answer: VM1/2/3/4

https://t.me/learningnets

So if it is that easy to auto deploy the agent by only enabling auto provisioning in ASC, then why go through the hassle of preparing and deploying an ARM template?

upvoted 2 times

kimalto452 3 weeks, 5 days ago

because template you can use for various subscriptions/accounts

upvoted 1 times

ByZaN 2 months ago

same as you i dont get it

upvoted 1 times

Neonlight8 1 month, 3 weeks ago

Because it is "baked" into the template, and does not require additiona configuration to setup auto provisioning on MMS.

upvoted 1 times

JohnYinToronto 3 months, 3 weeks ago

Answers correct.
In AzurePortal:
On the **Overview, Settings Dashboard** page, click **Connected Sources**, and then copy and paste the **Workspace ID** and **Workspace Key (Primary Key)** from the log analytics portal.

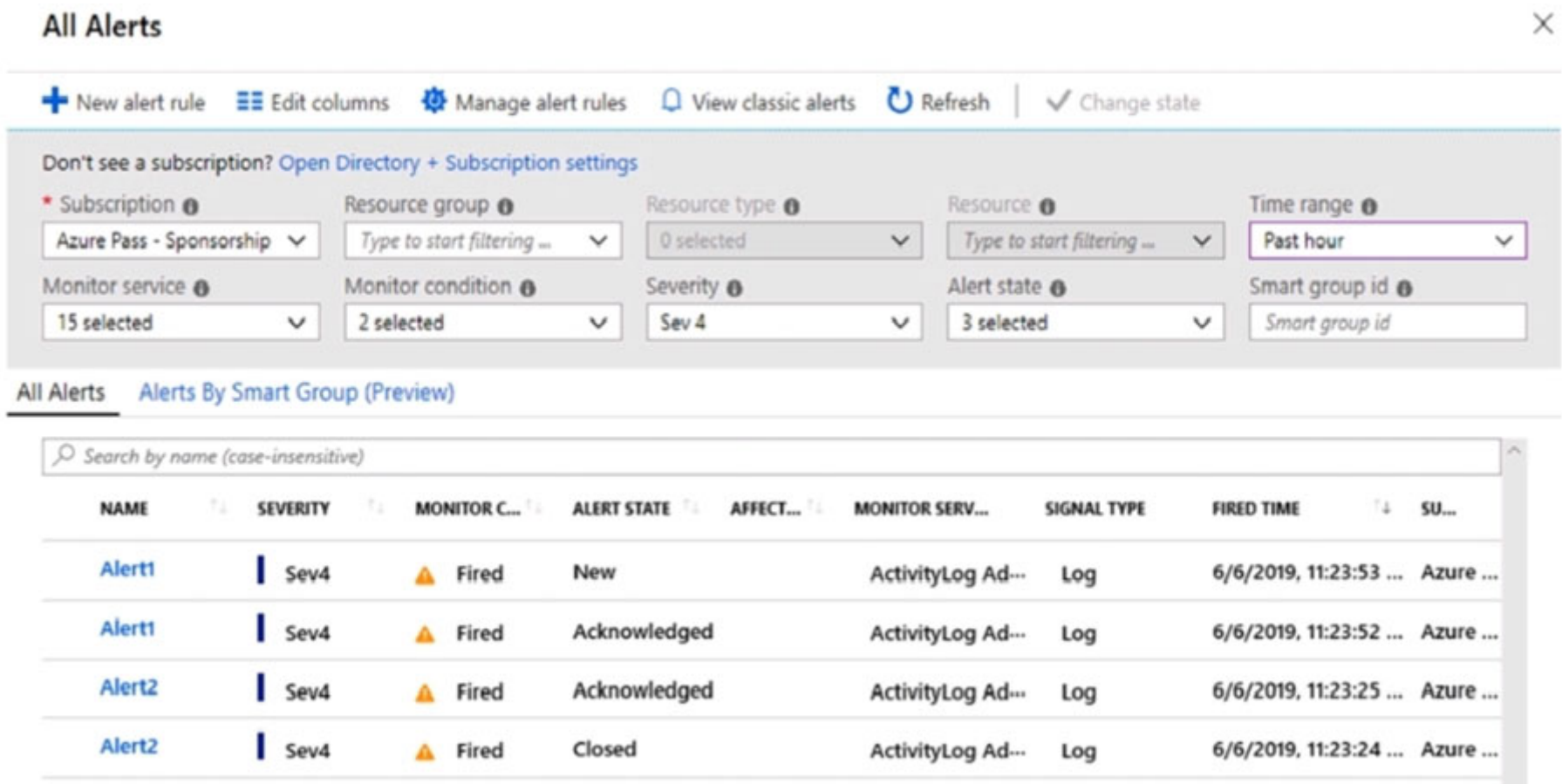
upvoted 2 times

https://t.me/learningnets

Question #22 *Topic 3*

HOTSPOT -

You have an Azure subscription that contains the alerts shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The state of Alert1 that was fired at 11:23:52

- cannot be changed
- can be changed to Closed only
- can be changed to New only
- can be changed to New or Closed

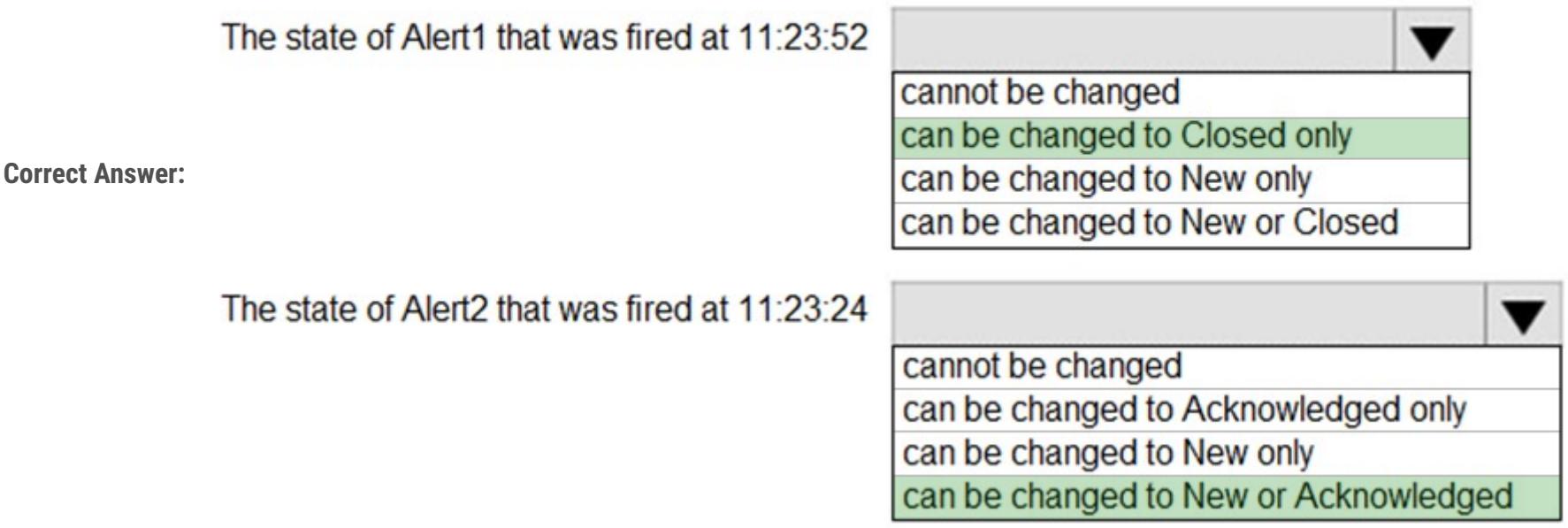
The state of Alert2 that was fired at 11:23:24

- cannot be changed
- can be changed to Acknowledged only
- can be changed to New only
- can be changed to New or Acknowledged

https://t.me/learningnets

Answer Area

Correct Answer:



References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview

nihao381 Highly Voted 4 months ago
I disagree with the first drop down, the alert state can be changed to any of the alternate options, so Alert1 @ 11:23:52 which has the state of Acknowledged can be changed to New or Closed. Alert2 @ 11:23:24 with the state of Closed can be changed to New or Acknowledged.
upvoted 17 times

Sethoo 4 months ago
You make a good point. If a closed alert can be changed to new or acknowledged, why cant one changed an acknowledged alert back to new or closed. I would changed the answer to new or closed on that one.
upvoted 2 times

WBXCC 4 months ago
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-managing-alert-states
Section: On clicking Change State, a popup opens up allowing you to select the state (New/Acknowledged/Closed) and enter a comment if necessary.
upvoted 1 times

JohnYinToronto Highly Voted 3 months, 3 weeks ago
Answers not quite correct.
Tested. Alert state can be changed to any state.
upvoted 15 times

kumax Most Recent 3 weeks, 4 days ago
On exam, May 2021.
This is a scenario that contains multiple (less than 5) questions.
upvoted 3 times

M21RUN 1 month ago
Tested in Lab: Alert state can be change to every state all the time.
upvoted 2 times

Cyberbug2021 2 months, 1 week ago
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-managing-alert-states
upvoted 1 times

glowglow 3 months, 2 weeks ago
Answers are correct.
You can set the state of an alert to specify where it is in the resolution process. When the criteria specified in the alert rule is met, an alert is created or fired, and it has a status of New. You can change the status when you acknowledge an alert and when you close it. All state changes are stored in the history of the alert.

The following alert states are supported.

MANAGE ALERTS
State Description
New The issue has been detected and hasn't yet been reviewed.
Acknowledged An administrator has reviewed the alert and started working on it.
Closed The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state.
upvoted 1 times

rgullini 2 months, 1 week ago
No, answers marked are not correct. you can change the alert to any state.

https://t.me/learningnets

upvoted 1 times

sjoerdstefma 3 months, 3 weeks ago

On clicking Change State, a popup opens up allowing you to select the state (New/Acknowledged/Closed) and enter a comment if necessary.

upvoted 3 times

Khumnan 3 months, 4 weeks ago

Tested, you can change to any state.
If the alert state is Closed. You can change to New or Acknowledge.
If the alert state is Acknowledge. You can change to New or Closed

upvoted 8 times

Pinto 3 months, 4 weeks ago

How is it that the alert times are out of order. Alert 1 list shows it was acknowledged first and then was marked as New if go by the timestamp.
Also would it make sense to move an alert from Ack to New?
Ideally the flow should be New->Ack->Closed->New...

upvoted 4 times

Pinto 3 months, 4 weeks ago

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview#manage-alerts
The following alert states are supported.
Manage alerts
State Description
New - The issue has been detected and hasn't yet been reviewed.
Acknowledged - An administrator has reviewed the alert and started working on it.
Closed - The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state.

The alert state isn't changed until the user changes it.

upvoted 2 times

https://t.me/learningnets

Question #23 *Topic 3*

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.
You need to create a custom sensitivity label.
What should you do?

A. Create a custom sensitive information type.

B. Elevate access for global administrators in Azure AD.

C. Upgrade the pricing tier of the Security Center to Standard.

D. Enable integration with Microsoft Cloud App Security.

Correct Answer: *A*
First, you need to create a new sensitive information type because you can't directly modify the default rules.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

teamaws Highly Voted 3 months, 1 week ago
saw this in the exam, so yes it is in scope
upvoted 7 times

Neonlight8 Most Recent 1 month, 3 weeks ago
If the options had P1 or P2 license on Azire AD then i would have went for that. But the best answer is A) creating the labels
upvoted 1 times

roy9889 2 months, 1 week ago
Azure has the same capabilities so cannot argue whether it should or should not be in exam - know your data, protect your data, DLP - but it should be in the syllabus though .. can sombody find any relevant link in the exam material provided by microsoft ?
upvoted 1 times

sureshatt 3 months, 2 weeks ago
is 0ffice365 in scope of this exam ?
upvoted 1 times

jonav94 2 months, 3 weeks ago
lol, I don't know what is Microsoft thinking really.. it seems to be a question for MS-500 exam not for AZ-500... :|
upvoted 2 times

Pinto 3 months, 4 weeks ago
choice A seems right
https://joannecklein.com/2018/08/07/build-and-use-custom-sensitive-information-types-in-office-365/
upvoted 2 times

Sethoo 4 months ago
I will go with A as well. As the other answers do not necessary apply. You do not have to upgrade your role if you are global admin to create sensitivity label. I also don't see the need to upgrade

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide
upvoted 2 times

sureshatt 3 months, 2 weeks ago
true. "The global admin for your organization has full permissions to create and manage all aspects of sensitivity labels."
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide#before-you-begin
upvoted 1 times

https://t.me/learningnets

Question #24 *Topic 3*

HOTSPOT -

You have the hierarchy of Azure resources shown in the following exhibit.



You create the Azure Blueprints definitions shown in the following table.

Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Blueprint1:

- ManagementGroup1 only
- ManagementGroup1, Subscription1, and RG1 only
- ManagementGroup1, Subscription1, RG1, and VM1
- Subscription1 only
- Tenant Root Group only
- Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

- ManagementGroup1 only
- Subscription1 and RG1 only
- Subscription1 only
- Subscription1, RG1, and VM1

https://t.me/learningnets

Answer Area

Correct Answer:

Blueprint1:

- ManagementGroup1 only
- ManagementGroup1, Subscription1, and RG1 only
- ManagementGroup1, Subscription1, RG1, and VM1
- **Subscription1 only**
- Tenant Root Group only
- Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

- ManagementGroup1 only
- Subscription1 and RG1 only
- **Subscription1 only**
- Subscription1, RG1, and VM1

Blueprints can only be assigned to subscriptions.

cvarl Highly Voted 4 months ago

"Each Published Version of a blueprint can be assigned to an existing management group or subscription." so:
Blueprint1: Tenant Root Group, ManagementGroup1, and Subscription 1 only
Blueprint2: Subscription1
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment

upvoted 35 times

zsedo 1 month ago

This article is ambigous a little bit. Check:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-definition-locations
When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.
So correct answer should be 'Subscription1 only' for both case. (Tested and confirmed on portal. Maybe you can assign to management group with API. I don't know.)

upvoted 2 times

Pratiko3 Highly Voted 1 month, 2 weeks ago

blueprint can only be assigned to a subscription. tested.
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-parameters

upvoted 7 times

alexk0 1 month, 2 weeks ago

Followed your link:
Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription

upvoted 2 times

Darvel 1 month, 2 weeks ago

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to "any child subscription of that management group."

upvoted 2 times

Lyonel Most Recent 2 days, 6 hours ago

Here's my two cents...
As documentation states: "Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription."
[Ref.: https://docs.microsoft.com/en-us/azure/governance/blueprints/overview]

Therefore:
Box 1 = Tenant Root Group, Management Group and Subscription
[Ref. for Root Tenant Group, which is a single top-level Management Group and operates as a Management Group in SDK:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview]

Box 2 = Subscription only

upvoted 1 times

kumax 3 weeks, 4 days ago

On exam, May 2021.

upvoted 3 times

https://t.me/learningnets

kimalto452 3 weeks, 5 days ago

Blueprint1: Tenant Root Group, ManagementGroup1, and Subscription 1 only
Blueprint2: Subscription1

Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription.

upvoted 2 times

Rajesh123 1 month ago

The answer is correct ,blueprint can only be assigned to a subscription within the scope of Tenant Root Group, ManagementGroup1

upvoted 4 times

ysm 1 month, 3 weeks ago

1=> F
2 => C

upvoted 1 times

nicksb19 1 month, 4 weeks ago

so in this link : https://docs.microsoft.com/en-us/azure/governance/blueprints/overview
it says - When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.
Now I didnt see anywhere mention it can be saved in Tenant Root group, but anyways and then :
Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription.
So I would say both answers as Sub1 only.

upvoted 1 times

Enitan 1 month, 4 weeks ago

Answers are correct

upvoted 1 times

rgullini 2 months, 1 week ago

Answers correct.
When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment

upvoted 3 times

Cyberbug2021 2 months, 1 week ago

Blueprint1: Tenant Root Group, ManagementGroup1, and Subscription 1 only
Blueprint2: Subscription1

upvoted 3 times

RohitGoel 2 months, 2 weeks ago

Which is the final answer?

upvoted 3 times

JerryGolais 2 months, 3 weeks ago

You can set the definition location of a blueprint to a management group or a subscription.
You can only assign it on a subscription.
This Microsoft Doc is confusing but you can easily verify it in the portal.
"Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription."
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment

upvoted 4 times

glowglow 3 months, 1 week ago

Blueprint assignment
Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription. In the portal, the blueprint defaults the Version to the one Published most recently. If there are artifact parameters or blueprint parameters, then the parameters are defined during the assignment process.
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment

upvoted 1 times

Tunde 4 months ago

Blueprint 1- F, Blueprint 2- D. Azure Blueprint can be assigned to either Management group or subscription

upvoted 2 times

Tunde 4 months ago

Sorry Blueprint 2- C

upvoted 1 times

https://t.me/learningnets

https://t.me/learningnets

Question #25 *Topic 3*

You have an Azure subscription that contains the Azure Log Analytics workspaces shown in the following table.

Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	*Not applicable*

You create the virtual machines shown in the following table.

Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	*None*
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	*None*
VM4	West US	Windows Server 2019	Workspace2

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines.

Which virtual machines you can connect to Azure Sentinel?

A. VM1 only

B. VM1 and VM3 only

C. VM1, VM2, VM3, and VM4

D. VM1 and VM2 only

Correct Answer: *C*

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

sureshatt Highly Voted 3 months, 2 weeks ago

Given answer is correct. It is true that VMs are connected to different workspaces, but you can always install the "Windows Firewall" data connector to those VMs from Azure Sentinel.

upvoted 6 times

glowglow Most Recent 3 months, 2 weeks ago

The Windows Defender Firewall with Advanced Security connector allows Azure Sentinel to easily ingest Windows Defender Firewall with Advanced Security logs from any Windows machines in your workspace.

upvoted 2 times

hang10z 3 months, 3 weeks ago

It does not matter where the VM is currently connected, you can deploy agents and have them connect to the Sentinel workspace at anytime. They are not suck in Workspace2 forever lol

upvoted 3 times

saran1987 3 months, 3 weeks ago

For physical and virtual machines, you can install the Log Analytics agent that collects the logs and forwards them to Azure Sentinel. For Firewalls and proxies, Azure Sentinel installs the Log Analytics agent on a Linux Syslog server, from which the agent collects the log files and forwards them to Azure Sentinel.

I think, you just need to install the log analytics agents on the VM's to send the data to Sentinel

upvoted 1 times

JohnYinToronto 3 months, 3 weeks ago

Answer wrong. Should be VM2 and VM4.
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall
The Windows Defender Firewall with Advanced Security connector allows Azure Sentinel to easily ingest Windows Defender Firewall with Advanced Security logs from any Windows machines in your workspace.

upvoted 1 times

Pinto 3 months, 4 weeks ago

Is this question even correct?
The linked doc says
Prerequisites: You must have read and write permissions on the workspace to which the machines you wish to monitor are connected.

If the machines are not connected to the workspace, then how will the Log Analytics agent send the data and Sentinel sits on top of Log Analytics Workspace.

upvoted 1 times

Sethoo 4 months ago

I will also go with the given answer. You do not need a workspace to connect to Sentinel. So the mere fact the other VMs are not on workspace does not meas they cant be connected to Sentinel. You can connect VMS to Sentinel through data connectors by installing agents on the Windows virtual machine.
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

https://t.me/learningnets

upvoted 2 times

nihao381 4 months ago

This should be B, as Sentinel is only connected to Workspace1. For this to work we would either need to replace with Workspace1 on VM2 and VM4 or connect Sentinel to Workspace1.

https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

upvoted 2 times

gcpbrig01 4 months ago

does this mean detaching the VMs from existing workspace(Stand alone) and attaching them to the workspace connected to Sentinel

upvoted 1 times

wawuuu 4 months ago

Given answer is correct.

upvoted 1 times

https://t.me/learningnets

Question #26 *Topic 3*

HOTSPOT -

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

Name	Resource	Condition
Rule1	RG1	All security operations
Rule2	RG1	All administrative operations
Rule3	Azure subscription	All security operations by Admin1
Rule4	Azure subscription	All administrative operations by Admin1

Admin1 performs the following actions on RG1:

- Adds a virtual network named VNET1
- Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Adding VNET1:

- Rule2 only
- Rule4 only
- Rule2 and Rule4 only
- Rule3 and Rule4 only
- Rule1, Rule2, Rule3, and Rule4

Adding Lock1:

- Rule2 only
- Rule4 only
- Rule2 and Rule4 only
- Rule3 and Rule4 only
- Rule1, Rule2, Rule3, and Rule4

Answer Area

Adding VNET1:

- Rule2 only
- Rule4 only
- Rule2 and Rule4 only
- Rule3 and Rule4 only
- Rule1, Rule2, Rule3, and Rule4

Correct Answer:

Adding Lock1:

- Rule2 only
- Rule4 only
- Rule2 and Rule4 only
- Rule3 and Rule4 only
- Rule1, Rule2, Rule3, and Rule4

https://t.me/learningnets

sureshatt Highly Voted 3 months, 2 weeks ago

Adding/Removing locks are also Administrative. Therefore given answer is correct.

upvoted 7 times

kumax Highly Voted 3 weeks, 4 days ago

On exam, May 2021.

upvoted 6 times

glowglow Most Recent 3 months, 2 weeks ago

Administrative category
This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would see in this category include "create virtual machine" and "delete network security group" Every action taken by a user or application using Resource Manager is modeled as an operation on a particular resource type. If the operation type is Write, Delete, or Action, the records of both the start and success or fail of that operation are recorded in the Administrative category. The Administrative category also includes any changes to Azure role-based access control in a subscription.

upvoted 4 times

JohnYinToronto 3 months, 3 weeks ago

answers correct

upvoted 4 times

Fred64 3 months, 4 weeks ago

There is no "all security operations" for resource group

upvoted 1 times

Pinto 3 months, 4 weeks ago

Should it not be Rule 2 only as both actions are being done at resource group level?

upvoted 1 times

Super_Pun 4 months ago

Given answer is correct, all are administrative activity

upvoted 3 times

gcpbrig01 4 months ago

the answer is correct: https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema#categories
Examples of Administrative events include create virtual machine and delete network security group.

upvoted 1 times

Tunde 4 months ago

Answer is correct: https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema

upvoted 4 times

milad123 4 months ago

think false response

upvoted 2 times

https://t.me/learningnets

Question #27 *Topic 3*

You have an Azure subscription that contains 100 virtual machines and has Azure Security Center Standard tier enabled.
You plan to perform a vulnerability scan of each virtual machine.
You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.
Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the user-assigned managed identity

B. the workspace ID

C. the Azure Active Directory (Azure AD) ID

D. the Key Vault managed storage account key

E. the system-assigned managed identity

F. the primary shared key

Correct Answer: *AC*

Deepmindx 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 2 times

MikeB19 2 months, 4 weeks ago
User assigned bc of the amount vms. If u select system assigned then u would need an mi for every machine. In case of user assigned you only need one mi and assign to all machines. It's a tricky question
upvoted 2 times

milad123 3 months, 2 weeks ago
Why it's not "the system-assigned managed identity" instead of "the user-assigned managed identity"
upvoted 2 times

sureshatt 3 months, 2 weeks ago
I think it will be not possible to define a system assigned identity in your code, because it is not available when you create the code.
upvoted 1 times

milind8451 4 months, 3 weeks ago
Here is ARM Code -

https://github.com/Azure/Azure-Security-Center/blob/master/Remediation%20scripts/Enable%20the%20built-in%20vulnerability%20assessment%20solution%20on%20virtual%20machines%20(powered%20by%20Qualys)/Azure%20Policy/deploy-qualys-va.json
upvoted 2 times

ttomaszoex 5 months ago
is there any MS documentation for this question?
upvoted 1 times

fallenDaffy 5 months ago
I found this page - https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal . Based on that I would say that answers are correct (they user tenant ID and spn id (user managed identity)
upvoted 2 times

Yuvithehustler 5 months, 1 week ago
answer is correct
upvoted 2 times

tuta 6 months, 4 weeks ago
correct
upvoted 4 times

https://t.me/learningnets

Question #28 *Topic 3*

You have an Azure subscription that contains a user named Admin1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.
Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.
You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1.
What should you do?

A. Create and configure a network security group (NSG).

B. Create and configure an additional public IP address for VM1.

C. Replace the Basic Load Balancer with an Azure Standard Load Balancer.

D. Assign an Azure Active Directory Premium Plan 1 license to Admin1.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc

gills Highly Voted 7 months, 2 weeks ago
A is correct.
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc

Unsupported - VMs without JIT enabled and which don't support the feature. Your VM might be in this tab for the following reasons:
Missing network security group (NSG) - JIT requires an NSG to be configured
Classic VM - JIT supports VMs that are deployed through Azure Resource Manager, not 'classic deployment'. Learn more about classic vs Azure Resource Manager deployment models.
Other - Your VM might be in this tab if the JIT solution is disabled in the security policy of the subscription or the resource group.

Unsupported - VMs without JIT enabled and which don't support the feature. Your VM might be in this tab for the following reasons:
Missing network security group (NSG) - JIT requires an NSG to be configured
Classic VM - JIT supports VMs that are deployed through Azure Resource Manager, not 'classic deployment'. Learn more about classic vs Azure Resource Manager deployment models.
Other - Your VM might be in this tab if the JIT solution is disabled in the security policy of the subscription or the resource group.

upvoted 19 times

Thi 5 months, 1 week ago
Thanks A is correct
upvoted 4 times

deegadaze1 Highly Voted 4 months, 2 weeks ago
In exam
upvoted 9 times

kumax Most Recent 3 weeks, 4 days ago
On exam, May 2021.
upvoted 3 times

roy9889 2 months, 1 week ago
This is an important question and correct answer
Load balancers connect directly to VM's NIC (not a subnet) so we cannot just assume in this question that an NSG has been created yet.
2nd piece of important info is JIT can only be enabled for an NSG - an NSG can only be applied for VM or Subnet (not the entire Vnet)
upvoted 1 times

glowglow 3 months, 2 weeks ago
Enable JIT on your VMs - You can enable JIT with your own custom options for one or more VMs using Security Center, PowerShell, or the REST API. Alternatively, you can enable JIT with default, hard-coded parameters, from Azure virtual machines. When enabled, JIT locks down inbound traffic to your Azure VMs by creating a rule in your network security group.
upvoted 1 times

mayenite 5 months, 2 weeks ago
Correct
upvoted 2 times

cunlu 6 months, 2 weeks ago
A is correct => Enable JIT on your VMs - You can enable JIT with your own custom options for one or more VMs using Security Center, PowerShell, or the REST API. Alternatively, you can enable JIT with default, hard-coded parameters, from Azure virtual machines. When enabled, JIT locks down inbound traffic to your Azure VMs by creating a rule in your network security group.
upvoted 4 times

https://t.me/learningnets

Question #29 *Topic 3*

HOTSPOT -

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1, and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.

You need to ensure that you can add Playbook1 to the new rule.

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

Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:

- A managed connector
- A system-assigned managed identity
- A trigger
- Diagnostic settings

Answer Area

Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- Scheduled

Correct Answer:

Configure the playbook to include:

- A managed connector
- A system-assigned managed identity
- A trigger
- Diagnostic settings

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

gcpbrig01 Highly Voted 4 months ago

Suggested answer is correct. The playbook is essentially a logic app wherein you set the trigger to "When a response to an Azure Sentinel alert is triggered" and follow it up with actions.

upvoted 11 times

kumax Most Recent 3 weeks, 4 days ago

On exam, May 2021.

upvoted 4 times

pal40sg 2 months ago

Answer is correct, https://docs.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules

1. When you click Create and one of the rule types (Scheduled query rule or Microsoft incident creation rule) from the top menu in the Analytics blade,

upvoted 4 times

https://t.me/learningnets

Question #30 *Topic 3*

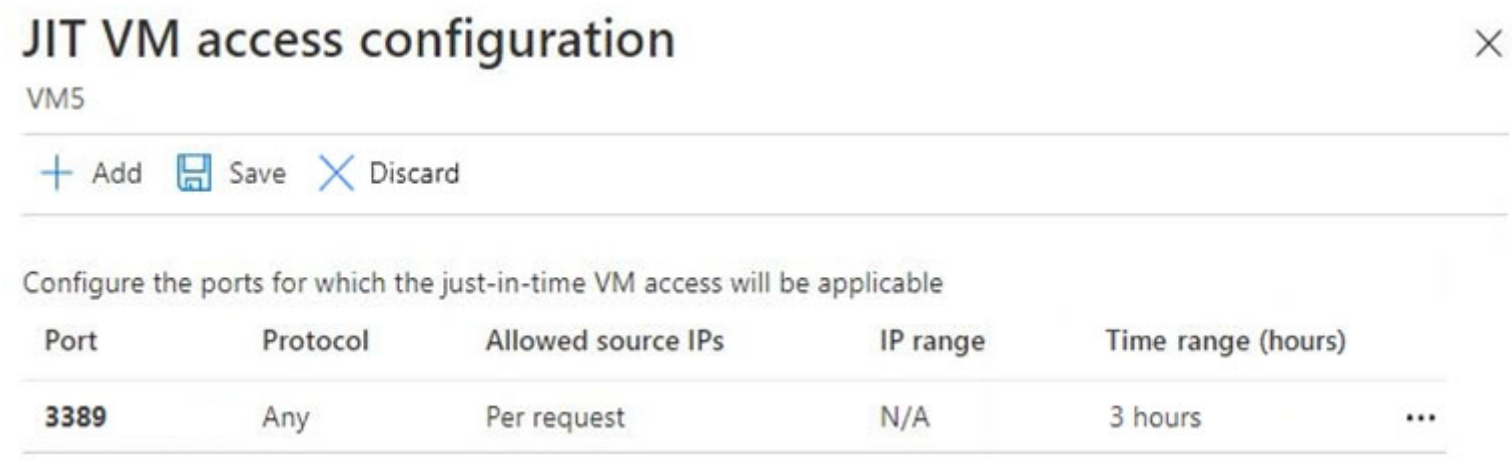
HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	*Not applicable*
NSG2	Network security group (NSG)	Subnet1	*Not applicable*
Subnet1	Subnet	*Not applicable*	*Not applicable*
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address.

VM5 has just in time (JIT) VM access configured as shown in the following exhibit.



You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	Deny
1001	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	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
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	○	○
Remote Desktop access to VM5 is blocked.	○	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	○

Answer Area Yes,No,Yes

Correct Answer:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	○	○
Remote Desktop access to VM5 is blocked.	○	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	○

https://t.me/learningnets

CASGTI Highly Voted 2 months, 2 weeks ago

Now... question 2...
For me, is "NO" also, because RDP is allowed, that the machine dont have a public IP means you cant access from internet, does not means you cant access.
and question 3 ... for me would be "YES"
Why? just because a well configured bastion host, will allow you to connect from the internet to the bastion, and then from there, to the machine by using the private IP (as stated on question 2, RDP is allowed, but just internally, so the bastion will solve this)

upvoted 8 times

Frosticus 4 weeks, 1 day ago

JIT does not work with bastion: https://charbelnemnom.com/how-to-configure-just-in-time-vm-access-for-azure-firewall-in-azure-security-center/#Azure_Bastion_and_Jut-In-Time_VM_access

upvoted 1 times

luismax Highly Voted 2 months, 1 week ago

In exam

upvoted 5 times

FableFa Most Recent 3 weeks, 4 days ago

NO, NO, YES

upvoted 3 times

Frosticus 4 weeks, 1 day ago

From my research:
1) No, it will automatically get added back
2) No, JIT will unblock as needed (bad question, ambiguous because it is blocked until it isn't)
3) No, Bastion does not work with JIT https://charbelnemnom.com/how-to-configure-just-in-time-vm-access-for-azure-firewall-in-azure-security-center/#Azure_Bastion_and_Jut-In-Time_VM_access

upvoted 2 times

hydrillo 1 month ago

Yes - tested in Lab: firewall rule is not recreated by JIT
No - the JIT rule allows RDP access, not from the internet bcoz the has no public IP but thats was not the question
Yes - RDP is allowed through the JIT rule. If you deploy Bastion on the same vNet you'll be able to connect

upvoted 2 times

Frosticus 4 weeks, 1 day ago

JIT does not work with Bastion https://charbelnemnom.com/how-to-configure-just-in-time-vm-access-for-azure-firewall-in-azure-security-center/#Azure_Bastion_and_Jut-In-Time_VM_access

upvoted 1 times

Bob00111 2 months ago

Yes - tested in Lab: the firewall rule is not re-created by JIT.
Yes - The JIT deny rule will block it.
No - Bastion is also blocked by JIT deny rule.

upvoted 5 times

roy9889 2 months, 1 week ago

Even if deletion of firewall rule adds it again, this particular access request will still be revoked and the user will have to request again. At least that is what I think.

upvoted 1 times

rgullini 2 months, 1 week ago

No - Deletion of Firewall rule for JIT will add it again.
yes - Rule "1000" blocks it to the VM IP
No - Traffic is blocked

upvoted 1 times

mateo2121 3 weeks, 2 days ago

Rule 1000 do not allow RDP connection (protocol ANY includes also TCP from rule 1001 to destination IP address 10.1.0.4), so the answer is YES

upvoted 1 times

souvik123 2 months, 1 week ago

No - Deletion of Firewall rule for JIT will add it again.
No - RDP is allowed
Yes - Bastion will allow internet connection and then RDP to internal IP

upvoted 3 times

Cyberbug2021 2 months, 1 week ago

VM5 does not have a public IP so remote rdp is not possible - what ip do you rdp to?

upvoted 2 times

Azuriste 2 months, 2 weeks ago

NO NO YES

https://t.me/learningnets

upvoted 2 times

CASGTI 2 months, 2 weeks ago

I tested in lab...
And question 1 will be "NO", when you remove the firewall rules, they will be added again!! automatically... so the access is not revoked at all.

upvoted 5 times

Fred64 2 months, 3 weeks ago

Without a public IP we can't connect from Internet, but we can with Bastion.
Anyway question 3 asks if bastion allow internet connection. The answer is NO

The provided solution is OK and I tested it

upvoted 3 times

Sitender 2 months, 4 weeks ago

3 - no because rule 1000 says rdp blocked

upvoted 2 times

glowglow 3 months, 2 weeks ago

Yes, Yes,
C is No - in question - VM5 does not have a public IP address. Does this matter when using Bastion?

upvoted 3 times

Rume 3 weeks, 4 days ago

Azure Bastion always uses target VM's private IP address to connect over RDP (will not use public IP even if the VM were to have it) and that you can define the rule on the target VM subnet to allow incoming 3389 only from AzureBastionSubnet.

https://feedback.azure.com/forums/217313-networking/suggestions/38231884-bastion-and-jit-access#:~:text=Currently%20Bastion%20in%20Azure%20Portal,Bastion%20to%20make%20the%20connection.

upvoted 2 times

Rume 3 weeks, 4 days ago

1. Deleting the JIT rule -> it will re-appear. Answer is NO
2. No
3. Yes. (as explained above)

upvoted 2 times

gcpbrig01 4 months ago

Answer to C is "Yes". Azure bastion host is a managed service that allows you to rdp/ssh to a VM from internet/azure portal without having to create
1) a pip for the vm
2) nsg rule to allow rdp/ssh to the VM

upvoted 5 times

gcpbrig01 4 months ago

Answer to C is "No". JIT would prevent Azure Bastion Host login

upvoted 1 times

milad123 3 months, 2 weeks ago

No, because we have the rule 1001 which allow rdp connection

upvoted 1 times

nihao381 4 months ago

After some thought, I agree with the answer. Deleting rule 100 will revoke the approved JIT request. Without any JIT approvals the JIT deny rule at 1000 blocks RDP. Azure Bastion is not compatible with JIT.

upvoted 2 times

malay1232489 4 months ago

Are the questions related.. meaning, if i delete, then no2 and then no3.. i think they are a stand alone.

upvoted 1 times

Sethoo 4 months ago

Not sure if the questions are related or standalone but i will lean towards being standalone and my answers will be
Yes
No
No

upvoted 7 times

gcpbrig01 4 months ago

Please ignore, the JIT would come in the way of Azure Bastion host

upvoted 1 times

https://t.me/learningnets

Question #31 *Topic 3*

You have an Azure Active Directory (Azure AD) tenant and a root management group.
You create 10 Azure subscriptions and add the subscriptions to the root management group.
You need to create an Azure Blueprints definition that will be stored in the root management group.
What should you do first?

A. Modify the role-based access control (RBAC) role assignments for the root management group.

B. Add an Azure Policy definition to the root management group.

C. Create a user-assigned identity.

D. Create a service principal.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

Stuudent Highly Voted 6 months, 3 weeks ago
When I tried to create a Blueprint at the root management group, I got the following message:
Deploy blueprint to root management group:
"You require additional permissions to manage blueprints within this management group. Contact the administrator of the management group to request Contributor rights."
Had to elevate myself to a Contributor at the root group, then I could create the blueprint.
Therefore option A is definitely correct.
upvoted 23 times

JerryGolais Most Recent 2 months, 3 weeks ago
I am not sure what access we have. For all we know we have the owner role and the correct answer is B. Or we don't have contributor rights and it's A.
I am thinking that if we are able to create 10 subs in this management group, we have contributor rights so I would go for B.
To sum up, I'm not sure.
upvoted 3 times

arunjana 7 months, 1 week ago
When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview
upvoted 3 times

https://t.me/learningnets

Question #32 *Topic 3*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? 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 create a security group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Users who can create a Microsoft 365 group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Answer Area

Correct Answer:

Users who can create a security group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Users who can create a Microsoft 365 group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Reference:

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

justinp 5 days, 14 hours ago

Is this question in exam?

upvoted 1 times

Lyonel 6 days, 9 hours ago

Explanation provided in the link shows the answer provided is CORRECT:

Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

Global Administrator
User Administrator

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

upvoted 2 times

ChinkSantana 1 week, 4 days ago

The following are the list of administrator roles exempted from the group naming policy.

Global administrator
User administrator

Given Answer is correct.

https://t.me/learningnets

upvoted 2 times

Rume 1 week, 6 days ago

https://www.examtopics.com/discussions/microsoft/view/46727-exam-az-500-topic-3-question-32-discussion/

upvoted 4 times

strugggg1 4 days, 2 hours ago

Admin1,2,3
Admin1,3

upvoted 1 times

Roger_Smurf 2 weeks ago

1) Admin1,2,3 because policy naming blocks only apply to O365
2) Admin 1,3 because Global Admin and User Admin are exempt.
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy

upvoted 4 times

https://t.me/learningnets

Question #33 *Topic 3*

DRAG DROP -

You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant.

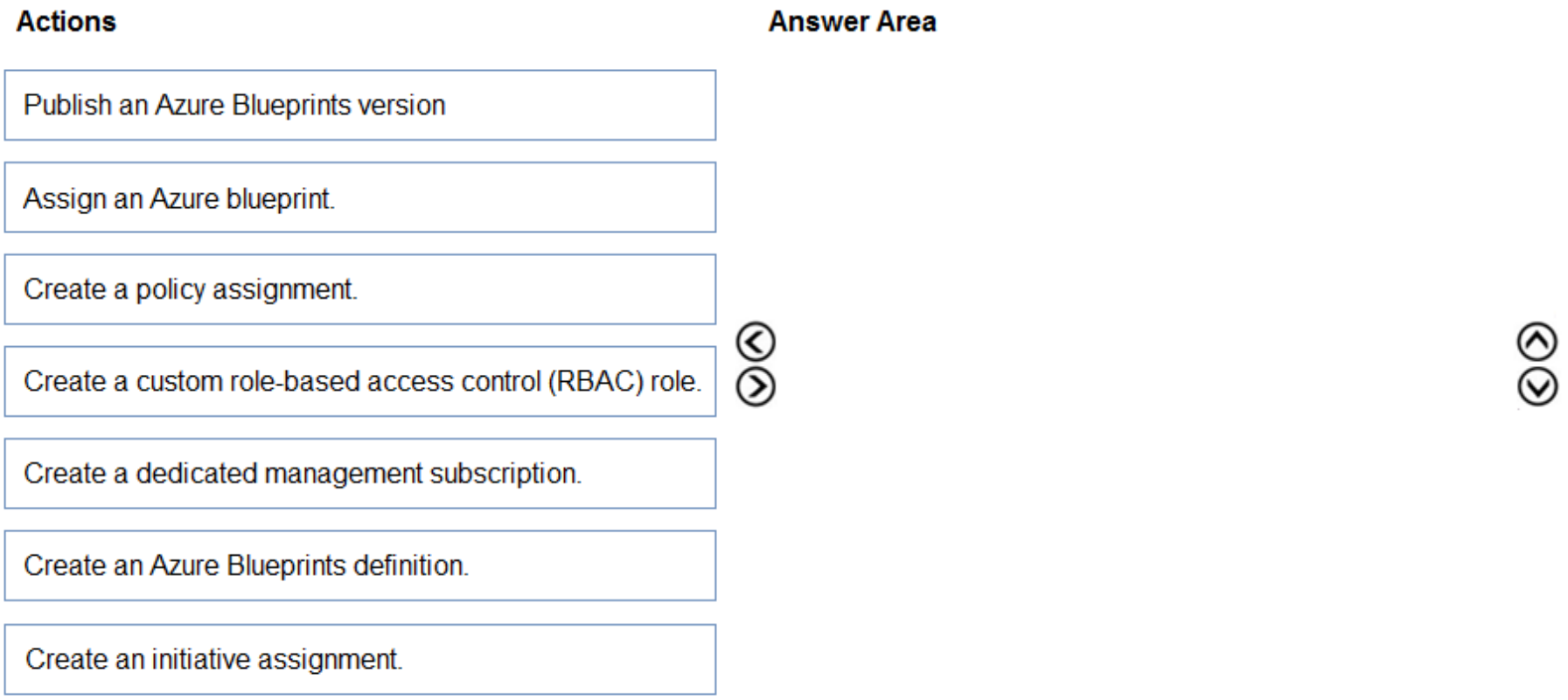
You create an Azure Policy initiative named SecurityPolicyInitiative1.

You identify which standard role assignments must be configured on all new resource groups.

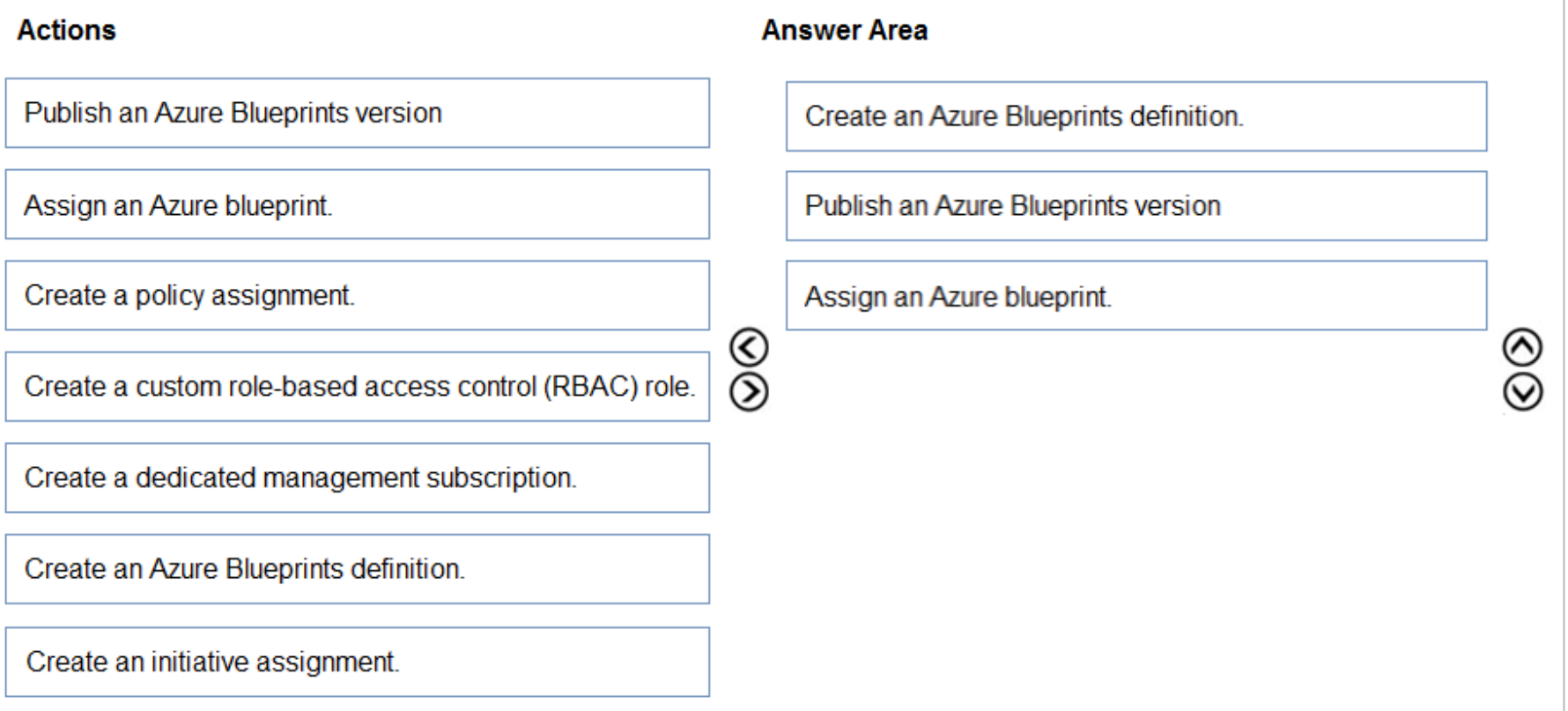
You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created.

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:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy

gcpbrig01 Highly Voted 4 months ago

Azure blueprint is the means to enforce a policy. hence the answer is correct

upvoted 9 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 4 times

https://t.me/learningnets

Question #34 *Topic 3*

You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server 2019. Server1 and Server2 and located on the internal network. Server3 is located on the perimeter network. All servers have access to Azure.
From Azure Sentinel, you install a Windows firewall data connector.
You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel.
What should you do?

A. Create an event subscription from Server1, Server2, and Server3.

B. Install the On-premises data gateway on each server.

C. Install the Microsoft Monitoring Agent on each server.

D. Install the Microsoft Monitoring Agent on Server1 and Server2. Install the On-premises data gateway on Server3.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

mehdimed 1 day, 12 hours ago
correct answer, clearly answers involving the data gateway are red herrings
upvoted 1 times

Question #35 *Topic 3*

You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.
You need to create a saved query in the workspace to find events reported by Azure Defender for SQL.
What should you do?

A. From Azure CLI run the Get-AzOperationalInsightsWorkspace cmdlet.

B. From the Azure SQL Database query editor, create a Transact-SQL query.

C. From the Azure Sentinel workspace, create a Kusto Query Language query.

D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Correct Answer: *C*

mehdimed 1 day, 12 hours ago
Fairly easy as the queries are written in kusto : https://docs.microsoft.com/en-us/azure/sentinel/hunting
upvoted 1 times

https://t.me/learningnets

Question #36 *Topic 3*

HOTSPOT -

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Detect suspicious threats:
- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:
- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Correct Answer:

Answer Area

Detect suspicious threats:
- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:
- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Sethoo Highly Voted 4 months ago

security playbook can help automate and orchestrate your response, and can be run manually or set to run automatically when specific alerts are triggered.

upvoted 5 times

jkklim Highly Voted 4 months ago

correct

upvoted 5 times

https://t.me/learningnets

Question #37 *Topic 3*

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace.
You plan to create alerts based on the collected events.
You need to identify which Azure services can be used to create the alerts.
Which two services should you identify? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure Monitor

B. Azure Security Center

C. Azure Analysis Services

D. Azure Sentinel

E. Azure Advisor

Correct Answer: *AD*

tuta Highly Voted 6 months, 4 weeks ago
correct
upvoted 15 times

Deepmindx Most Recent 1 week, 6 days ago
IN THE EXAM 29/6/2021
upvoted 2 times

Cyberbug2021 2 months, 1 week ago
Question does not say what type of alerts I.e security - could be any alerts. Sentinel does not create alerts

You can create Alerts through Azure Advisor
You can create Alerts through Azure Monitor

you create incidents from alerts in sentinel
upvoted 3 times

alexk0 1 month, 3 weeks ago
Yes, you can create an Advisor alert but it's said: "You are collecting events from Azure virtual machines to an Azure Log Analytics workspace. You plan to create alerts based on the collected events"
From my best understand Advisor has nothing to do with LA workspace and VMs events in it.
upvoted 3 times

zic04 5 months, 3 weeks ago
D & A correct
upvoted 3 times

fdera 6 months, 4 weeks ago
A and C not A and D. Analytic tool helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.
upvoted 1 times

stewfreed 6 months, 3 weeks ago
azure analytics is different than azure logs analytics.
azure analytics is a service to leverage big-data (cosmodb) even if is used in background of sentinel an logs analytics. it's not the service to activate directly to have log analysis.
you must use azure sentinel (detect analysis and action) or azure monitor.
source:https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-overview
A and D should be the response
upvoted 15 times

https://t.me/learningnets

Question #38 *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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create an initiative and an assignment that is scoped to a management group.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

glowglow Highly Voted 3 months, 1 week ago
An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to. Assignments are inherited by all child resources. This design means that a definition applied to a resource group is also applied to resources in that resource group. However, you can exclude a subscope from the assignment.
https://docs.microsoft.com/en-us/azure/governance/policy/overview#assignments
upvoted 6 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago
An Azure initiative is a collection of Azure policy definitions that are grouped together towards a specific goal or purpose in mind. Azure initiatives simplify management of your policies by grouping a set of policies together as one single item
upvoted 3 times

hendry781 3 months, 2 weeks ago
Answer is No. Assignment cannot only be scoped to Subscriptions and RG level
upvoted 2 times

hendry781 3 months, 2 weeks ago
Correction. Answer is correct. assignment can be done at management group level
upvoted 6 times

https://t.me/learningnets

Question #39 *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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and assignments that are scoped to resource groups.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

gfhbox0083 Highly Voted 1 year ago
B, for sure.
Using Management Groups
upvoted 14 times

g01d Highly Voted 1 year, 5 months ago
There's a prev question where some guys state initiative is the correct instead of resource graph
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously. However, you need to use an initiative, not a resource graph to bundle the policy definitions into a group that can be applied to the management group.
upvoted 10 times

kristiann21 1 year, 1 month ago
Yes. Initiative is a way of grouping policies together. For example an inbuilt initiative is Azure Security Center rules (actually are a bunch of policies combined in an initiative) that run when Azure Security Center runs.

So policies are grouped as initiatives and can be applied at a management group level to enforce policies on subscriptions that fall under that management group.

In here, the suggessted flow is to create an initiative, which is correct, but assigning needs to be to a management group.

hence, no.
upvoted 6 times

gcpbrig01 Most Recent 4 months ago
I think the best practise is to create and apply policies/initiatives to the scope of either Management Groups or subscriptions. So answer is "No"
upvoted 1 times

Stuudent 7 months, 4 weeks ago
This is a tricky question and the key word is "assignmentS" (plural) in my opinion. When I read first time I was like "create assignment to three subscriptions" -> so yeah, create assignment to management group and exclude any subscriptions you don't want, meets the goal, answer A. But since you can't actually assign a policy to three subscriptions WITHOUT using the management group and they tell you to create three separate assignments - that's why it's a no. Right?
upvoted 1 times

Freeze 1 year ago
Answer is Correct
Apply initiative to management groups
upvoted 5 times

examexpert 6 months, 1 week ago
to mgt groups not resource groups
upvoted 1 times

Philipp 1 year ago
keyword is " policy management of three Azure subscriptions." that means better take managment groups instead of assign it 3 times to three ressource groups, which is techical possible but not nice

https://t.me/learningnets

upvoted 4 times

Fred64 4 months, 1 week ago

What if the initiative has 50 rules?

The question has a bad statement I thing

upvoted 1 times

Fred64 4 months, 1 week ago

" that are scoped to resource groups.".

My bad you are right

upvoted 1 times

g01d 1 year, 5 months ago

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

upvoted 1 times

https://t.me/learningnets

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy definition and assignments that are scoped to resource groups.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

D_PaW Highly Voted 1 year, 1 month ago
Answer B (no) is correct. You can only group subscriptions in management groups, NOT i resource groups... as they are for resources ;)
https://azure.microsoft.com/features/management-groups/
upvoted 10 times

kdkdk Highly Voted 7 months ago
in the exams
upvoted 6 times

Thi Most Recent 5 months, 2 weeks ago
Answer B.No
Reason: If we apply policy at resource group then it's scope is limited to that resource group. We need to put policy at Management group->Sub1,sub2,sub3 then answer can be Yes because it will inherit policy down to subscription resource groups etc.
upvoted 3 times

gfhbox0083 1 year ago
B, for sure.
Management Groups and not Resource Groups
upvoted 6 times

gboyega 1 year ago
CORRECT
upvoted 1 times

anonymous654 1 year, 6 months ago
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/
upvoted 2 times

mat73 1 year, 6 months ago
You assign policies to Management Groupor 1 Subscription (and optionally 1 RG)
upvoted 4 times

Rp69 1 year, 7 months ago
URL provided re-directs to a broken link
upvoted 2 times

https://t.me/learningnets

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a resource graph and an assignment that is scoped to a management group.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
However, you need to use an initiative, not a resource graph to bundle the policy definitions into a group that can be applied to the management group.
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

g01d Highly Voted 1 year, 5 months ago
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously. However, you need to use an initiative, not a resource graph to bundle the policy definitions into a group that can be applied to the management group.
upvoted 28 times

ForeverStudent 1 year, 4 months ago
g01d is right.. You bundle up policies into Initiatives and apply the initiatives to the management groups. Not resource graphs.
upvoted 6 times

kdkdk Highly Voted 7 months ago
in the exams
upvoted 10 times

saby16 Most Recent 4 months ago
Correct answer should be no.
upvoted 1 times

Super_Pun 4 months ago
the correct answer is "NO" because the resource graph is incorrect
upvoted 2 times

sensa 4 months, 2 weeks ago
in exam.. 5
upvoted 2 times

Thi 5 months, 2 weeks ago
Answer : B. No (not relevant to resource graph)
Answer can be yes if appeard in exam like this: You decide to create management groups and then scope the policies at the management group level.
upvoted 1 times

shuhaidawahab 5 months, 3 weeks ago
ANSWER B. No
upvoted 1 times

kiketxu 7 months, 3 weeks ago
The question should be...
"You decide to create MG and then scope the policies at the MG level"
...and then, the answer is YES
upvoted 5 times

awssecuritynewbie 8 months ago
in the exam from what i heard

https://t.me/learningnets

upvoted 4 times

awssecuritynewbie 8 months, 3 weeks ago

but in the question it does not say the subs are under any sort of management groups ? so how we don't have any management group then how we can apply policy to?

upvoted 3 times

jt2214 10 months ago

this is a typo, should read :Solution: You create an initiative and an assignment that is scoped to a management group.
thus making it true.

upvoted 6 times

GraceCyborg 10 months, 1 week ago

should by typo (resource graph) = policy definition

upvoted 2 times

eug45 11 months, 2 weeks ago

No, B

The resource graph is used for querying resources and not for assigning policies.

upvoted 2 times

jenkiiz 1 year ago

the question was corrected so it's YES for MANAGEMENT GROUP

upvoted 10 times

gfhbox0083 1 year ago

B, for sure.
Use Management Group

upvoted 4 times

gfhbox0083 1 year ago

This series of questions appeared on my exam on 02/07/2020

upvoted 2 times

gboyega 1 year ago

CORRECT

upvoted 1 times

lnn_az 1 year, 1 month ago

Answer is B (No).

correct solution is to "Create a Management Group and assign an initiative to the Management Group"

upvoted 5 times

Rajuuu 1 year, 1 month ago

The answer should be to use Management Group and not a Resource Group/Graph .
No.

upvoted 1 times

https://t.me/learningnets

Question #42 *Topic 3*

HOTSPOT -

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

How should you configure the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [ ▼ ] == 4625
| summarize failed_login_attempts= [ ▼ ]
  latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
```

ActivityID / DataType / EventID / QuantityUnit

Count(), / Countif(), / Makeset(), / Split(),

Answer Area

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [ ▼ ] == 4625
| summarize failed_login_attempts= [ ▼ ]
  latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
```

ActivityID / DataType / EventID / QuantityUnit

Count(), / Countif(), / Makeset(), / Split(),

Correct Answer:

The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

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

https://t.me/learningnets

| project-away Account1

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

gboyega Highly Voted 1 year ago

Answer is Correct

upvoted 19 times

Davidq3 Highly Voted 1 year ago

Correct

upvoted 6 times

PM2 Most Recent 4 months, 1 week ago

in the exam

upvoted 5 times

zic04 5 months, 4 weeks ago

correct

upvoted 1 times

tuta 7 months ago

simple logic = correct

upvoted 5 times

maj79 1 year ago

agree with answer

upvoted 2 times

https://t.me/learningnets

Question #43 *Topic 3*

You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.
You need to modify Play1 to send email messages to a distribution group named Alerts.
What should you use to modify Play1?

A. Azure DevOps

B. Azure Application Insights

C. Azure Monitor

D. Azure Logic Apps Designer

Correct Answer: *D*
You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

ExamUser Highly Voted 1 year, 2 months ago
Correct...
upvoted 10 times

gustavo935 Highly Voted 1 year ago
The playbook names changed to Workflow automation
upvoted 9 times

Sanil_Kumar Most Recent 1 month, 3 weeks ago
D is Correct
upvoted 2 times

sensa 4 months, 2 weeks ago
in exam..6
upvoted 4 times

zic04 5 months, 3 weeks ago
D correct
upvoted 1 times

pppes 6 months, 2 weeks ago
Yep, you modify the playbook in the Logic App designer
upvoted 1 times

celomomo 7 months, 2 weeks ago
D is correct
upvoted 2 times

gboyega 1 year ago
Answer is Correct
upvoted 5 times

SadioMane 1 year, 1 month ago
Answer D is correct
upvoted 3 times

kristiann21 1 year, 1 month ago
correct answer
upvoted 4 times

https://t.me/learningnets

Question #44 *Topic 3*

You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Onboard Azure Active Directory (Azure AD) Identity Protection.

B. Create an Azure Storage account.

C. Implement Azure Advisor recommendations.

D. Create an Azure Log Analytics workspace.

E. Upgrade the pricing tier of Security Center to Standard.

Correct Answer: *BD* DE
D: 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

eug45 Highly Voted 11 months, 2 weeks ago
Wrong

Correct Answers is D and E

You need to upgrade the pricing tier of Azure Security Center to standard. You can also create a new Log Analytics workspace which can be used by Azure Security Center to send data with regards to your Azure resources
upvoted 32 times

Pankaj_Leo Highly Voted 10 months ago
D and E
upvoted 11 times

Keem Most Recent 1 month, 2 weeks ago
without storage account where will your Log Analytics workspace domicile? since All logs require to be stored ?i go for B and D
upvoted 1 times

kimalto452 3 weeks, 4 days ago
they two different things for example diagnostic logs can be saved in sa and/or log workspace...
upvoted 2 times

JAGUDERO 3 months ago
read well, the question is NOT what is the first thing you should do, which in this case would be "Change Tier Standard", the question is what is needed to configure "Custom Alerts", so the answer is correct.
upvoted 2 times

JOKERO 2 months, 1 week ago
Each correct answer presents part of the solution / what can you do with storage account + log analytics workspace ?
upvoted 2 times

glowglow 3 months, 1 week ago
but the question does not have anything about what tier your on so E can be ruled out.
for me B and D looks good.
upvoted 1 times

BalderkVeit 1 month, 3 weeks ago
it does. it says: "You create a new Azure subscription". Which means, you have default tier. which is... the one that requires upgrading to Standard.
upvoted 1 times

Sethoo 3 months, 3 weeks ago
It should be D and E. Without the standard tier, you can create custom rules
upvoted 2 times

milind8451 4 months, 3 weeks ago
Custom alerts feature is not available anymore in Security Center as of Jan 2021. This ques is out of date.
upvoted 7 times

https://t.me/learningnets

Nerd_Remo 5 months, 3 weeks ago

D & E are correct

upvoted 2 times

zic04 5 months, 3 weeks ago

D & E for me

upvoted 2 times

paulxyz90 6 months, 2 weeks ago

Quick note. What was STANDARD before is called DEFENDER now. Either one is the non-FREE tier. Microsoft page says - Security alerts are triggered by advanced detections and are available only with Azure Defender tier. So E is correct. You can view the alerts in the ASC portal page and you can also send them to Azure Log Analytics Workspace (or Azure Event Hubs) using the 'continuous export' feature. So that would be D. Therefore D&E are correct.

upvoted 8 times

msftman 6 months, 3 weeks ago

D & E are the correct answers. Log Analytics comes with a storage space so don't need an extra one.

upvoted 7 times

leaderbud 2 months, 1 week ago

For more details: https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging
'All logs are stored in block blobs in a container named $logs, which is automatically created when Storage Analytics is enabled for a storage account. The $logs container is located in the blob namespace of the storage account, for example: http://<accountname>.blob.core.windows.net/$logs. This container cannot be deleted once Storage Analytics has been enabled, though its contents can be deleted. If you use your storage-browsing tool to navigate to the container directly, you will see all the blobs that contain your logging data.'

upvoted 1 times

leaderbud 2 months, 1 week ago

Although this is when 'enabling logging for a storage', the idea is that Log Analytics create its own storage capability when you activate/deploy its features

upvoted 1 times

ipindado2020 9 months, 1 week ago

DE is the way

upvoted 5 times

jaykrist 9 months, 3 weeks ago

https://docs.microsoft.com/en-us/azure/security-center/security-center-features-retirement-july2019#custom-alert-rules-preview

upvoted 2 times

Saar5 10 months ago

so what is the correct answer?

upvoted 1 times

pmr123 1 year ago

You have to upgrade the pricing tier of security center to have custom alert rules feature

upvoted 3 times

Rave763 1 year, 2 months ago

Agreed , the replacement for this is Azure Sentinel. So just look out if the question is adpoted for that

upvoted 7 times

JohnCrawford 1 year, 8 months ago

Custom Alerts were only in Preview and have since been retired. https://docs.microsoft.com/en-us/azure/security-center/security-center-features-retirement-july2019#menu_customalerts

upvoted 8 times

https://t.me/learningnets

Question #45 *Topic 3*

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.
You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.
You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:
- Alert rules must support dimensions.
- The time it takes to generate an alert must be minimized.
- Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

A. Log

B. Log (Saved Query)

C. Metric

D. Activity Log

Correct 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

gfhbox0083 Highly Voted 1 year ago
C, for sure
There are many benefits for using Metric Alerts for Logs over query based Log Alerts in Azure; some of them are listed below:

Metric Alerts offer near-real time monitoring capability and Metric Alerts for Logs forks data from log source to ensure the same.
Metric Alerts are stateful - only notifying once when alert is fired and once when alert is resolved; as opposed to Log alerts, which are stateless and keep firing at every interval if the alert condition is met.
Metric Alerts for Log provide multiple dimensions, allowing filtering to specific values like Computers, OS Type, etc. simpler; without the need for penning query in analytics.
upvoted 18 times

AdnanEzzi Highly Voted 1 year, 2 months ago
The answer is correct. But the correct link is this - https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-logs
upvoted 12 times

SadioMane 1 year, 1 month ago
Thank you for sharing the link. It clearly mentions the dimension & logs need to be produced once
upvoted 2 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago
Metric Alerts offer near-real time monitoring capability and Metric Alerts for Logs forks data from log source to ensure the same.
Metric Alerts are stateful - only notifying once when alert is fired and once when alert is resolved; as opposed to Log alerts, which are stateless and keep firing at every interval if the alert condition is met.
Metric Alerts for Log provide multiple dimensions, allowing filtering to specific values like Computers, OS Type, etc. simpler; without the need for penning query in analytics.
upvoted 2 times

sensa 4 months, 2 weeks ago
in exam
upvoted 5 times

milind8451 4 months, 3 weeks ago
Right ans. Metric Alerts for Log provide multiple dimensions.
upvoted 1 times

pooppants 6 months, 1 week ago
had this in the exam
upvoted 6 times

DA0410 7 months, 2 weeks ago
Correct. Here dimension refers the multi instances monitoring for Process , i/o, network , cpu, mem, disk % utilization consumed by Application and accordingly when threshold is reached, alert shall be generated to prevent application performance degradation.

https://t.me/learningnets

upvoted 1 times

DA0410 7 months, 2 weeks ago

Solution also addresses generating two alerts only , alert one when threshold reached and alert 2 when issue resolved and threshould reaches to normal level. No multiple 100s of errors iin between.

upvoted 2 times

gboyega 1 year ago

C is correct according to the docs

upvoted 7 times

https://t.me/learningnets

Question #46 *Topic 3*

HOTSPOT -

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

- When Azure Sentinel identifies a threat, an incident must be created.
- A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

When Azure Sentinel identifies a threat, an incident must be created: [▼]
- Analytics
- Data connectors
- Playbooks
- Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel: [▼]
- Analytics
- Data connectors
- Playbooks
- Workbooks

Correct Answer:

Answer Area

When Azure Sentinel identifies a threat, an incident must be created: [▼]
- Analytics
- Data connectors
- Playbooks
- Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel: [▼]
- Analytics
- Data connectors
- Playbooks
- Workbooks

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

gcpbrig01 Highly Voted 4 months ago

Answer is correct. Analytics rule allows grouping of alerts into an incident and playbook can be configured to log a ticket in third party system as a response to the incident

upvoted 5 times

kimalto452 Most Recent 3 weeks, 4 days ago

playbook, workbook, notebook, mambook, daybook, microbook, winbook...

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

Easier way is to think of a Workbook as a Report, Playbooks take actions - and Now there are Notebooks - classic MS

upvoted 1 times

juandiegope 3 months, 2 weeks ago

The answer is correct based on the provided link
Guys!! What is the difference between WorkBook and PlayBook?

upvoted 1 times

https://t.me/learningnets

OhBee 3 months, 1 week ago

Good day!

From this source: https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview...

Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive experiences.

These can be found under your log analytics workspace resource or Azure Sentinel itself. I don't have much experience with this but its like a custom dashboard which lets you create graphs and other visual using KQL.

Playbooks here are related to Azure Sentinel. They are basically Logic Apps with a trigger that activates the Log App/Playbook when an Azure Sentinel query rule is matched.

upvoted 4 times

https://t.me/learningnets

Question #47 *Topic 3*

HOTSPOT -

You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

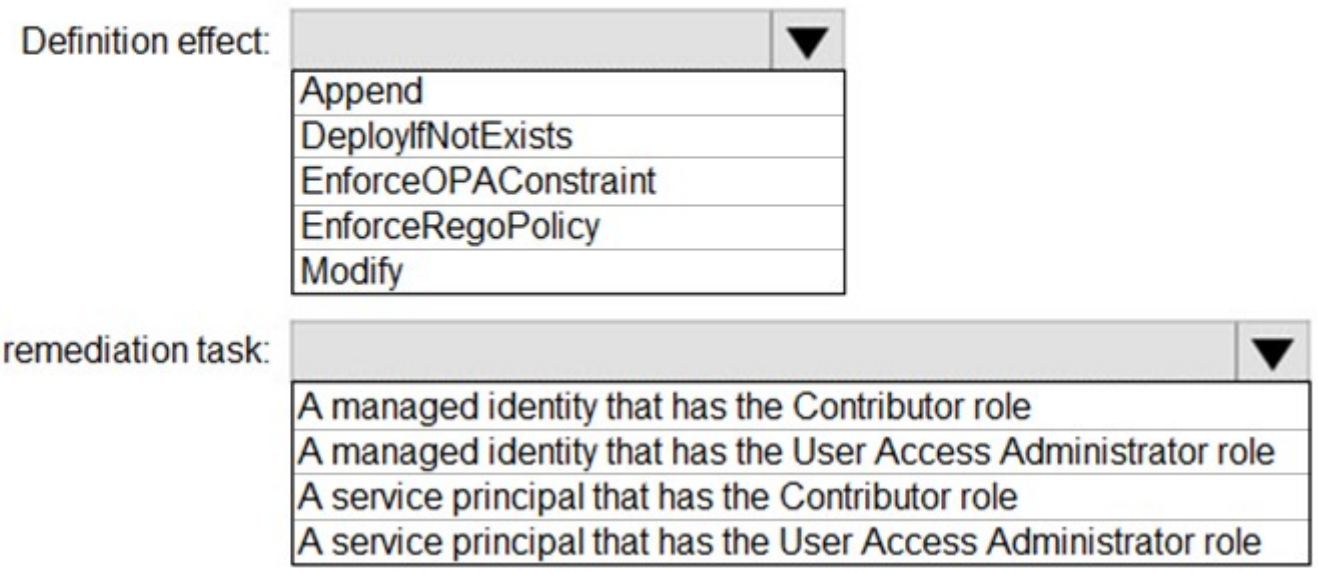
- When a new virtual machine is deployed, automatically install a custom security extension.
- Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

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

NOTE: Each correct selection is worth one point.

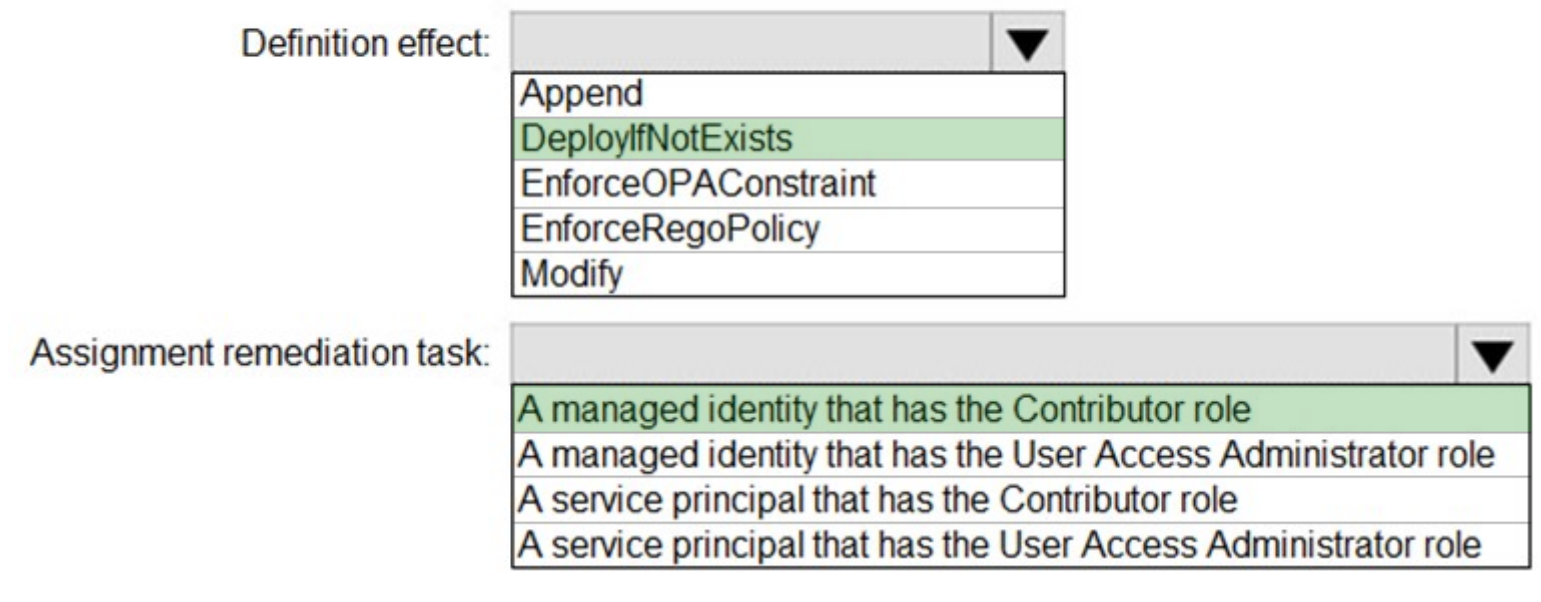
Hot Area:

Answer Area



Correct Answer:

Answer Area



Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Deepmindx 1 week, 6 days ago

IN THE EXAM 29/6/2021

upvoted 1 times

kimalto452 3 weeks, 4 days ago

correct

upvoted 2 times

JerryGolais 2 months, 3 weeks ago

1st box could be Modify, not sure
2nd box is definitely correct

upvoted 1 times

neokrieg 2 weeks, 5 days ago

1st box should be DeployIfNotExist as the Modify is only used to modify tags or fields while the former executes deployments

upvoted 1 times

Pinto 3 months, 3 weeks ago

https://t.me/learningnets

For box1 if the word was operation, we could go with Modify choice.
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

upvoted 2 times

https://t.me/learningnets

Question #48 *Topic 3*

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Category
Initiative1	Initiative definition	Security Center
Initiative2	Initiative definition	My Custom Category
Policy1	Policy definition	Security Center
Policy2	Policy definition	My Custom Category

You need to identify which initiatives and policies you can add to Subscription1 by using Azure Security Center.

What should you identify?

A. Policy1 and Policy2 only

B. Initiative1 only

C. Initiative1 and Initiative2 only

D. Initiative1, Initiative2, Policy1, and Policy2

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies

D999999 Highly Voted 3 months, 1 week ago

the correct answer should be " C. Initiative1 and Initiative2 only " as ASC does not support the integration of policies as is, just initiatives (which is a set of policies)

upvoted 9 times

jonav94 2 months, 4 weeks ago

I agree with this answer. From the link it says that "you can add your own custom initiatives" but in no one place it says that can add custom policy outside an initiative. And based on the options that the Security Policy inside ASC give us, and the answers given, the best one seems to be "Initiative1 and Initiative2 only"

upvoted 1 times

vijeet 2 months, 3 weeks ago

D is correct:
An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to. Assignments are inherited by all child resources. This design means that a definition applied to a resource group is also applied to resources in that resource group. However, you can exclude a subscope from the assignment.

upvoted 2 times

kimalto452 Most Recent 3 weeks, 4 days ago

no such option "Assign policy" in ASC...

upvoted 1 times

Jacquesvz 1 month ago

Ignore my previous post. D is correct. you can assign built in and custom policies & built in initiatives and custom initiatives to the subscription. my bad, sorry about the previous post. Check on Azure portal, Policy blade > Assignments (Assign Policy/ Assign Initiative)

upvoted 2 times

kimalto452 3 weeks, 4 days ago

You need to identify which initiatives and policies you can add to Subscription1 by using -----Azure Security Center----- not Policy...

upvoted 2 times

Jacquesvz 1 month ago

no correct answer on this question. From ASC you can 1.) Assign Security Centre default policy on the subscription, 2.) Assign Custom Initiatives (there are no ASC default Initiatives on the portal/blade).

upvoted 1 times

nicksu 1 month, 3 weeks ago

In a live portal I see only the option to assign a custom initiative, the answer should be C

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

Initiative is a set of policy definitions, it could have just one policy definition
ASC > Security Policy > Add custom initiatives
that is the only way to add custom policy or initiative to your subscription. I would have to go with D as well

upvoted 4 times

glowglow 3 months, 1 week ago

https://t.me/learningnets

D is correct.
"you can add your own custom initiatives. You'll then receive recommendations if your environment doesn't follow the policies you create. Any custom initiatives you create will appear alongside the built-in initiatives in the regulatory compliance dashboard"
https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies?pivots=azure-portal

upvoted 3 times

Question #49 *Topic 3*

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts.

What should you use to modify WF1?

A. Azure Application Insights

B. Azure Monitor

C. Azure Logic Apps Designer

D. Azure DevOps

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exercise-configure-playbook

Fred64 Highly Voted 2 months, 3 weeks ago
correct

upvoted 5 times

https://t.me/learningnets

Question #50 *Topic 3*

You have an Azure resource group that contains 100 virtual machines.
You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.
You need to identify which resources do NOT match the policy definitions.
What should you do?

A. From Azure Security Center, view the Regulatory compliance assessment.

B. From the Policy blade of the Azure Active Directory admin center, select Compliance.

C. From Azure Security Center, view the Secure Score.

D. From the Policy blade of the Azure Active Directory admin center, select Assignments.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal

ham56141 Highly Voted 5 months ago
Answer is wrong. I think A is the best fit.
upvoted 9 times

Fred64 Highly Voted 2 months, 1 week ago
A is not the best fit because it only display rgulatory compliance info. The question is about matching policy definition.

No other box are correct, BUT if we go to Policy blade there is a Compliance menu.
So I thing box B has a type and is the right solution
upvoted 5 times

L_c Most Recent 1 week, 1 day ago
A is best fit there is no Policy in AD admin panel
upvoted 1 times

kimalto452 3 weeks, 4 days ago
Correct answer go to Azure>>Search "Policy" >>> Select "Compliance"

To view the compliance details, follow these steps:

Launch the Azure Policy service in the Azure portal by selecting All services, then searching for and selecting Policy.

On the Overview or Compliance page, select a policy in a compliance state that is Non-compliant.

Under the Resource compliance tab of the Policy compliance page, select and hold (or right-click) or select the ellipsis of a resource in a compliance state that is Non-compliant. Then select View compliance details.
upvoted 2 times

rgullini 2 months, 1 week ago
Either this question is outdated or the answers are wrong. There is no Policy blade in the Azure AD Admin Center nor in the Azure AD section in the portal.
To view the policies, you need to go to "Policy" blade as per the link:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal
upvoted 3 times

Fred64 2 months, 2 weeks ago
A: check regulatory compliance obligations and complying with all the requirements of benchmark standards. Not what is asked

The answer is C, one just has to open the blade
upvoted 1 times

Fred64 2 months, 2 weeks ago
Sorry B, type mistake
upvoted 3 times

Cyberbug2021 2 months, 2 weeks ago
Correct Answer is B, even though policy blade its on its own now out of AAD, Go to Policy and click compliance. Question does not ask for regulatory compliance, but all policy compliance
upvoted 3 times

kimalto452 3 weeks, 4 days ago
no such option "Policy" in Azure Active Directory admin center, answer is incorrect

https://t.me/learningnets

upvoted 1 times

Azuriste 2 months, 2 weeks ago

Correct answer A
No policy blade exist under azure Active directory portal

upvoted 1 times

peacegrace 2 months, 2 weeks ago

Answer seems correct

Link : https://docs.microsoft.com/en-us/azure/governance/policy/how-to/determine-non-compliance

Under the Resource compliance tab of the Policy compliance page, right-click or select the ellipsis of a resource in a compliance state that is Non-compliant. Then select View compliance details.

upvoted 2 times

macco455 3 months, 3 weeks ago

It seems the best answer is not even listed as A is for regulatory compliance and the question is looking at Azure policy initiative that have been created. The only place you would go for compliance of azure policies is in the portal-Policy-Compliance blade. Here you can sort by resource group to see what resources are in and out of compliance. Doesn't this make sense? Am I reading it wrong?

upvoted 3 times

hang10z 3 months, 4 weeks ago

The answer is A, there is no policy blade in Azure AD admin portal. You can view what resources are not compliant for both custom and pre-defined policies under Regulator Compliance blade in Security Center.

upvoted 2 times

sureshatt 4 months ago

Answer is clearly A. We use this daily basis in our system. You go to security center -> Under Cloud Security -> Regulatory Compliance. You see all information you need to see there.
I cannot understand why people here "Blindly" say the answer is B. B is wrong because it says "Azure AD Admin Centre", the Azure AD Admin Center has nothing to do with Regulatory compliance and there is no option there. Please read the answer completely before confusing others. Thanks.

upvoted 3 times

milind8451 4 months, 2 weeks ago

I think given ans is correct go to Azure Policy -> Compliance, here you will see all policies listed and underneath that you can find which resources are not compliant.

upvoted 1 times

JAGUDERO 3 months ago

Azure Policy It is not within the 4 options, if it were, it would be the correct answer

upvoted 1 times

dadageer 4 months, 1 week ago

B would have been correct if it was "From the Policy blade of the Azure Subscription, select Compliance" but it says Azure Active Directory which has nothing to do with Policy. I think "A" is correct because if you go to Security Centre > Scroll down to Security Policy > Select your Subscription > Here you have options a) Assign a Security default Policy b) Industry regulatory standards (ISO, SOC..) c) Your custom initiatives. "c" is the option where you can add your custom initiative and hence "A" is the answer

upvoted 2 times

NunoVarelaa 4 months, 3 weeks ago

Don't listen to this people, go check by yourself...
This answer is 100% correct.
It can't be A and this is why: https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard ---> Only for ISO's and so on...
This initiative was created in Azure Policy, and you can see his Compliance by checking Compliance tab :)

upvoted 1 times

JaggRO 4 months, 2 weeks ago

The correct answer is A. See https://docs.microsoft.com/en-us/azure/governance/policy/concepts/regulatory-compliance. There are custom defined initiatives and here is description how to link custom initiatives to Security Center dashboard: https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies. So the answer is A.

upvoted 2 times

FoxBoss 4 months, 3 weeks ago

Really? “Azure Active Directory admin center” 😉

See:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/regulatory-compliance#regulatory-compliance-defined
“Customers can create their own Regulatory Compliance initiatives”

And Fig. 7 in this link that shows how to use ASC Regulatory Compliance to include a custom initiative:
https://francescomolfese.it/en/2020/03/azure-security-center-come-personalizzare-la-soluzione-per-soddisfare-i-propri-requisiti-di-sicurezza/

So, I believe it’s A

upvoted 3 times

https://t.me/learningnets

v078 4 months, 2 weeks ago

Regulatory compliance is something different, I would say. Although line is blurred, I believe, here answer is B - just go check Policy -> Compliance section on the Az portal.

upvoted 1 times

dadageer 4 months, 1 week ago

Whoever is saying B is not reading the option correctly. It is clearly mentioned "Azure Active Directory Admin". Do you see a Policy option under Active Directory blade? I'd encourage you to go and try to find it in Active Directory blade. Answer is A and I have explained below.

upvoted 2 times

LPGill 4 months, 4 weeks ago

A is correct

upvoted 1 times

deegadaze1 4 months, 4 weeks ago

A) supposed to be the correct answer!

upvoted 1 times

https://t.me/learningnets

Question #51 *Topic 3*

You have an Azure subscription named Subscription1.
You need to view which security settings are assigned to Subscription1 by default.
Which Azure policy or initiative definition should you review?

A. the Audit diagnostic setting policy definition

B. the Enable Monitoring in Azure Security Center initiative definition

C. the Enable Azure Monitor for VMs initiative definition

D. the Azure Monitor solution ג€˜Security and Auditג€™ must be deployed policy definition

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy https://docs.microsoft.com/en-us/azure/security-center/policy-reference

Kinanke Highly Voted 4 months, 3 weeks ago
Correct answer. See the ref:
https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy#manage-your-security-policies
upvoted 5 times

macco455 3 months, 2 weeks ago
Based on this link, the answer is not completely correct. You do not need to click enable monitoring, the policies just show up there when you go into security center- security policies. Plus Enable monitoring is in preview and thus not on the test
upvoted 2 times

sukhdeep Most Recent 3 months, 2 weeks ago
I can see default policy in Azure security center under security policies.
upvoted 4 times

rgullini 2 months, 3 weeks ago
Right. None of the answers provided is correct. You have to go to Security Center - Security Policy and there.
upvoted 1 times

Fred64 2 months, 2 weeks ago
B doesn't exist
but none of the other proposed are the solution. Is there a bug in this question?
upvoted 1 times

sureshatt 4 months ago
Is it really called "Monitoring in Azure Security Center" ??? Not a term I can see in any of the references. These are Azure Security Center policies, not "Monitoring"
upvoted 2 times

Jul1 5 months, 1 week ago
When you enable Security Center, the initiative named 'Azure Security Benchmark' is automatically assigned to all Security Center registered subscriptions
upvoted 2 times

deegadaze1 5 months ago
is it correct or not?
upvoted 1 times

https://t.me/learningnets

Question #52 *Topic 3*

DRAG DROP -

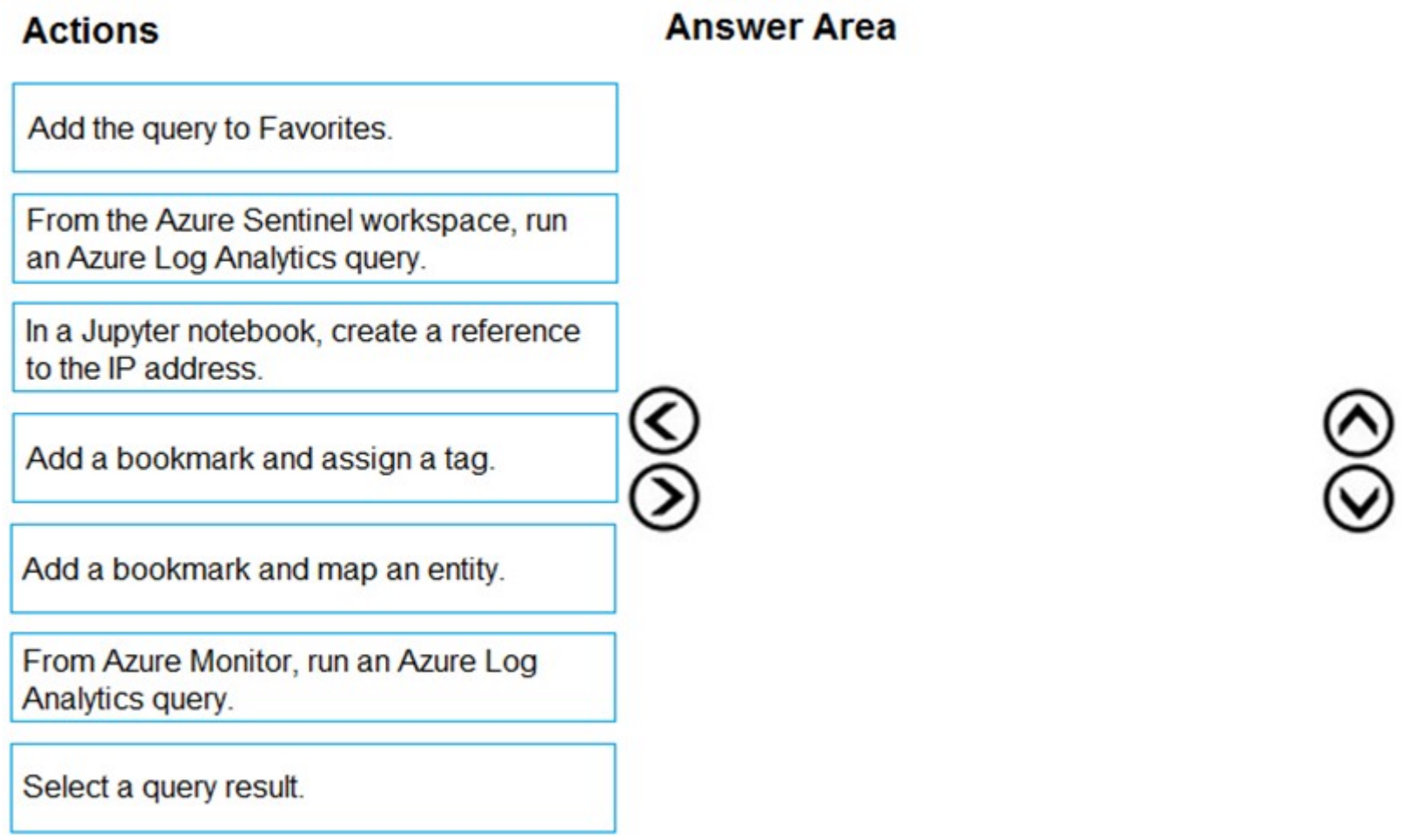
You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector.

You are threat hunting suspicious traffic from a specific IP address.

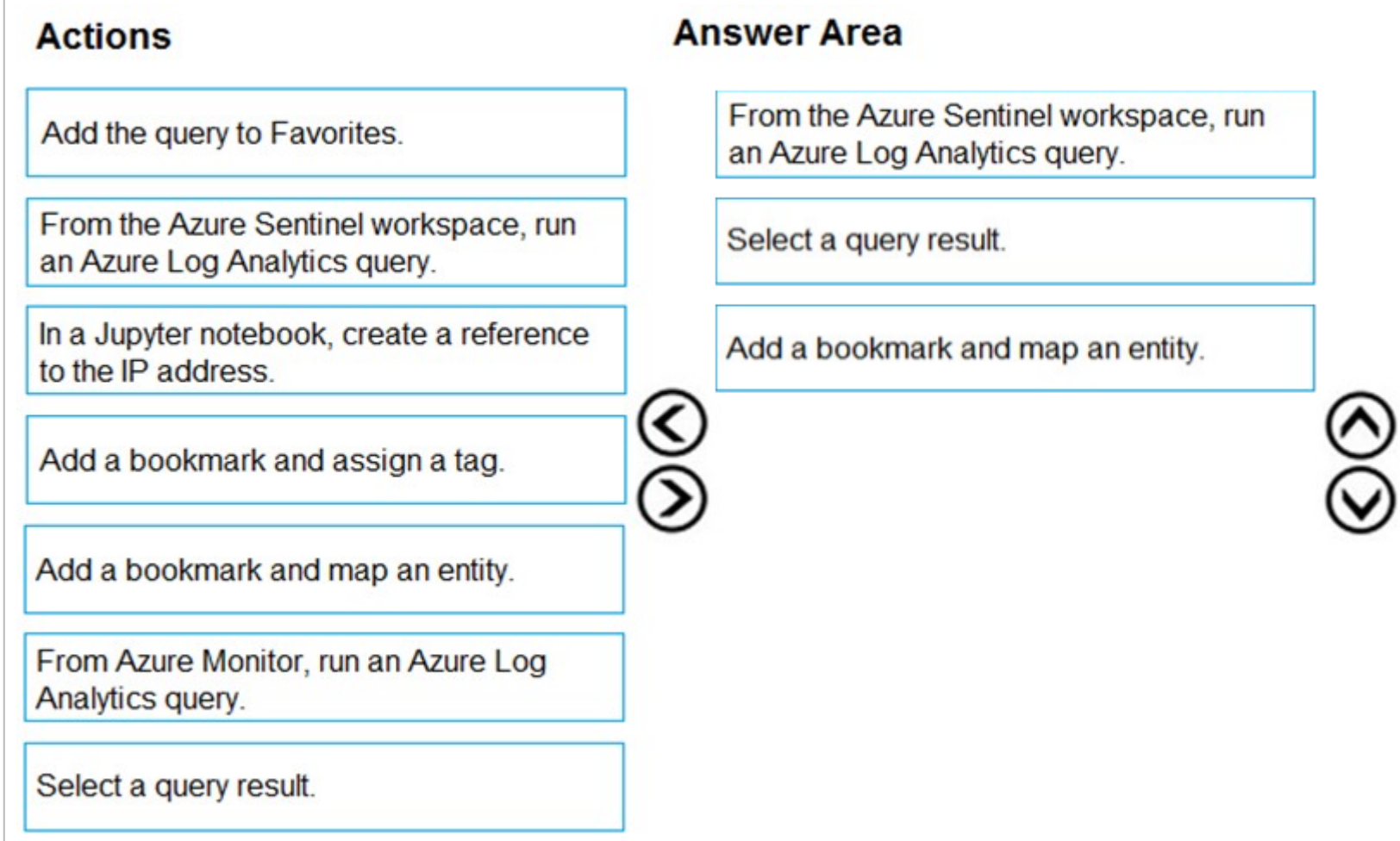
You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.

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:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

teamaws 3 months, 1 week ago

Answer is correct but the word choices are terrible

upvoted 2 times

Pinto 3 months, 3 weeks ago

https://t.me/learningnets

Seems correct as per https://docs.microsoft.com/en-us/azure/sentinel/bookmarks#exploring-bookmarks-in-the-investigation-graph

upvoted 3 times

https://t.me/learningnets

Question #53 *Topic 3*

HOTSPOT -

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.

Each subscription contains a resource group named RG1.

You need to ensure that for each subscription RG1 meets the following requirements:

- The members of Group1 are assigned the Owner role.
- The modification of permissions to RG1 is prevented.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Configure role-based access control (RBAC) role assignments by using:

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

- A resource lock
- A role-based access control (RBAC) role assignment at the resource group level
- Azure Blueprint assignments in locking mode

Correct Answer:

Answer Area

Configure role-based access control (RBAC) role assignments by using:

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

- A resource lock
- A role-based access control (RBAC) role assignment at the resource group level
- Azure Blueprint assignments in locking mode

hang10z Highly Voted 3 months, 4 weeks ago

Question 1 is Blueprints

Question 2:
Azure blueprint locking won't affect existing resources, RG1 already exists
A resource lock will either make RG1 read only or prevent deletion, not just stopping permission changes, not the best solution.
The only good answer is RBAC role assignment at the RG level.

upvoted 11 times

Pinto Highly Voted 3 months, 3 weeks ago

Azure blueprint with locks for sure is the answer to 2nd part. I think the whole question is derived from this article - https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking#overriding-locking-states

It's typically possible for someone with appropriate Azure role-based access control (Azure RBAC) on the subscription, such as the 'Owner' role, to be allowed to alter or delete any resource. This access isn't the case when Azure Blueprints applies locking as part of a deployed assignment. If the assignment was set with the Read Only or Do Not Delete option, not even the subscription owner can perform the blocked action on the protected resource.

This security measure protects the consistency of the defined blueprint and the environment it was designed to create from accidental or programmatic deletion or alteration.

upvoted 6 times

rgullini 2 months, 1 week ago

wrong, you need to prevent modifying permissions in the resource groups but not prevent modifying the resources themselves.

upvoted 1 times

https://t.me/learningnets

JAGUDERO 3 months ago

wrong, on the same link

Resource locks deployed by Azure Blueprints are only applied to resources deployed by the blueprint assignment. Existing resources, such as those in resource groups that already exist, don't have locks added to them.

upvoted 1 times

Lyonel Most Recent 1 day, 13 hours ago

Question 1: Blueprints - 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. [Ref. https://docs.microsoft.com/en-us/azure/governance/blueprints/overview]

Question 2: Resource Lock - use the 'ReadOnly' Resource Lock as it prevents modification of the Resource Group, including permissions. [Ref. https://techcommunity.microsoft.com/t5/itops-talk-blog/how-to-lock-azure-resources-to-prevent-modification-or-deletion/ba-p/356945] ... THIS ANSWER is based on the fact that in the question provided the Subscriptions are already created and are located in RG1.

upvoted 1 times

zsedo 1 month ago

Question2 should be blueprint as well (with Deny assignment):
Deny assignments block users from performing specific actions even if a role assignment grants them access. At this time, the only way you can add your own deny assignments is by using Azure Blueprints.
Otherwise owners will be able to modify the RBAC settings.

upvoted 2 times

Khumnan 3 months, 4 weeks ago

The answer should be blueprint on both
"With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint."

upvoted 2 times

milad123 4 months ago

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

upvoted 1 times

dadageer 4 months ago

For 2nd I think it should be Azure BP in locking mode because otherwise RG1 will have users of Group 1 as 'owners' who can change/assign roles so a Deployment of BP in locking mode will Deny it.

upvoted 2 times

Sethoo 4 months ago

Same here. I thought the last answer being putting a lock on the BP should be the answer

upvoted 1 times

Question #54 *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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and an assignment that is scoped to the Tenant Root Group management group.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

https://t.me/learningnets

Question #55 *Topic 3*

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards.

What should you use?

A. Azure Sentinel

B. Azure Active Directory (Azure AD) Identity Protection

C. Azure Security Center

D. Azure Advanced Threat Protection (ATP)

Correct Answer: *C*

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

Jul1 Highly Voted 5 months, 1 week ago

From Security Center's menu, select Regulatory compliance.

upvoted 14 times

deegadaze1 Most Recent 4 months, 2 weeks ago

Correct Answer is C

upvoted 3 times

https://t.me/learningnets

Question #56 *Topic 3*

DRAG DROP -

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

- Identify the user who deleted a virtual machine three weeks ago.
- Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration 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.

Select and Place:



Correct Answer:



Box1: Activity log -

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.

Activity logs help you determine the ג€what, who, and whenג€ for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs -

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

kristiann21 Highly Voted 1 year, 1 month ago

correct answer. undeniably.

upvoted 18 times

gfhbox0083 Highly Voted 1 year ago

Answer is Correct

upvoted 10 times

sensa Most Recent 4 months, 2 weeks ago

https://t.me/learningnets

in exam

upvoted 8 times

mayenite 5 months ago

In exam

upvoted 7 times

DA0410 7 months, 2 weeks ago

correct. I was monitoring manually 150 servers till 2008. First it took 3 months to analize all logs. Then it reduce to 3 days. I was making amber and red logs green by resolving issues. (SQL autheticcation error, due pwd change, Disk failure warning first amber, then red, then boom!, I prevented so many disasters by proactive monitoring)) I thought I am outdated, but Azure created things I was thinking as shortcoming in OS world in past for monitoring event logs. Now queries made it simple. I was thinking of such queries in 2002!

upvoted 6 times

DA0410 7 months, 2 weeks ago

Also I remember how we had caught hacker by evaluating logs. There was incident in 2012 when user reported unwanted suspicious folders created in d drive on windows server. I checked who created folder , user name %user% IP address was detected (RDP was used). We checked IP address on internet. SIM was pointing to country %country name%. Complained was logged. INtruder was caught with the help of SIM ISP provider telecom company. No tool was used Just log monitoring was used.

upvoted 8 times

AlaReAla 4 weeks ago

Wasn't azure launched in Feb'10?

upvoted 2 times

celomomo 7 months, 2 weeks ago

Correct

upvoted 1 times

Spamuel 11 months, 3 weeks ago

Correct, but think "Logs" should be titled "Resource Logs"

upvoted 3 times

Pinto 3 months, 3 weeks ago

Nope. Azure Resource logs ->Frequent data about the operation of Azure Resource Manager resources in subscription
https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit#types-of-logs-in-azure

upvoted 1 times

gboyega 1 year ago

Correct

upvoted 4 times

Jhonsteve83 1 year, 2 months ago

Correct

upvoted 3 times

https://t.me/learningnets

Question #57 *Topic 3*

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group
RG1	Resource group	*Not applicable*
VM1	Virtual machine	RG1
VM2	Virtual machine	RG1
ActionGroup1	Action group	RG1

VM1 and VM2 are stopped.

You create an alert rule that has the following settings:

- Resource: RG1
- Condition: All Administrative operations
- Actions: Action groups configured for this alert rule: ActionGroup1
- Alert rule name: Alert1

You create an action rule that has the following settings:

- Scope: VM1
- Filter criteria: Resource Type = "Virtual Machines"
- Define on this scope: Suppression
- Suppression config: From now (always)
- Name: ActionRule1

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 you start VM1, an alert is triggered.	○	○
If you start VM2, an alert is triggered.	○	○
If you add a tag to RG1, an alert is triggered.	○	○

Correct Answer:

Answer area

Statements	Yes	No
If you start VM1, an alert is triggered.	○	●
If you start VM2, an alert is triggered.	●	○
If you add a tag to RG1, an alert is triggered.	○	●

Box 1:

The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.

Box 2:

The scope for the action rule is not set to VM2.

Box 3:

Adding a tag is not an administrative operation.

References:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules

https://t.me/learningnets

JAGUDERO Highly Voted 3 months ago

NO: VM1 is suppressed, examplae maintenance
YES: Rule is OK
NO: Tags not Administrative operations

upvoted 10 times

Lobo 3 weeks, 3 days ago

NYY, Tags are administrative actions...

upvoted 1 times

wannabepro789 5 days, 20 hours ago

Can confirm - tested in lab
Adding a tag adds a 'Write Tags' operation event under RG1 activity log. Also, for completeness, obviously gets written to the subscription Activity logs as well.

upvoted 1 times

rctm_bm Most Recent 14 hours ago

Tested in Lab, and got the answer N/N/N

upvoted 1 times

JasonTest 2 months ago

No - because Suppression
No - because scope is VM1
No - add tag is not Administrative operation

upvoted 1 times

nicksu 1 month, 3 weeks ago

VM1 is in the scope of suppression rule but alert rule has in cope all administrative operations

upvoted 1 times

rgullini 2 months, 1 week ago

Answers are correct

upvoted 1 times

JerryGolais 2 months, 3 weeks ago

Action rule are in preview. Odd that Microsoft ask us about them, I did not even know what they were.
No Yes No is the right answer

upvoted 2 times

macco455 3 months, 2 weeks ago

No, alerts for VM1 are suppressed
Yes, based on alert rule
No, alerts cannot be created based on tags
Answer is correct, to me

upvoted 3 times

JhonyTrujillo 3 months, 3 weeks ago

Option 1 = No
Option 2 = No
Option 3 = No

upvoted 2 times

OhBee 3 months, 1 week ago

Downvote. Provide reasoning, please.

upvoted 2 times

https://t.me/learningnets

Question #58 *Topic 3*

DRAG DROP -

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

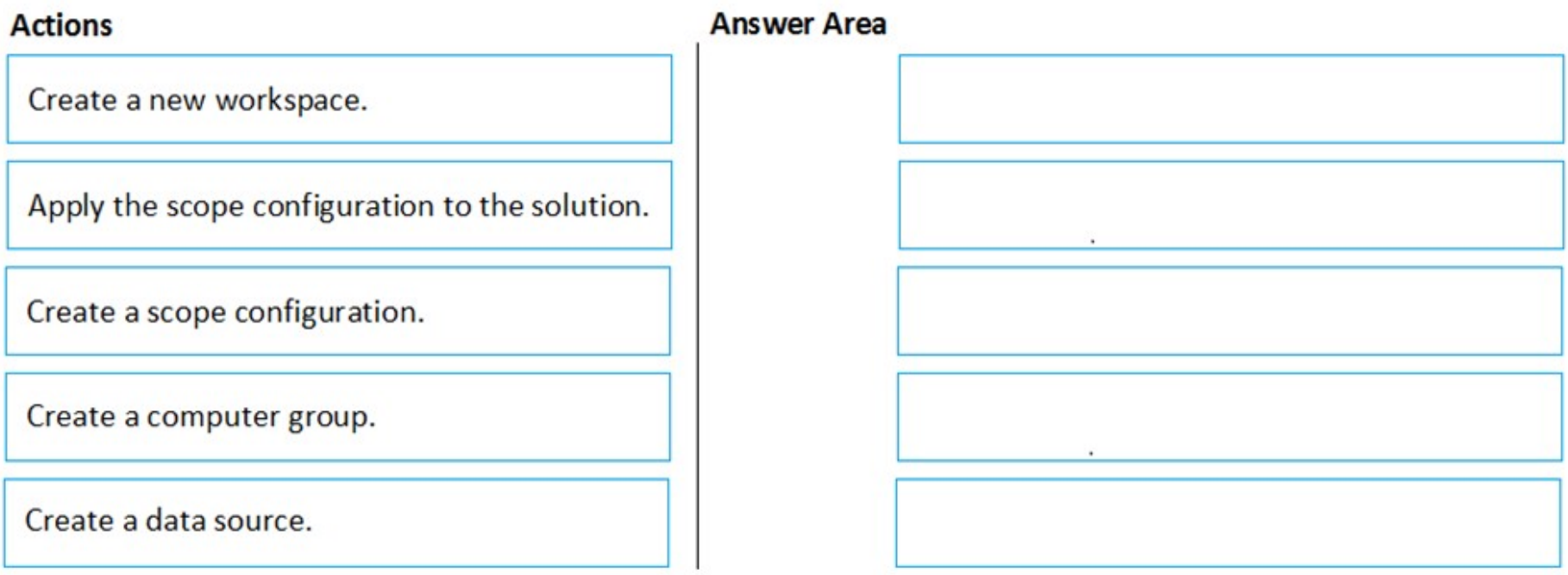
You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

You plan to add the System Update Assessment solution to LAW1.

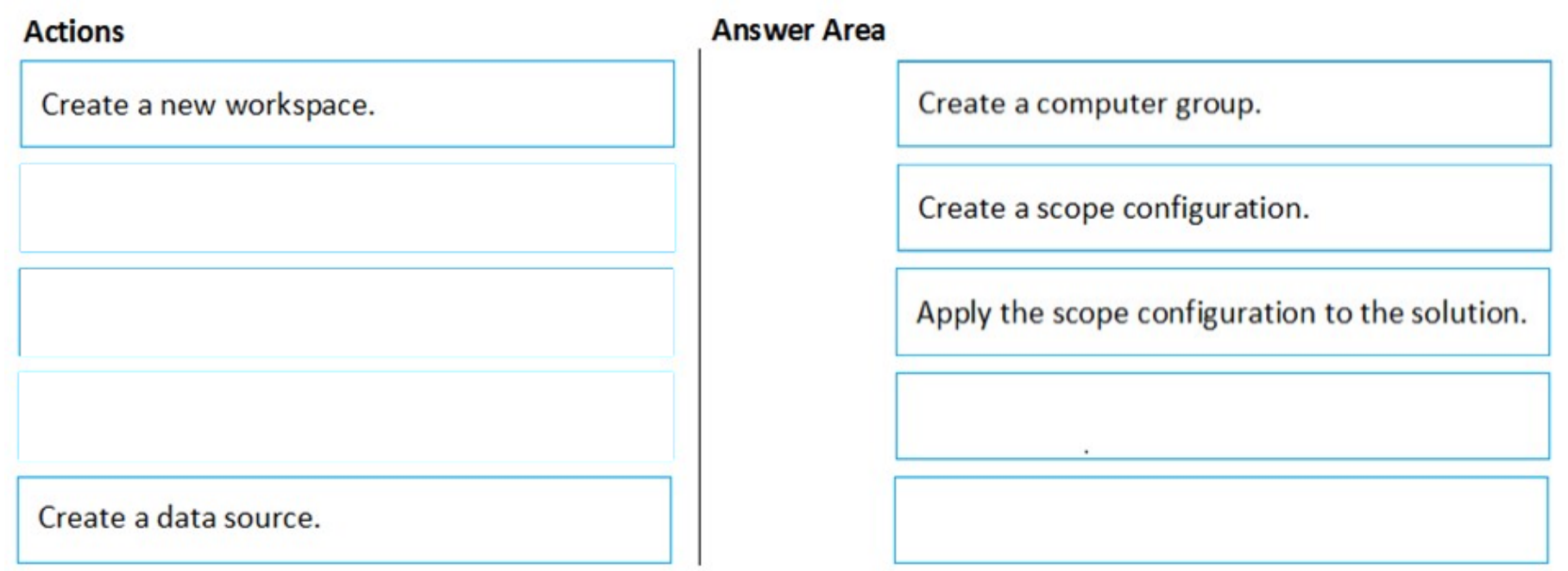
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

gfhbox0083 Highly Voted 1 year ago

The provided answer is Correct

upvoted 18 times

bystic 10 months ago

i was waiting for you to add "for sure" :D

upvoted 10 times

Daniel777 8 months, 1 week ago

For sure :)

upvoted 5 times

lnn_az Highly Voted 1 year, 1 month ago

answer is correct

upvoted 8 times

JAGUDERO Most Recent 3 months ago

in order correct: https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting#how-to-target-a-solution

upvoted 1 times

https://t.me/learningnets

rrv 4 months, 3 weeks ago

First create a computer group.

Then create a scope configuration

Then finally apply the scope configuration to the solution

upvoted 6 times

https://t.me/learningnets

Question #59 *Topic 3*

You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.
What should you configure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

B. an application security group

C. Azure Active Directory (Azure AD) conditional access

D. just in time (JIT) VM access

Correct Answer: *D*
Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.
When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security
Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

gfhbox0083 Highly Voted 1 year ago
D, for sure
upvoted 18 times

arytech 2 weeks, 3 days ago
This is what I call confidence!
upvoted 1 times

Ozwel 7 months ago
For sure!
upvoted 3 times

gboyega Highly Voted 1 year ago
D is correct
upvoted 8 times

prubio Most Recent 3 months, 3 weeks ago
Sorry but.... PIM should be activated to enable JIT, shouldn't it?
Therefore, I would choose A. What do you think?
upvoted 1 times

Ed2learn 3 weeks, 3 days ago
You don't have to have PIM for JIT.
upvoted 1 times

Ed2learn 3 weeks, 3 days ago
I should be more clear - You can use PIM for the required roles but it is not necessary to do so. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc
upvoted 1 times

kimalto452 3 weeks, 4 days ago
standart tier >defender for vm
upvoted 1 times

https://t.me/learningnets

OhBee 3 months, 1 week ago
I thought only Security Center was required.
upvoted 2 times

zic04 5 months, 3 weeks ago
Correct D
upvoted 2 times

tuta 7 months ago
D- No doubt
upvoted 2 times

Andy998 1 year ago
D is correct.
upvoted 4 times

Question #60 *Topic 3*

SIMULATION -

You need to ensure that web11597200 is protected from malware by using Microsoft Antimalware for Virtual Machines and is scanned every Friday at 01:00.

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

You need to install and configure the Microsoft Antimalware extension on the virtual machine named web11597200.

1. In the Azure portal, type Virtual Machines in the search box, select Virtual Machines from the search results then select web11597200.
Alternatively, browse to Virtual Machines in the left navigation pane.
2. In the properties of web11597200, click on Extensions.
3. Click the Add button to add an Extension.
4. Scroll down the list of extensions and select Microsoft Antimalware.
5. Click the Create button. This will open the settings pane for the Microsoft Antimalware Extension.
6. In the Scan day field, select Friday.
7. In the Scan time field, enter 60. The scan time is measured in minutes after midnight so 60 would be 01:00, 120 would be 02:00 etc.
8. Click the OK button to save the configuration and install the extension.

JhonyTrujillo 3 months, 3 weeks ago
0 = 12AM, 60 = 1AM, 120 = 2AM
upvoted 1 times

LiamRT 8 months, 2 weeks ago
You have to select 'Enable' under 'Run a scheduled scan'. The default selection is 'Disable'
upvoted 2 times

planb7000 11 months, 2 weeks ago
very good. the default is also 120 at 2:00 am
U can also increase it by 60 mins..nothing in between
upvoted 2 times

https://t.me/learningnets

Question #61 *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 logs11597200 Azure Storage account for 30 days.
To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*
You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.
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 doesnλ€™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 logs11597200 storage account.
8. In the Retention (days) field, enter 30.
9. Click the Save button to save the changes.

https://t.me/learningnets

Question #62 *Topic 3*

HOTSPOT -

On Monday, you configure an email notification in Azure Security Center to email notifications to user1@contoso.com.

On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Total number of Security Center email notifications about an RDP brute force attack on Tuesday: [1 / 2 / 3 / 4]

Total number of Security Center email notifications on Tuesday: [3 / 4 / 6 / 9 / 11]

Answer Area 4,7

Total number of Security Center email notifications about an RDP brute force attack on Tuesday: [1 / 2 / 3 / **4**]

Correct Answer:

Total number of Security Center email notifications on Tuesday: [3 / 4 / 6 / 9 / **11**]

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

https://t.me/learningnets

VJVSGP 4 days, 20 hours ago

In Exam on 10/7/2021

upvoted 1 times

Deepmindx 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 1 times

bhbh2020 2 weeks, 4 days ago

a maximum of one email per 6 hours (4 emails per day) for high-severity alerts
a maximum of one email per 12 hours (2 emails per day) for medium-severity alerts
a maximum of one email per 24 hours for low-severity alerts

first box = 4
second box = 7

upvoted 1 times

Geetar 1 month, 1 week ago

As per the link https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details the 6, 12, 24 makes sense when you work it out. The answers are 4 and 7. The given options for question 2 look to be wrong as reported by others.

upvoted 1 times

alexk0 1 month, 2 weeks ago

So I've read all comments and MS doc and still have no idea how this is calculated.

1. Calculate only by severity within a time window (box 2 is 7). So we consider that MS sends only ONE notification for the selected severity level within the corresponding period of hours. From my point of view, this is frustrating: f.e. Sec Center generated 20 high alerts of 5 different types within 6 hours but I was notified only once???

2. Calculate by severity & alert kind (box 2 is 11). f.e. Sec Center generated 20 high alerts of 5 different types and I got 5 notifications. This way makes sense for me.

But which of way is correct I cannot understand, it's not clear from the doc

upvoted 1 times

rgullini 1 month, 2 weeks ago

DISREGARD ALL MY PREVIOUS COMMENTS.
This question was in the exam. Correct answers are 4 and 7 (in the real exam, the second option shows "7" in the options.

upvoted 3 times

roy9889 2 months, 1 week ago

Box 2 - definitely not 11 (there are 2 low alerts .. only 1 can be notified in 24 hour window .. so there is that - it cannot be 11)

upvoted 1 times

rgullini 2 months, 1 week ago

Answers are correct.
Calculate the time of the day the high alerts were generated, and think in 1 every 6 hours only during Tuesday.
In the other hand, calculate the same for each other of the other ones. Even when the description is the same it doesn´t mean it is the same event (e.g.: There might be two different RDP brute force attacks.
Hence, showed answers are correct.

upvoted 1 times

rgullini 1 month, 2 weeks ago

DISREGARD ALL MY PREVIOUS COMMENTS.
This question was in the exam. Correct answers are 4 and 7 (in the real exam, the second option shows "7" in the options.

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

Think about it - if had an environment that generetated 100 unique high severity alerts every day would you like to be notified about them only 4 of them (times)? but if it was 100 of the same alert then being notified 4 times in 24 is okay. so look at the different alerts not just the severity.

upvoted 3 times

rgullini 2 months, 1 week ago

Finally, someone with the right explanation! thank you!

upvoted 1 times

rgullini 1 month, 2 weeks ago

DISREGARD ALL MY PREVIOUS COMMENTS.
This question was in the exam. Correct answers are 4 and 7 (in the real exam, the second option shows "7" in the options.

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

Given answer is correct, even if you apply the 4-2-1 (6-12-24hr) rule. 4 high alert, every 6 hr applies to A specific alert not to every high alert, which wouldn't make send. So you if you carefully apply the said rule you will get the given correct answer.

upvoted 3 times

rgullini 1 month, 2 weeks ago

https://t.me/learningnets

Given answer is not correct. DISREGARD ALL MY PREVIOUS COMMENTS.
This question was in the exam. Correct answers are 4 and 7 (in the real exam, the second option shows "7" in the options.

upvoted 1 times

souvik123 2 months, 1 week ago

The given answer is correct and I tend to agree with the explanation.
Box 1 - Each unique RDP alert does not repeat within the threshold based on the severity.
Box2 - Same is the case for all alerts which are not repeated withing threshold for every alert type.

upvoted 2 times

CASGTI 2 months, 2 weeks ago

Oh waaaaaaait! ... by default, it only sends for HIGH severity... not for all...
So, correct answer will be:
1) 1 (you will only get the first RDP alert, not the second, as you already got the 13:30 High alert, and its on the same 6 hours window)
2) 4 (max of 4 high alerts in 1 day)

upvoted 1 times

rgullini 2 months, 1 week ago

Answers showed are correct. For high alerts, the maximum is 4 mails during SAME DAY, PER ALERT. So the first alert at 01:00 will generate 3 emails during tuesday.

upvoted 1 times

rgullini 1 month, 2 weeks ago

DISREGARD ALL MY PREVIOUS COMMENTS.
This question was in the exam. Correct answers are 4 and 7 (in the real exam, the second option shows "7" in the options.

upvoted 1 times

CASGTI 2 months, 2 weeks ago

I am thinking... but another possibility is that the total email is "6" instead of 7 ... because the first two alerts, are just with 1 min different... so just guessing, maybe you get 1 email with the two? ...

upvoted 1 times

rgullini 2 months, 1 week ago

Think about this:
High alerts: Maximum 4 emails per day per alert
Medium: 2 emails maximum per day per alert
Low: 1 email maximum per day per alert

upvoted 1 times

CASGTI 2 months, 2 weeks ago

What I think is... Based on maximum emails per every X hours (1 every : H.6/M.12/L.24 hs):
You would only get "3" RDP alerts. (you wont get the one at 16:01, as you already got one high alert in this "6 hours window" at 13:30hs.
Total of alerts... I also tink it´s 7 ... but is not on the list... so not sure if we are seeing how this really works...
Say, divide the table in 6 and 12 hours windows ... mark one High in every window, you get 4 (out of 7)
then, mark one medium every 12 hours... since there are 2 only in different windows, you get both.
then, you get only the first "low" one, out of the 2.
So 4 + 2 + 1 = 7 ...

upvoted 2 times

rraviska 2 months, 3 weeks ago

RDP – 2 high, Medium -2 =4 Total – 3 high, 2 medium, 1 low = 6
a maximum of one email per 6 hours (4 emails per day) for high-severity alerts
a maximum of one email per 12 hours (2 emails per day) for medium-severity alerts
a maximum of one email per 24 hours for low-severity alerts

upvoted 2 times

JOKERO 2 months, 3 weeks ago

i think we are not reading all the informations in the table : first alert was triggered on Tuesday at 1:00 - last one at 23:... that means user has an interval of 12h to recieve notifications on Tuesday.
if severity = low or higher(2/4)
= Med or higher (2/3)
= High (2/2)

upvoted 1 times

stgunner 3 months ago

By default, Security Center emails subscription owners whenever a high-severity alert is triggered for their subscription.
Because of: "a maximum of one email per 6 hours (4 emails per day) for high-severity alerts" we have intervals 00 00 - 06 00 - 12 00 -18 00 - 00 00.
So in the first interval, we get mail in 06 00 about one of brutforce(01 01), then we get mail in 18 00 about alert in 16 01, so there are just two notifications about brutforce, and that's why first box is 2.
For second box is 3(4 if we know that before 00 00 was alerts), because notifications from 23 00 go to mail at 00 00 and it will be a new day.

upvoted 2 times

macco455 3 months, 2 weeks ago

Based on:
a maximum of one email per 6 hours (4 emails per day) for high-severity alerts
a maximum of one email per 12 hours (2 emails per day) for medium-severity alerts
a maximum of one email per 24 hours for low-severity alerts

https://t.me/learningnets

It should be
4
7
So the answers for this one are wrong and if its in the test it will have a otpion for 7 in the 2nd part.

upvoted 1 times

rgullini 1 month, 2 weeks ago

DISREGARD ALL MY PREVIOUS COMMENTS.
This question was in the exam. Correct answers are 4 and 7 (in the real exam, the second option shows "7" in the options.

upvoted 1 times

macco455 3 months, 2 weeks ago

the more I look at this one, the more I agree with Fred64 and not what I said above. We cannot answer this question as it sits given we are not told what the lowest severity is that gets an alert

upvoted 1 times

https://t.me/learningnets

Question #63 *Topic 3*

You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?

A. Azure Security Center

B. Azure Monitor

C. the Security admin center

D. Azure Storage Explorer

Correct Answer: *B* D
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/monitor-blob-storage?tabs=azure-portal

Pratham123 Highly Voted 2 months, 2 weeks ago
Answer is Azure Storage Explorer - No doubt
upvoted 15 times

samankaluarach Most Recent 3 days, 3 hours ago
B- correct answer.
"use Azure Storage logs in Azure Monitor instead of Storage Analytics logs. Azure Storage logs in Azure Monitor" as per link
https://docs.microsoft.com/en-us/azure/storage/common/manage-storage-analytics-logs?tabs=azure-portal
upvoted 1 times

Enitan 1 month, 3 weeks ago
D is the correct Answer
upvoted 3 times

nicksu 1 month, 3 weeks ago
Storage Explorer or AzCopy
upvoted 3 times

Sanil_Kumar 1 month, 3 weeks ago
Answer is D
upvoted 2 times

souvik123 2 months, 1 week ago
Answer is D - Azure Storage Explorer.
upvoted 3 times

Cyberbug2021 2 months, 2 weeks ago
Correct Answer is D - Azure Storage Explorer, These are storage account longs
https://docs.microsoft.com/en-us/azure/storage/common/manage-storage-analytics-logs?tabs=azure-portal
upvoted 4 times

https://t.me/learningnets

Question #64 *Topic 3*

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Azure Defender for the subscription.

Which resources can be protected by using Azure Defender?

A. VM1, VNET1, storage1, and Vault1

B. VM1, VNET1, and storage1 only

C. VM1, storage1, and Vault1 only

D. VM1 and VNET1 only

E. VM1 and storage1 only

Correct Answer: *A* C

Reference:

https://docs.microsoft.com/en-us/azure/security-center/azure-defender

tim_f Highly Voted 2 months, 1 week ago

Answer is C - VNET cannot be subscribed for defender

upvoted 5 times

samankaluarach Most Recent 3 days, 3 hours ago

Answer is right. A - Correct.

upvoted 1 times

dfernandes 4 days, 3 hours ago

Answer is C

upvoted 2 times

souvik123 2 months, 1 week ago

Correct answer should C- VM1, storage1, and Vault1 only. VNET cannot be subscribed for Defender.

upvoted 1 times

Pratham123 2 months, 2 weeks ago

Answer should be C.

Please check this link: https://docs.microsoft.com/en-us/azure/security-center/azure-defender#:~:text=What%20resource%20types%20can%20Azure,%2C%20your%20network%2C%20and%20more.

a

upvoted 3 times

Cyberbug2021 2 months, 2 weeks ago

Correct Answer is C

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

VNET is not in the list for Defender, you can check in the security center subscription. Servers, Storage and Key Vault is there. But no Network or Virtual Network in the list.

upvoted 3 times

https://t.me/learningnets

Question #65 *Topic 3*

DRAG DROP -

You have an Azure subscription that contains the following resources:

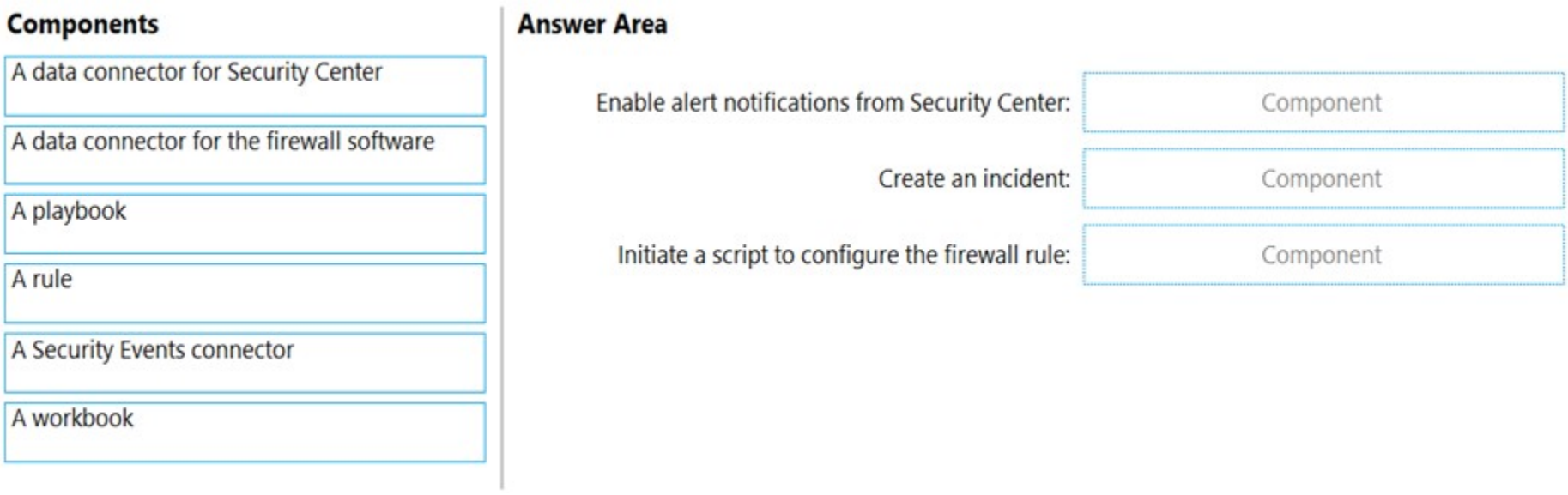
- A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
- An Azure function that contains a script to manage the firewall rules of the NVA
- Azure Security Center standard tier enabled for all virtual machines
- An Azure Sentinel workspace
- 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

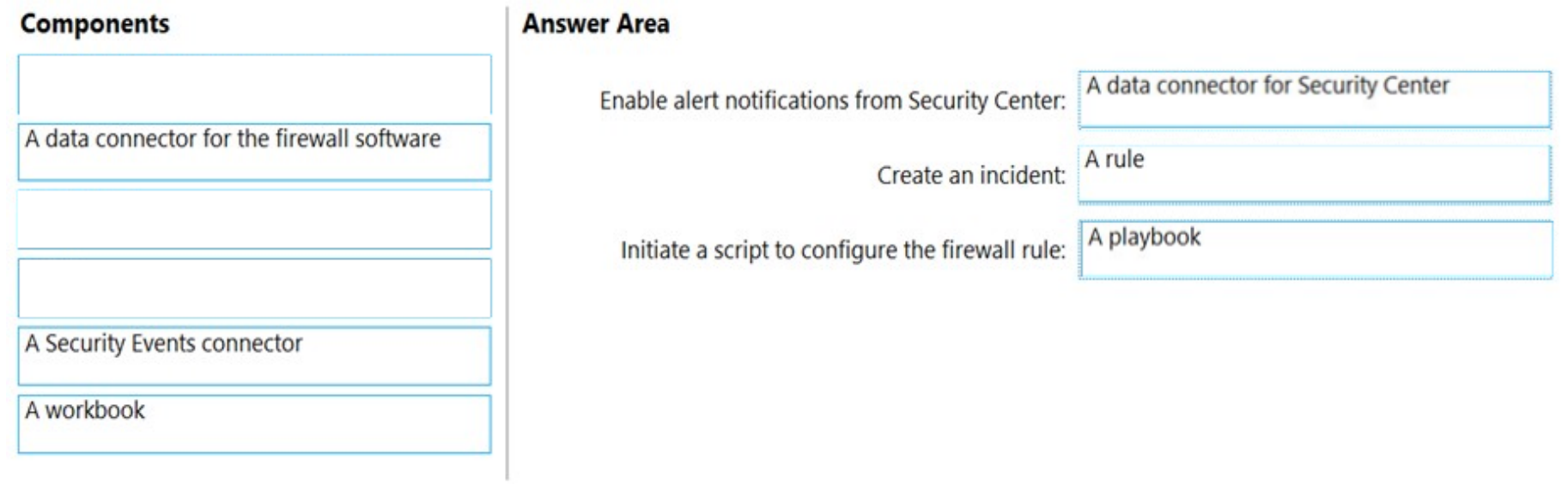
How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

https://t.me/learningnets

Question #66 *Topic 3*

You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access.
What should you configure?

A. an Azure policy assigned to RG1

B. a just in time (JIT) VM access policy in Azure Security Center

C. an Azure Active Directory (Azure AD) Privileged Identity Management (PIM) role assignment

D. an Azure Bastion host on VNET1

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained

thienvupt 1 week, 5 days ago
Correct answer
upvoted 1 times

Rume 1 week, 6 days ago
Given answer is correct
upvoted 1 times

https://t.me/learningnets

Question #67 *Topic 3*

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Description
EventHub1	Azure Event Hubs	**Not applicable**
Adf1	Azure Data Factory	**Not applicable**
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:

- An Azure Sentinel workspace
- An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel.

What should you configure for each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Subscription1:
- An Azure Log Analytics agent on a Linux virtual machine
- A Data Factory pipeline
- An Event Hubs namespace
- An Azure Service Bus queue

Subscription2:
- A new Azure Log Analytics workspace
- A new Azure Sentinel data connector
- A new Azure Sentinel playbook
- A new Event Grid resource provider

Correct Answer:

Answer Area

Log analytics agent
Azure Sentinel Playbook

Subscription1:
- An Azure Log Analytics agent on a Linux virtual machine
- A Data Factory pipeline
- **An Event Hubs namespace**
- An Azure Service Bus queue

Subscription2:
- **A new Azure Log Analytics workspace**
- A new Azure Sentinel data connector
- A new Azure Sentinel playbook
- A new Event Grid resource provider

jpons Highly Voted 2 weeks ago

Logs analytics agent and Sentinel data connector
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

upvoted 5 times

romaso82 Most Recent 14 hours, 26 minutes ago

BOX1: Azure log analytics agent
BOX2: A new azure sentinel playbook

upvoted 1 times

Topic 4 - Question Set 4

https://t.me/learningnets

Question #1 *Topic 4*

SIMULATION -

You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks.

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

You need to configure the backup policy for the Azure SQL database.

1. In the Azure portal, type Azure SQL Database in the search box, select Azure SQL Database from the search results then select Homepage.
Alternatively, browse to Azure SQL Database in the left navigation pane.
2. Select the server hosting the Homepage database and click on Manage backups.
3. Click on Configure policies.
4. Ensure that the Weekly Backups option is ticked.
5. Configure the How long would you like weekly backups to be retained option to 8 weeks.
6. Click Apply to save the changes.

Lexa Highly Voted 10 months, 3 weeks ago

Wrong. Azure portal doesn`t support backup management in the database`s blade. It`s available in the "SQL server" blade.
Go to Search -> "Homepage" -> Database overview -> Click on Server name -> Manage Backups -> Choose database "Homepage" -> Configure retention -> Long-term Retention Configurations set to 8 weeks.

upvoted 11 times

Scotimus Highly Voted 9 months, 1 week ago

The solution instructions seem correct. Step 2 states "Select the server hosting the Homepage database" as there is a link to the Server in the Overview blade of the SQL Database.

upvoted 5 times

Johnshoww Most Recent 8 months, 3 weeks ago

Did you guys know if simulations are included in the exam?

upvoted 2 times

Rafael1984 7 months ago

No have more labs for this exam

upvoted 1 times

Stuudent 6 months, 4 weeks ago

I have been trying to find some reliable lab excercises but I am sad to say I have failed. Anyone can provide any examples?

upvoted 1 times

Kampo 10 months, 1 week ago

Lexa is correct. "Manage Backup" navigation is under SQL server and not under Database.

upvoted 1 times

https://t.me/learningnets

Question #2 *Topic 4*

SIMULATION -
You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV11597200.
To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*
You need to configure an option in the Advanced Access Policy of the key vault.
1. In the Azure portal, type Azure Key Vault in the search box, select Azure Key Vault from the search results then select the key vault named KV11597200.
Alternatively, browse to Azure Key Vault in the left navigation pane.
2. In the properties of the key vault, click on Advanced Access Policies.
3. Tick the checkbox labelled Enable access to Azure Resource Manager for template deployment.
4. Click Save to save the changes.

planb7000 Highly Voted 11 months, 2 weeks ago
You will get lost in properties theres nothing there...August 2020....
just click access policies in the left pane of the KV

the box you need to check to enable access of the ARM templates is the 2nd of 3.
upvoted 13 times

Aanandan Most Recent 11 hours, 49 minutes ago
There is no Advanced Access Policies option , just select access policies on left navigation panel and tick the Azure Resource Manager for template deployment option
upvoted 1 times

https://t.me/learningnets

Question #3 *Topic 4*

HOTSPOT -

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Performance	Account kind	Azure Data Lake Storage Gen2
storage1	Standard	BlobStorage	Enabled
storage2	Premium	BlockBlobStorage	Disabled
storage3	Standard	Storage	Disabled
storage4	Premium	FileStorage	Disabled
storage5	Standard	StorageV2	Enabled

You enable Azure Defender for Storage.

Which storage services of storage5 are monitored by Azure Defender for Storage, and which storage accounts are protected by Azure Defender for Storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Monitored storage5 services:
- File services only
- Data Lake Storage only
- File services and table services only
- File service and Data Lake Storage only
- Data Lake Storage, file services, and table services

Protected storage accounts:
- storage3 and storage5 only
- storage1, storage2, and storage5 only
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

Correct Answer:

Answer Area

Monitored storage5 services:
- File services only
- Data Lake Storage only
- File services and table services only
- File service and Data Lake Storage only
- Data Lake Storage, file services, and table services

Protected storage accounts:
- storage3 and storage5 only
- storage1, storage2, and storage5 only
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center

thienvupt 1 week, 5 days ago

1st: File service and Data Lake Storage only
2nd: storage1, storage4, and storage5 only

upvoted 2 times

ChinkSantana 1 week, 6 days ago

Not sure about the 1st dropdown, but the 2nd dropdown choice is correct.

Availability
Azure Defender for Storage is currently available for Blob storage, Azure Files, and Azure Data Lake Storage Gen2. Account types that support Azure Defender include general-purpose v2, block blob, and Blob storage accounts.

https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center

upvoted 2 times

https://t.me/learningnets

Question #4 *Topic 4*

You have an Azure subscription that contains as Azure key vault and an Azure Storage account. The key vault contains customer-managed keys.
The storage account is configured to use the customer-managed keys stored in the key vault.
You plan to store data in Azure by using the following services:

- Azure Files
- Azure Blob storage
- Azure Log Analytics
- Azure Table storage
- Azure Queue storage

Which two services support data encryption by using the keys stored in the key vault? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Table storage

B. Azure Files

C. Blob storage

D. Queue storage

Correct Answer: *BC*
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

thienvupt 1 week, 5 days ago
Correct answer
upvoted 1 times

https://t.me/learningnets

Question #5 *Topic 4*

SIMULATION -

You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.

To complete this task, sign in to the Azure portal.

You do not need to wait for the task to complete.

Correct Answer: *See the explanation below.*

You need to enable the Web Application Firewall on the Application Gateway.

1. In the Azure portal, type Application gateways in the search box, select Application gateways from the search results then select the gateway named

Homepage-AGW. Alternatively, browse to Application Gateways in the left navigation pane.

2. In the properties of the application gateway, click on Web application firewall.

3. For the Tier setting, select WAF V2.

4. In the Firewall status section, click the slider to switch to Enabled.

5. In the Firewall mode section, click the slider to switch to Prevention.

6. Click Save to save the changes.

Ppetr0 2 months, 2 weeks ago

I would use firewall mode "protection" as long as they don't ask to block some traffic.

Check for WAF modes on this page
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

Should say in "Settings" Section - Properties in left pane are not used for configuration

upvoted 1 times

Nnanna29 7 months, 3 weeks ago

Regarding the mode, as long as the application gateway tier is WAF, all traffic would be inspected by the gateway whether in Detection or Prevention mode

upvoted 2 times

planb7000 11 months, 2 weeks ago

2. In the properties (SECTION) of the application gateway...

upvoted 4 times

https://t.me/learningnets

Question #6 *Topic 4*

SIMULATION -

You need to create a web app named Intranet11597200 and enable users to authenticate to the web app by using Azure Active Directory (Azure AD).

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

1. In the Azure portal, type App services in the search box and select App services from the search results.
2. Click the Create app service button to create a new app service.
3. In the Resource Group section, click the Create new link to create a new resource group.
4. Give the resource group a name such as Intranet11597200RG and click OK.
5. In the Instance Details section, enter Intranet11597200 in the Name field.
6. In the Runtime stack field, select any runtime stack such as .NET Core 3.1.
7. Click the Review + create button.
8. Click the Create button to create the web app.
9. Click the Go to resource button to open the properties of the new web app.
10. In the Settings section, click on Authentication / Authorization.
11. Click the App Service Authentication slider to set it to On.
12. In the Action to take when request is not authentication box, select Log in with Azure Active Directory.
13. Click Save to save the changes.

Cyberbug2021 2 months, 2 weeks ago

app services not to be confused with application services - stupid azure

upvoted 1 times

macco455 3 months, 2 weeks ago

Correct
https://docs.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service

upvoted 1 times

https://t.me/learningnets

Question #7 *Topic 4*

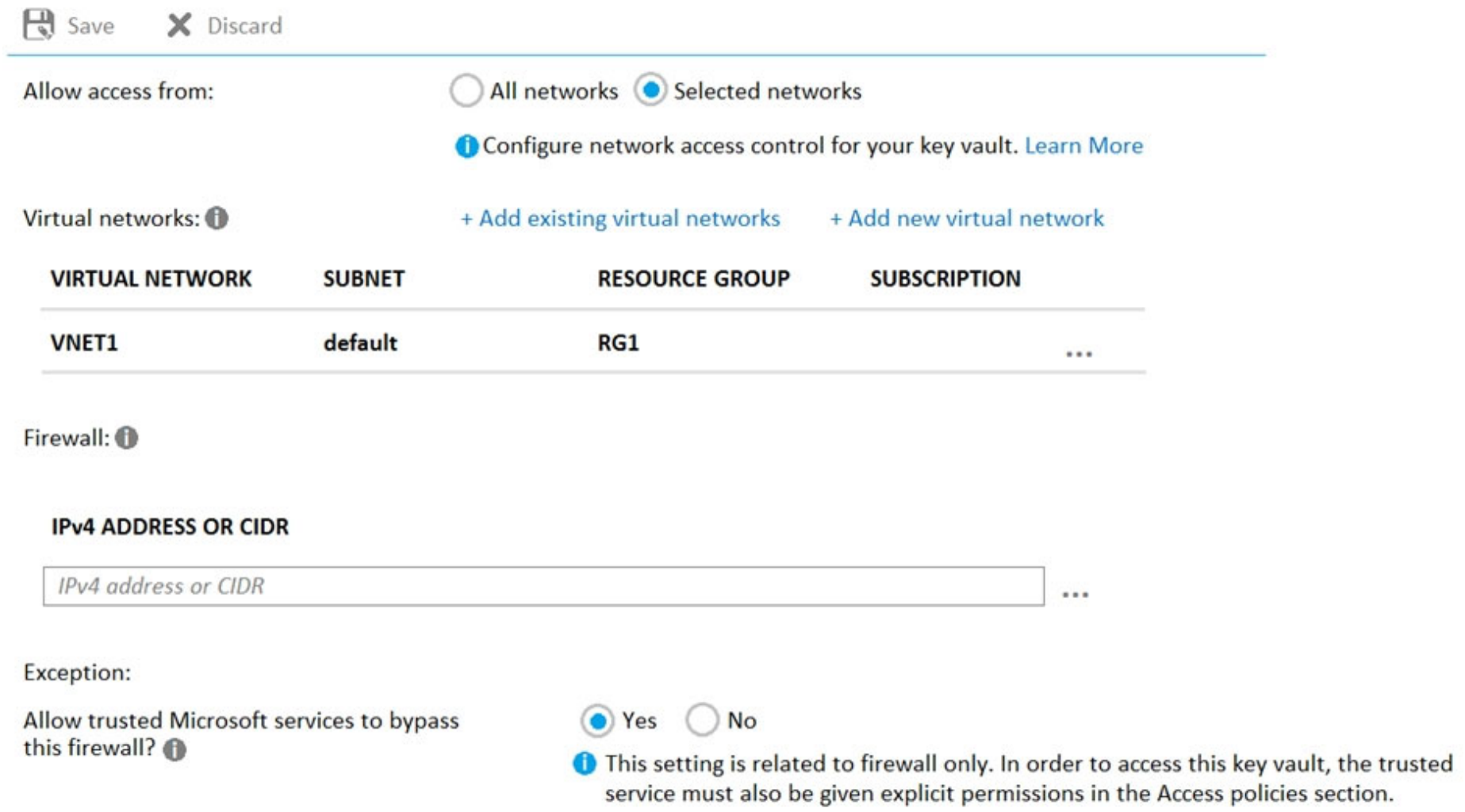
HOTSPOT -

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption.

KeyVault1 is configured as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	○	○
From VM2, users can manage the keys and secrets stored in KeyVault1.	○	○
VM2 can use KeyVault for Azure Disk Encryption	○	○

https://t.me/learningnets

Correct Answer:

Answer Area

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	○	○
From VM2, users can manage the keys and secrets stored in KeyVault1.	○	○
VM2 can use KeyVault for Azure Disk Encryption	○	○

sobby Highly Voted 4 months ago

VM2 in not allowed access to KV. Ans is
Yes
No
Yes

upvoted 37 times

nihao381 3 months, 4 weeks ago

Yes, No, Yes. VM2 can use Azure Disk Encryption with this Key Vault as that is a trusted Microsoft service.
https://docs.microsoft.com/en-us/azure/key-vault/general/overview-vnet-service-endpoints#trusted-services

upvoted 5 times

dadageer 4 months ago

Yes, No, No - How can VM2 access Vault for Disk Encryption when VNET2 is not allowed access.

upvoted 5 times

rgullini 2 months, 1 week ago

Because the Disk Encryption is a Trusted service which is allowed to bypass the firewall.

upvoted 3 times

Super_Pun 4 months ago

I thought that @sobby means "VM2 can use KeyVault for Disk Encryption" but need to configure it first.

upvoted 1 times

rgullini 2 months, 1 week ago

And it is configured as stated in the question

upvoted 1 times

macco455 Highly Voted 3 months, 2 weeks ago

Yes, Allowed thru firewall due to VNET1 having access thru firewall
No, Not allowed thru firewall since it is in VNET2(has no access thru firewall) not VNET 1
Yes, Since Allow Trusted Microsoft Services to bypass this firewall is checked, this allows access to key vault for disk encryption based off the trusted service list at this link:
https://docs.microsoft.com/en-us/azure/key-vault/general/overview-vnet-service-endpoints#trusted-services

upvoted 11 times

redbeard Most Recent 2 months, 1 week ago

I notice vnet1 and vnet2 both have the same subnet. Would this imply they are peered and if so would that make any differences with the questions?

upvoted 1 times

DCarma 2 weeks, 6 days ago

You aren't provided with a subnet mask, so you can't know that. Could be 10.7.0.4/26 and 10.8.0.4/16 for all you know.

upvoted 1 times

sureshatt 3 months, 2 weeks ago

my answer is: NO, NO, YES

NO:
VM1 cannot access the Keyvault. Unless the subnet in which VM1 lives has enabled service endpoint “Microsoft.Storage”, the VM1 will be using its public IP to connect to the KV, therefore the firewall will block it. Users accessing KV using VM1 is not treated as “Trusted Microsoft Service”. The requests will be blocked.

NO:
VM2 will be blocked due to the same reason as above.

YES:

https://t.me/learningnets

Azure Disk Encryption is a “Trusted Microsoft Service” which will bypass the firewall. Next, the question says the policy is set to allow Azure Disk Encryption to access the Keyvault. Therefore VM2 can use the keyvault for disk encryption unless they are in different regions.

upvoted 4 times

rgullini 2 months, 1 week ago

Wrong for the First:
When you select the allowed networks, today the option says "Private Endpoints and selected Network" so you don´t need to configure a endpoint unless you want to just redirect the traffic thru the Azure backbone.

upvoted 1 times

fabianotrd 3 months, 3 weeks ago

The access policy allows "enable to acces to zzure disk encryption" not to "users manage the keys and secrets" So No, No and No because the firewall rule "access from VNET1"

upvoted 6 times

alexander11 1 month, 3 weeks ago

I would say that it's No, No and Yes
Disk encryption is a trusted service:
https://docs.microsoft.com/en-us/azure/key-vault/general/overview-vnet-service-endpoints

upvoted 1 times

Khumnan 3 months, 4 weeks ago

The Azure Disk Encryption can access Key Vault as long as
"You must select the option in the Azure Key Vault access policy settings to enable access to Azure Disk Encryption for volume encryption. If you have enabled the firewall on the key vault, you must go to the Networking tab on the key vault and enable access to Microsoft Trusted Services."
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

upvoted 2 times

hang10z 3 months, 3 weeks ago

YES, NO, YES

upvoted 2 times

AcTiVeGrEnAdE 3 months, 4 weeks ago

My vote is also Yes, No, No due to VNET2 not being allowed

upvoted 5 times

rgullini 2 months, 1 week ago

Encryption is a trusted service, which can bypass the firewall so, number 3 is Yes

upvoted 2 times

Sethoo 4 months ago

My first take is also Yes, No , No. No for 2 and 3 because the VNET2 is not on the allowed network and thus it cannot access the key vault.

upvoted 3 times

https://t.me/learningnets

Question #8 *Topic 4*

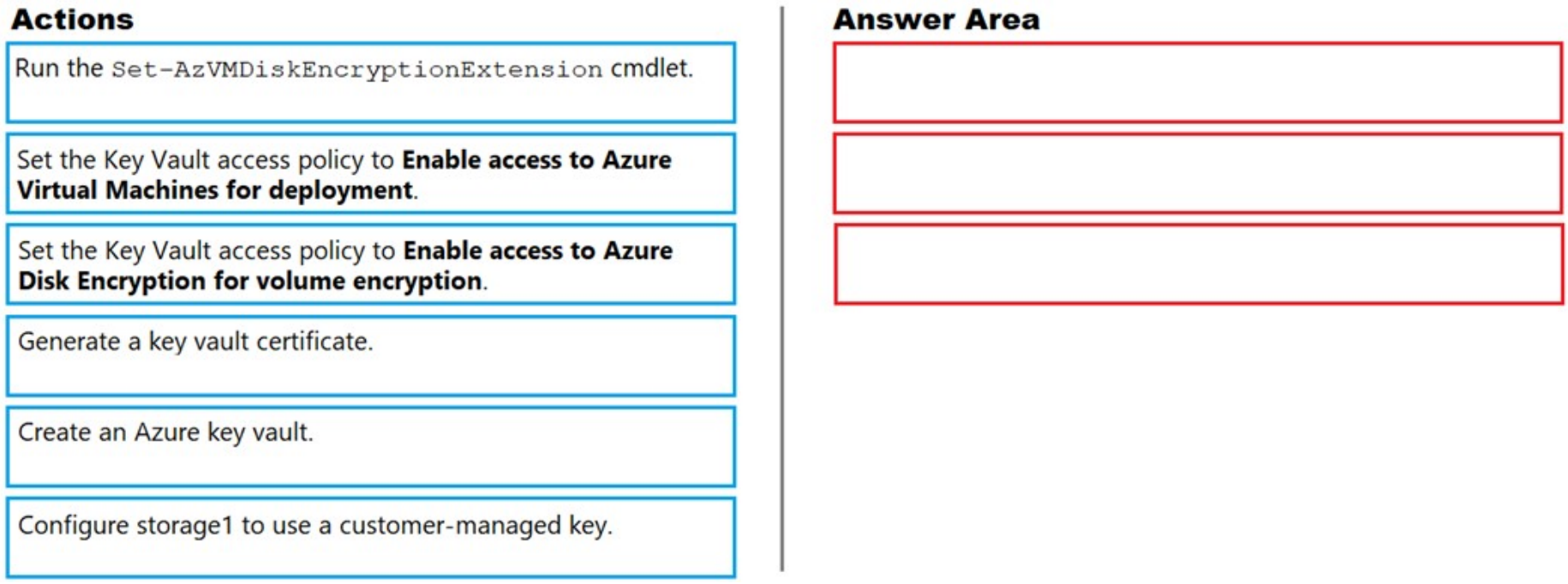
DRAG DROP -

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

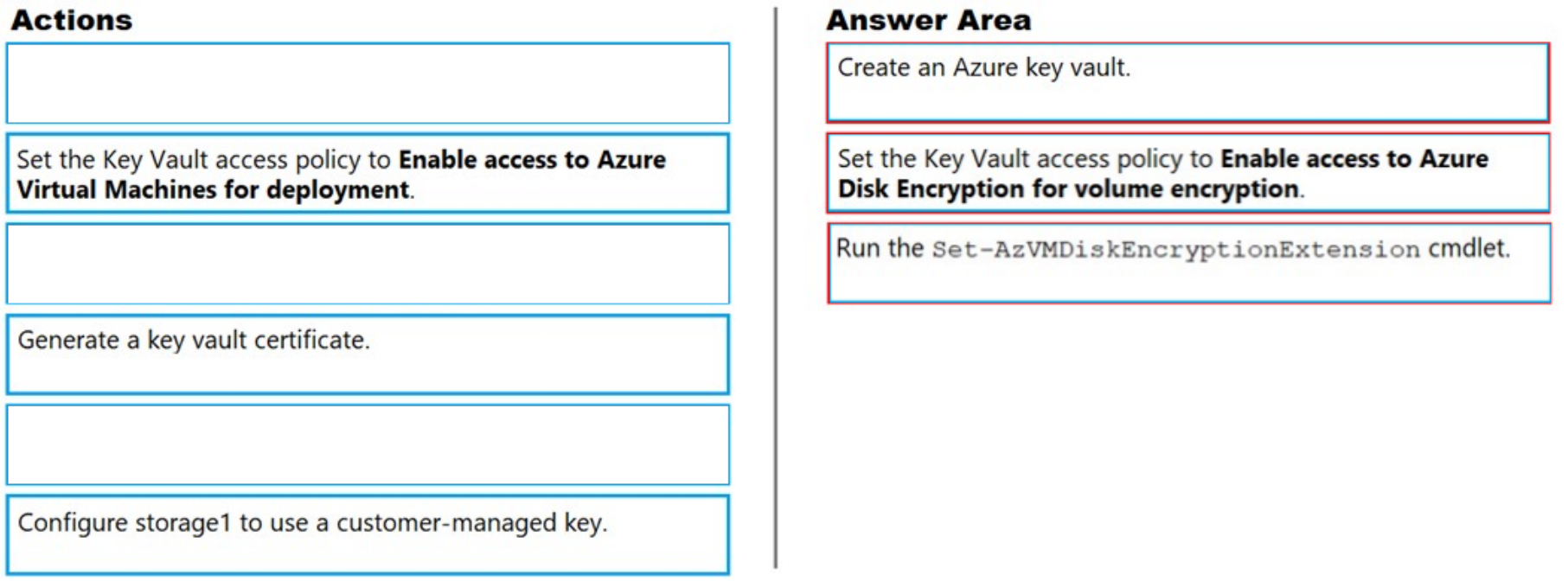
You need to enable Azure Disk Encryption for VM1.

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:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

JerryGolais 2 months, 3 weeks ago

Does it matter if you run the command before you set the access policy?

upvoted 2 times

ZakS 1 month, 3 weeks ago

I think for exams, it is better to take the order that will work 100% of the time, i.e. if we run the command first, then there is a period of time (let's say a few seconds) till you make config changes to the Key Vault settings when the command you have executed will fail, i.e. the VM cannot use the KV for disk encryption. If you do the order specified, then the KV is ready for disk encryption and the VM can use it as soon as the command is run.

upvoted 3 times

https://t.me/learningnets

Question #9 *Topic 4*

SIMULATION -
You need to enable Advanced Data Security for the SQLdb1 Azure SQL database. The solution must ensure that Azure Advanced Threat Protection (ATP) alerts are sent to User1@contoso.com.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Correct Answer: *See the explanation below.*
1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the Security section and select Advanced data security.
3. Click on the Settings icon.
4. Tick the Enable Advanced Data Security at the database level checkbox.
5. Click Yes at the confirmation prompt.
6. In the Storage account select a storage account if one isnλ€™t selected by default.
7. Under Advanced Threat Protection Settings, enter User1@contoso.com in the Send alerts to box.
8. Click the Save button to save the changes.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security

thomastrain Highly Voted 8 months ago
This has changed. Now you must go to Azure Sql servers -> click on your server name.
Security -> Security Center. Under Advanced Threat Protection enter email address: User1@contoso.com and click save.
upvoted 6 times

Stuudent 6 months, 3 weeks ago
Not necessarily. If you go to the database>Security>Security Center, click on Settings icon in the bar above the graphs, check "Enable Azure Defender for SQL server settings", you will get a following message:
"This enables Azure Defender for SQL at the database level, enabling you to receive separate Advanced Threat Protection alerts for this database only. Generally we recommend enabling Azure Defender for SQL at the Server level, unless you have a particular requirement to separately generate alerts for this database. Do you want to continue?"
Tested in live Azure environment.
upvoted 9 times

https://t.me/learningnets

Question #10 *Topic 4*

SIMULATION -

You plan to use Azure Disk Encryption for several virtual machine disks.

You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault11641655 Azure key vault.

To complete this task, sign in to the Azure portal and modify the Azure resources.

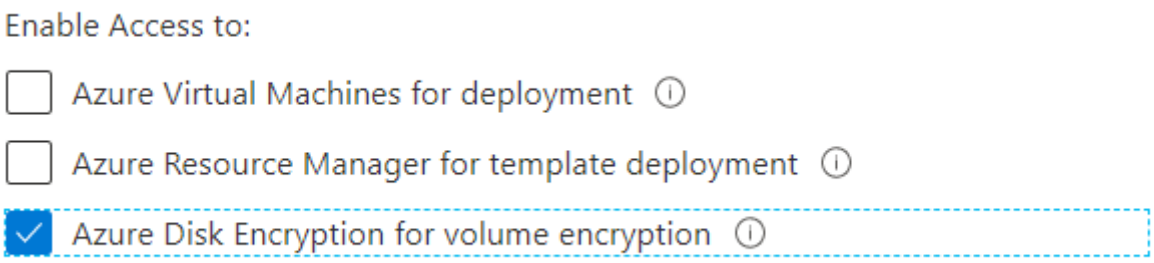
Correct Answer: *See the explanation below.*

1. In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key

Vaults in the left navigation pane.

2. In the Key Vault properties, scroll down to the Settings section and select Access Policies.

3. Select the Azure Disk Encryption for volume encryption



4. Click Save to save the changes.

https://t.me/learningnets

Question #11 *Topic 4*

HOTSPOT -

You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1.

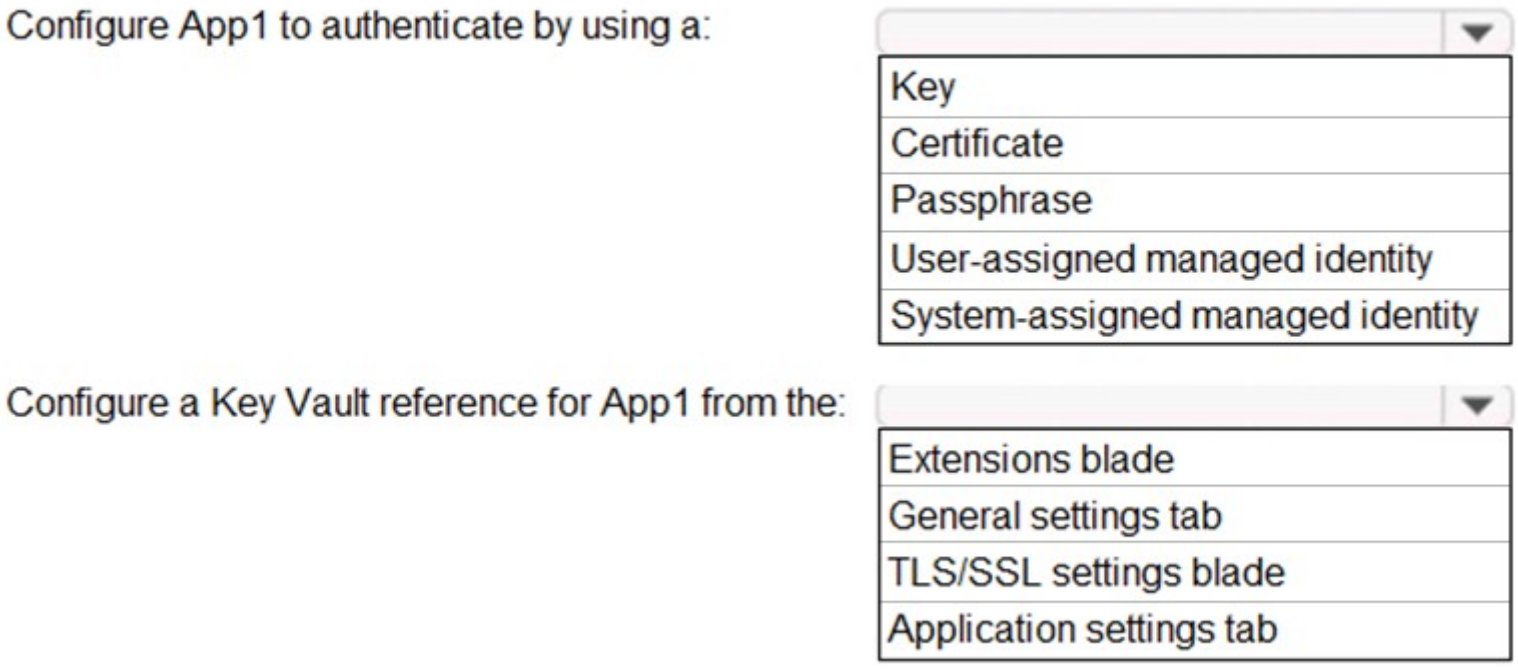
You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

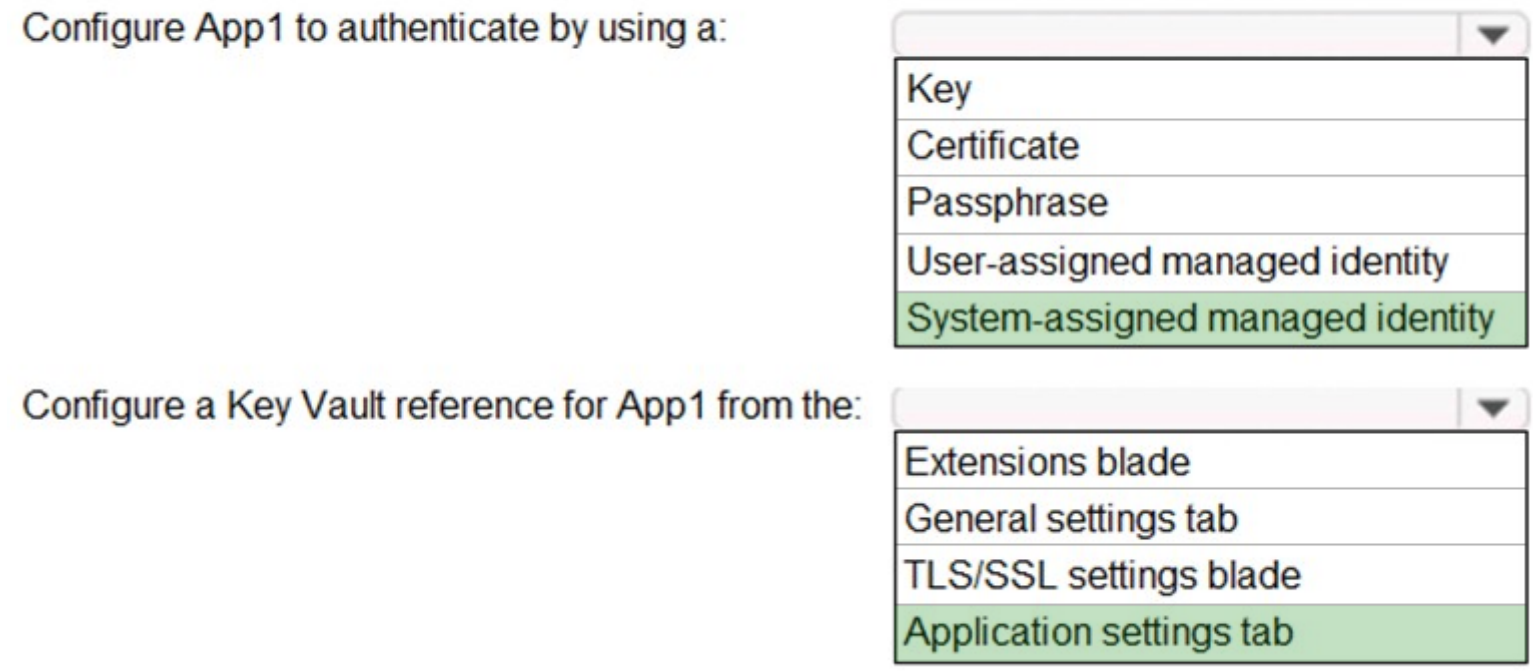
Hot Area:

Answer Area



Correct Answer:

Answer Area



Reference:

https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

kumax 3 weeks, 3 days ago

On exam, May 2021.

upvoted 4 times

ZakS 1 month, 3 weeks ago

Ans provided are correct.

Box 1 - System assigned managed identity
https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

Box 2 - Application settings
https://docs.microsoft.com/en-us/azure/key-vault/general/tutorial-net-create-vault-azure-web-app#configure-the-web-app-to-connect-to-key-

https://t.me/learningnets

vault

The link shows the code version. I think the Application setting is to be used to configure the URI of the Key Vault to be accessed by the Application

upvoted 2 times

BalderkVeit 1 month, 3 weeks ago

correct, as per: https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references
box 1: Only System managed is supported and it's the best choice
box 2: references to KV for saving and reading secrets should be configured in application settings

upvoted 1 times

MarioMK 1 month, 3 weeks ago

box 1: system managed identity
box 2: app > settings > TLS/SSL settings > Private key certificates tab
tested in azure account

upvoted 1 times

BalderkVeit 1 month, 3 weeks ago

you're wrong. Question is not about SSL settings. It's about app being able to save and read secrets from KV. So it's Application settings, not TLS/SSL settings

upvoted 2 times

SSTan 2 months, 4 weeks ago

Key Vault references currently only support system-assigned managed identities. User-assigned identities cannot be used.

upvoted 2 times

JAGUDERO 3 months ago

Box 1, only system managed is enabled for this scenario

Box 2, in key vault settings, you create an access policies, there you create the policy to refer to the application.

upvoted 2 times

Fred64 3 months, 3 weeks ago

We need to create a identity and provide this identity an access policy in the KV to access keys.

box 1 is "system assigned managed identity" but I thing "user assign" should work

box2 is unclear. next step is not in web app blade, but KV's. We create a policy in the general setting table

upvoted 2 times

macco455 3 months, 2 weeks ago

As per this link:
https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references
System Assigned is correct

upvoted 1 times

Fred64 2 months, 3 weeks ago

yes and in fact none of the proposition in box2 work

upvoted 1 times

dadageer 4 months ago

Answers are correct:

https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

upvoted 4 times

sobby 4 months ago

wrong
Certificate and TLS blade

upvoted 2 times

kimalto452 3 weeks, 3 days ago

do you use tls to connect to kv ? good for you haha

upvoted 1 times

macco455 3 months, 2 weeks ago

wrong, system assigned

upvoted 1 times

https://t.me/learningnets

Question #12 *Topic 4*

HOTSPOT -

You have an Azure key vault named KeyVault1 that has soft delete disabled and contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault1, the following events occur in sequence:

- Item1 is deleted.
- An administrator enables soft delete.
- Item2 and Policy1 are deleted.

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 recover Policy1.	○	○
You can add a new key named Item1.	○	○
You can add a new secret named Item2.	○	○

Answer Area

Statements	Yes	No
You can recover Policy1.	○	○
You can add a new key named Item1.	○	○
You can add a new secret named Item2.	○	○

Correct Answer:

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

Lyonel 5 days, 13 hours ago

As specified in this link provided in the answer (https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview)...

A key vault with the same name cannot be created in the same location; correspondingly, a key vault object cannot be created in a given vault if that key vault contains an object with the same name and which is in a deleted state.

Therefore, I believe the correct answers should be -> Yes, No, No

upvoted 1 times

Lyonel 5 days, 13 hours ago

CORRECTION: Should be -> No, Yes, No

upvoted 2 times

Lyonel 5 days, 12 hours ago

CORRECTION to my CORRECTION (sorry about that..) Should be...
YES = Policy1 CAN BE recovered
YES = Item1 was deleted PRIOR to Soft-Delete being enabled; no longer exists and Name CAN BE used
NO = Item2 Name can NOT be used as it was deleted AFTER Soft-Delete was enable; Name still exists as 'deleted'

https://t.me/learningnets

upvoted 1 times

thienvupt 1 week, 5 days ago

Yes-Yes-No
Soft-deleted resources are retained for a set period of time, 90 days.

upvoted 2 times

Rume 1 week, 6 days ago

https://www.examtopics.com/discussions/microsoft/view/46955-exam-az-500-topic-4-question-10-discussion/

Answer: N Y N

upvoted 1 times

Joillane 2 weeks ago

Should be Yes No Yes

upvoted 1 times

Joillane 2 weeks ago

And I meant No Yes No ;-)

upvoted 1 times

Question #13 *Topic 4*

You have an Azure SQL Database server named SQL1.
For SQL1, you turn on Azure Defender for SQL to detect all threat detection types.
Which action will Azure Defender for SQL detect as a threat?

A. A user updates more than 50 percent of the records in a table.

B. A user attempts to sign in as SELECT * FROM table1.

C. A user is added to the db_owner database role.

D. A user deletes more than 100 records from the same table.

Correct Answer: *B*
Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql

https://t.me/learningnets

Question #14 *Topic 4*

HOTSPOT -

You have the Azure Information Protection labels as shown in the following table.

Name	Use condition	Label is applied	Pattern	Case sensitivity
Label1	Condition1	Automatically	White	On
Label2	Condition2	Automatically	Black	Off

You have the Azure Information Protection policies as shown in the following table.

Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

You need to identify how Azure Information Protection will label files.

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

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

- No label
- Label1 only
- Label2 only
- Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

- No label
- Label1 only
- Label2 only
- Label1 and Label2

Correct Answer:

Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

- No label
- Label1 only
- **Label2 only**
- Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

- **No label**
- Label1 only
- Label2 only
- Label1 and Label2

Box 1: Label 2 only -

How multiple conditions are evaluated when they apply to more than one label

1. The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).

https://t.me/learningnets

2. The most sensitive label is applied.
3. The last sublabel is applied.

Box 2: No Label -
Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent.
Automatic classification does not apply to Microsoft Notepad.
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

smruk12 Highly Voted 1 year, 2 months ago
Correct answers are given.

"The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive)"

and

"The most sensitive label is applied."

So in this case label 2 is positioned last and is therefore the most sensitive.

(https://docs.microsoft.com/nl-nl/azure/information-protection/configure-policy-classification)
upvoted 24 times

Thi 5 months, 2 weeks ago
Agree box1: label2, box2: no label
upvoted 2 times

kiketxu 9 months, 3 weeks ago
thank you for the detailed explanation.
upvoted 1 times

skb1996 1 year, 1 month ago
Black and white, last label is label1
upvoted 3 times

rgullini 2 months, 1 week ago
No, because of Case sensitivity settings
upvoted 1 times

Maximillian Highly Voted 1 year, 1 month ago
They are not talking about the position of Black and White but the position of the labels in the first table given. Since the first table has the label2 on the bottom, it will have the higher priority than that label1 according to the Microsoft documentation.
upvoted 16 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Label priority (order matters)

When you create your sensitivity labels in your admin center, they appear in a list on the Sensitivity tab on the Labels page. In this list, the order of the labels is important because it reflects their priority. You want your most restrictive sensitivity label, such as Highly Confidential, to appear at the bottom of the list, and your least restrictive sensitivity label, such as Public, to appear at the top.
You can apply just one sensitivity label to an item such as a document, email, or container. If you set an option that requires your users to provide a justification for changing a label to a lower classification, the order of this list identifies the lower classifications. However, this option does not apply to sublabels.
The ordering of sublabels is used with automatic labeling, though. When you configure labels to be applied automatically or as a recommendation, multiple matches can result for more than one label. To determine the label to apply or recommend, the label ordering is used: The last sensitive label is selected, and then if applicable, the last sublabel.
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
https://docs.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-file-types

.txt is not supported
upvoted 2 times

macco455 3 months, 2 weeks ago
Label 2
No Label
Scoped policies, just like labels, are ordered in the Azure portal. If a user is configured for multiple scopes, an effective policy is computed for that user before it is downloaded. According to the order of the policies, the last policy setting is applied. The labels that the user sees are from the global policy and any additional labels from scoped policies that the user belongs to.
upvoted 1 times

https://t.me/learningnets

HCL 5 months, 1 week ago

Box1: Label 1 and Label 2
Box2: No Label

Explanation:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-scope#how-scoped-policies-work
"The labels that the user sees are from the global policy and any additional labels from scoped policies that the user belongs to."
The labels are in two different policies. So all policies were applied in order. Thus, Label 1 and Label 2 were both applied.

From AIP blade in Azure Portal: "Policies can be scoped to specific users and groups. Users belonging to multiple scopes will get all labels applied to them in the policy order configured here."

upvoted 2 times

lateralus 6 months ago

Answer seems correct.
Q1. "Label 2 only" is correct as only Policy 2 is applied with Label 2. See here: https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-scope#how-scoped-policies-work
Scoped policies, just like labels, are ordered in the Azure portal. If a user is configured for multiple scopes, an effective policy is computed for that user before it is downloaded. According to the order of the policies, the last policy setting is applied.

Q2. "No Label" is correct - As we are talking about classification, Notepad .txt formats is not supported. Refer to https://docs.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-file-types#file-types-supported-for-classification-only
The format .txt would be supported in a scenario where classification and protection is required.

upvoted 7 times

sureshatt 3 months, 2 weeks ago

This is the best explanation with enough evidence. The solution here depends on the order of the policies not by the order of labels because each policy has only one label.

upvoted 1 times

Kal20 6 months, 2 weeks ago

Box 1: Label 1 only
Box 2: No label

upvoted 1 times

Danish12 7 months ago

The answer is correct, well explained here https://docs.microsoft.com/nl-nl/azure/information-protection/configure-policy-classification

upvoted 1 times

hitandrun 8 months, 1 week ago

I feel the second answer is "not labled" - for the reason that the text is written in a notepad, but not in a word document or email. Azure Identity Protection doesn't apply to notepad.

upvoted 4 times

kiketxu 7 months, 3 weeks ago

Just a comment.....autolabeling not applies to any apart from Word, Excel, Powerpoint. But you can label with the AIP UL client from the Explorer txt, pdf, jpf, and more types of files.

upvoted 2 times

kiketxu 7 months, 3 weeks ago

Btw, both answers are correct.

upvoted 3 times

Andy998 1 year ago

Given answers are correct

upvoted 6 times

jakobaszek 1 year, 1 month ago

Word „black” is Label 2 = policy2
no label for option 2

upvoted 1 times

Prash85 1 year, 2 months ago

agree it must be label 1 for the first one

upvoted 1 times

jam3sb0nd 1 year, 2 months ago

I think the answer for the first question is Label 1 only. In "Black and White", the label for White is assigned as it is the most sensitive label. The label for White is Label1.

upvoted 3 times

DavidSapery 1 year, 1 month ago

The label conditions are evaluated from the bottom up. So since the Label 2 condition passes, that will be the label applied. Not Label1.

upvoted 3 times

ExamUser 1 year, 2 months ago

Correct answers...

https://t.me/learningnets

upvoted 13 times

Question #15 *Topic 4*

Your company uses Azure DevOps.
You need to recommend a method to validate whether the code meets the companyג€™s quality standards and code review standards.
What should you recommend implementing in Azure DevOps?

A. branch folders

B. branch permissions

C. branch policies

D. branch locking

Correct Answer: *C*
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

Andy998 Highly Voted 1 year ago
C is correct.
upvoted 17 times

Kumar1983 Most Recent 2 months, 2 weeks ago
C is right
upvoted 2 times

zic04 5 months, 3 weeks ago
C is ok
upvoted 2 times

ksinger 9 months, 2 weeks ago
C is OK
upvoted 4 times

kiketxu 9 months, 3 weeks ago
It's Ok.
upvoted 4 times

https://t.me/learningnets

Question #16 *Topic 4*

SIMULATION -

You need to ensure that User2-11641655 has all the key permissions for KeyVault11641655.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Correct Answer: *See the explanation below.*

You need to assign the user the Key Vault Secrets Officer role.

1. In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key
Vaults in the left navigation pane.
2. In the key vault properties, select Access control (IAM).
3. In the Add a role assignment section, click the Add button.
4. In the Role box, select the Key Vault Secrets Officer role from the drop-down list.
5. In the Select box, start typing User2-11641655 and select User2-11641655 from the search results.
6. Click the Save button to save the changes.

Stuudent Highly Voted 6 months, 3 weeks ago

I am happy to inform that everyone in this discussion missed the point. The task is to give a specific user all key privileges for a specific key vault.

In the key vault, you go to Access policies, click Add policy and then you can select specific Key, Secret and Certification permissions. So you select all the key privileges, then select the user and voila.

Tested in Azure live environment.

upvoted 17 times

inf 5 months, 3 weeks ago

Technically correct, or simpler use the built-in 'template' - "Key Management" - which selects the 9 x key permissions for you within the wizard.

upvoted 2 times

Toyeeb 6 months, 2 weeks ago

exactly

upvoted 1 times

Zjorzke Highly Voted 12 months ago

Nope, access policy with all key permissions.

upvoted 13 times

Lexa 10 months, 3 weeks ago

I`m agree, this way is more clear than templates.

upvoted 1 times

cryodax Most Recent 1 month, 3 weeks ago

The question is ambiguous as it does not state whether the key vault permission model is set to vault access policy or azure role-based access control. If set to vault access policy, then use a policy. If set to role-based, then use IAM to assign the secrets officer role. Based on the answer given, they're assuming it's set to role-based.

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

Key Vault
Settings > Access Policy
+Add policy
select template for key permissions only
click all key permission to select all (16)
Select principal (user)
add

DO NOT FORGET TO SAVE ACCESS POLICY

upvoted 1 times

JAGUDERO 3 months ago

support with documentation

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 1 times

JAGUDERO 3 months ago

Giving permissions in RBAC as "Key Vault Crypto Officer" ensures that all "Key" permissions are given in the Key Vault

https://t.me/learningnets

upvoted 1 times

Gjferweb 7 months ago

for all the key permissions documentation says its the crypto officer not the secret officer:
Key Management Keys: all operations Key Vault Crypto Officer (preview)
Secret Management Secrets: all operations Key Vault Secrets Officer (preview)

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

upvoted 1 times

paradoxx 10 months, 1 week ago

On Azure simulation questions Does it need to open Azure portal with your own account or there is a link to open a Microsoft simulation lab?

upvoted 1 times

levo017 9 months, 4 weeks ago

The exam provider is hosting a Azure Stack, and exam provider stuff will help you login to the Azure Stack. So it's like a simulation lab.

upvoted 1 times

levo017 9 months, 4 weeks ago

staff *

upvoted 1 times

MrMozz 10 months, 2 weeks ago

Key Vault Administrator and Key Vault Certificates Officer are in preview, hence won't apply to the current exam.
so the answer is wrong Key Vault Contributor is the right Role at this time.

upvoted 1 times

planb7000 11 months, 2 weeks ago

Key Vault Administrator has more permissions than KV Secrets Officer .

This is getting a little bit confusing

upvoted 1 times

pmr123 1 year ago

How can Key Vault Secrets Officer mange the permissions?? I think it should be Key vault contributor

upvoted 2 times

planb7000 11 months, 2 weeks ago

The KV Contributor lets you manage key vaults, but not access to them.

upvoted 1 times

https://t.me/learningnets

Question #17 *Topic 4*

You have an Azure web app named WebApp1.
You upload a certificate to WebApp1.
You need to make the certificate accessible to the app code of WebApp1.
What should you do?

A. Add a user-assigned managed identity to WebApp1.

B. Add an app setting to the WebApp1 configuration.

C. Enable system-assigned managed identity for WebApp1.

D. Configure the TLS/SSL binding for WebApp1.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code

mrwhite Highly Voted 1 year ago
Looks to me that B is the anwer?

To access a certificate in your app code, add its thumbprint to the WEBSITE_LOAD_CERTIFICATES app setting, by running the following command in the Cloud Shell:

Azure CLI

Copy

Try It
az webapp config appsettings set --name <app-name> --resource-group <resource-group-name> --settings WEBSITE_LOAD_CERTIFICATES=<comma-separated-certificate-thumbprints>
upvoted 22 times

Thi 5 months, 1 week ago
exactly thanks mrwhite
upvoted 2 times

deegadaze1 Highly Voted 4 months, 2 weeks ago
In Exam & no Simulation
upvoted 7 times

Sash82 1 month, 1 week ago
did you take exam and how many question simulation in the exam
upvoted 1 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago
Prepare your web app
To create custom TLS/SSL bindings or enable client certificates for your App Service app, your App Service plan must be in the Basic, Standard, Premium, or Isolated tier. In this step, you make sure that your web app is in the supported pricing tier.
upvoted 2 times

HardcodedCloud 4 months, 1 week ago
Given answer B is correct.
upvoted 2 times

milind8451 4 months, 3 weeks ago
Right Ans.
upvoted 1 times

finolweb 5 months ago
Make the certificate accessible
To access a certificate in your app code, add its thumbprint to the WEBSITE_LOAD_CERTIFICATES app setting, by running the following command in the Cloud Shell:

az webapp config appsettings set --name <app-name> --resource-group <resource-group-name> --settings WEBSITE_LOAD_CERTIFICATES=<comma-separated-certificate-thumbprints>

To make all your certificates accessible, set the value to *.
upvoted 2 times

mayenite 5 months ago

https://t.me/learningnets

In exam
upvoted 3 times

deegadaze1 5 months ago
Thanks,
Did you see any Simulation in Exam?
upvoted 3 times

deegadaze1 4 months, 2 weeks ago
In Exam & no Simulation
upvoted 2 times

kimalto452 3 weeks, 3 days ago
Are you bot ?
upvoted 2 times

mayenite 5 months, 2 weeks ago
Answer given is correct
To access a certificate in your app code, add its thumbprint to the WEBSITE_LOAD_CERTIFICATES app setting...
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code
upvoted 3 times

fdera 6 months, 4 weeks ago
D
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjSqqjJ89ftAhXEWhUIHXizAK0QFjAAegQIAhAC&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fapp-service%2Fconfigure-ssl-certificate-in-code&usg=AOvVaw3-EeTc8r7FxgKTpfdqxeii
upvoted 1 times

ipindado2020 9 months, 1 week ago
B is correct WEBSITE_LOAD_CERTIFICATES
upvoted 1 times

Spamuel 11 months, 3 weeks ago
Agree - definitely B
upvoted 4 times

qruekhvblzfbrztbnz 11 months, 3 weeks ago
Seems to me B is correct answer.
upvoted 4 times

gboyega 1 year ago
The correct answer is D

https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code
upvoted 4 times

jimmyjose 9 months, 2 weeks ago
The link you provided is correct, but the answer is 'B'.

Under section "Make the certificate accessible", the Azure CLI command is as follows.
az webapp config appsettings set --name <app-name> --resource-group <resource-group-name> --settings WEBSITE_LOAD_CERTIFICATES=<comma-separated-certificate-thumbprints>

The command makes the certificate available to the app code by adding the thumbprint of the certificate. The app setting is WEBSITE_LOAD_CERTIFICATES, and it is configured
in the command using the parameter 'appsettings'.

Hence, the answer is 'B'.
upvoted 10 times

planb7000 11 months, 2 weeks ago
I understand why you say this but if you look carefully...this binding is for custom domains specifically. B is the correct answer from my research.
upvoted 1 times

https://t.me/learningnets

Question #18 *Topic 4*

HOTSPOT -

You have the Azure key vaults shown in the following table.

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can restore the Secret1 backup to: ▼
- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to: ▼
- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

Answer Area

You can restore the Secret1 backup to: ▼
- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

Correct Answer:

You can restore the Key1 backup to: ▼
- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

Sethoo Highly Voted 3 months, 4 weeks ago

I will go with the given answers -"When you back up a key vault object, such as a secret, key, or certificate, the backup operation will download the object as an encrypted blob. This blob can't be decrypted outside of Azure. To get usable data from this blob, you must restore the blob into

https://t.me/learningnets

a key vault within the same Azure subscription and Azure geography
https://docs.microsoft.com/en-us/azure/key-vault/general/backup

upvoted 14 times

JohnRe 2 months ago

Yep, same Azure subscription and Azure geography including the paired region.

upvoted 1 times

rgullini Most Recent 2 months, 3 weeks ago

Answers are correct.
When you back up a key vault object, such as a secret, key, or certificate, the backup operation will download the object as an encrypted blob. This blob can't be decrypted outside of Azure. To get usable data from this blob, you must restore the blob into a key vault within the same Azure subscription and Azure geography.

upvoted 1 times

JCWF 3 months, 4 weeks ago

Why the answer include KV3? KV1 and KV2 are in West US but KV3 is in East US.

upvoted 1 times

rgullini 2 months, 1 week ago

United states is a geography itself

upvoted 1 times

JCWF 3 months, 4 weeks ago

Missed out this - You can restore to a different region in the same geography.

upvoted 7 times

rgullini 2 months, 3 weeks ago

Totally correct as per: https://docs.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli

upvoted 1 times

https://t.me/learningnets

Question #19 *Topic 4*

HOTSPOT -

You have an Azure subscription that contains an Azure key vault named Vault1.

On January 1, 2019, Vault1 stores the following secrets.

```
Enabled     : False
Expires     :
NotBefore   : 5/1/19 12:00:00 AM
Created     : 12/20/18 2:55:00 PM
Updated     : 12/20/18 2:55:00 PM
ContentType :
Tags        :
TagsTable   :
VaultName   : vault1
Name        : Password1
Version     :
Id          : https://vault1.vault.azure.net:443/secrets/Password1

Enabled     : True
Expires     : 5/1/19 12:00:00 AM
NotBefore   : 3/1/19 12:00:00 AM
Created     : 12/20/18 3:00:00 PM
Updated     : 12/20/18 3:00:00 PM
ContentType :
Tags        :
TagsTable   :
VaultName   : vault1
Name        : Password2
Version     :
Id          : https://vault1.vault.azure.net:443/secrets/Password2
```

When can each secret be used by an application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Password1:

- Never
- Always
- Only after May 1, 2019

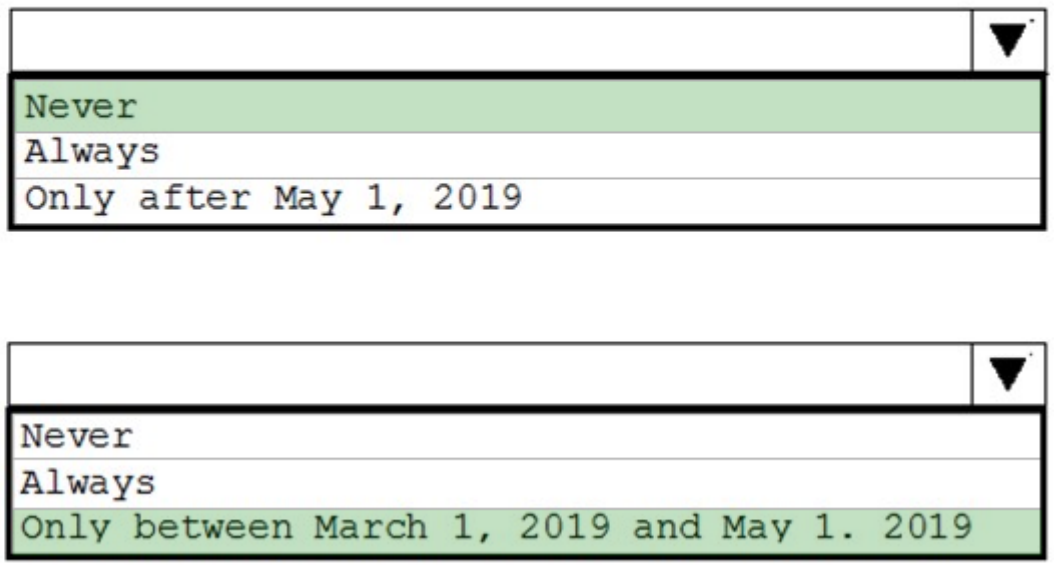
Password2:

- Never
- Always
- Only between March 1, 2019 and May 1. 2019

https://t.me/learningnets

Answer Area

Correct Answer:



Box 1: Never -

Password1 is disabled.

Box 2: Only between March 1, 2019 and May 1,

Password2:

```
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
```

Reference:

https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

badaboom Highly Voted 3 months, 3 weeks ago

Correct answer !

upvoted 7 times

am20 1 month, 4 weeks ago

Correct Answer as "... The enabled attribute is used in conjunction with nbf and exp when an operation occurs between nbf and exp, it will only be permitted if enabled is set to true. Operations outside the nbf and exp window are automatically disallowed, except in particular situations." https://docs.microsoft.com/en-us/azure/key-vault/secrets/about-secrets#secret-attributes

upvoted 2 times

OhBee 3 months ago

I don't think so. The expired and Not Before fields are for informational purposes only for secrets as per the following reference: https://docs.microsoft.com/en-us/azure/key-vault/secrets/about-secrets#secret-attributes.

The first answer is correct, but the second one should be Always.

upvoted 10 times

Fred64 2 months, 1 week ago

so, the answer is always/always

upvoted 1 times

rgullini 2 months, 3 weeks ago

Turns out it´s confusing. Because the provided link in the answer talks about the attributes of a secret but says nothing they are informational only

upvoted 1 times

nicksu 1 month, 3 weeks ago

https://docs.microsoft.com/en-us/azure/key-vault/secrets/about-secrets#date-time-controlled-operations

Date-time controlled operations
A secret's get operation will work for not-yet-valid and expired secrets, outside the nbf / exp window. Calling a secret's get operation, for a not-yet-valid secret, can be used for test purposes. Retrieving (getting) an expired secret, can be used for recovery operations.

upvoted 1 times

nicksu 1 month, 3 weeks ago

I'd say the answer is Never/Always, but it depends on what they mean by "application can use". Reading secret will work irrespectively of expiration, but secret management won't work outside nbf-exp

upvoted 2 times

Fred64 2 months, 3 weeks ago

I tested, that's true

upvoted 1 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

https://t.me/learningnets

upvoted 3 times

ChinkSantana 1 week, 6 days ago
Did you get any simulations ?
upvoted 1 times

kumax 3 weeks, 3 days ago
On exam, May 2021.
upvoted 2 times

Question #20 *Topic 4*

You have an Azure web app named webapp1.
You need to configure continuous deployment for webapp1 by using an Azure Repo.
What should you create first?

A. an Azure Application Insights service
B. an Azure DevOps organization
C. an Azure Storage account
D. an Azure DevTest Labs lab

Correct Answer: *B*
To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment

barchetta Highly Voted 1 year, 5 months ago
This is not security. Perhaps not on the exam. This site is free, im not gonna complain unless its on the test and then the complaint will be to MS not examtopics. Im going to contrbute to ET because I see they are having performance issues.. Im sure they can use some cash.
upvoted 17 times

Shaw90 Highly Voted 9 months ago
This was actually in the Exam Azure-500, I am surprised too.
upvoted 13 times

sureshatt Most Recent 4 months, 2 weeks ago
This question is silly, the question says there is already an Azure Repo. If you have an Azure Repo, you have an organisation already.
upvoted 1 times

bluetaurianbull 6 months, 2 weeks ago
if such questions are not their how can MS guarantee that no one ever scored 100% in the exam :) LOL
upvoted 2 times

Basit_Khan 10 months ago
This is related to AZ-400 Exam Topic
upvoted 1 times

kristiann21 1 year, 1 month ago
correct answer
upvoted 2 times

anonek 1 year, 2 months ago
Correct answer is B
upvoted 9 times

D0yle 1 year, 5 months ago
I am wondering why this question is here - it is not in AZ-500 scope?
upvoted 6 times

https://t.me/learningnets

Question #21 *Topic 4*

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
The company develops an application named App1. App1 is registered in Azure AD.
You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.
What should you configure?

A. an application permission without admin consent

B. a delegated permission without admin consent

C. a delegated permission that requires admin consent

D. an application permission that requires admin consent

Correct Answer: *B*
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.
Incorrect Answers:
A, D: Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

AS007 Highly Voted 1 year, 2 months ago
Answer is correct - have validated
upvoted 26 times

juselasmc Highly Voted 10 months, 1 week ago
in the exam
upvoted 10 times

g2d2 Most Recent 4 months, 2 weeks ago
In order to achieve what is being asked, you need to assign API permission to the registered App. The API permission is Azure Key Vault user_impersonation and that is of type 'Delegated' and Admin Consent Required 'No'
Hence B is correct.
upvoted 2 times

sureshatt 4 months, 3 weeks ago
Provided answer is correct. The term "on behalf of" always means "delegation" in OAuth2. Therefore it has to be the permission of the logged in user. However, since this is just a read of a keyvault (not high privileged), the app does not need the admin privilege.
upvoted 4 times

milind8451 4 months, 3 weeks ago
"On-Behalf of" says that answer should be B. No admin consent needed.

Let me explain Delegated permission with an Example, assume your app has been granted the User.ReadWrite.All delegated permission. This permission nominally grants your app permission to read and update the profile of every user in an organization. If the signed-in user is a global administrator, your app can update the profile of every user in the organization. However, if the signed-in user doesn't have an administrator role, your app can update only the profile of the signed-in user. It can't update the profiles of other users in the organization because the user that it has permission to act on behalf of doesn't have those privileges. This is "On-Behalf of" permission which ques mentioned.
upvoted 2 times

abd500 5 months, 1 week ago
NO
YES NO
upvoted 1 times

karia3 5 months ago
NO NO NOOOO
upvoted 2 times

Thi 5 months, 2 weeks ago
Answer:B. a delegated permission without admin consent
Between Application and Deleted permissions, you have to choose Delegated permissions, becausethis can be done on behalf of the user.
upvoted 1 times

PM2 6 months, 3 weeks ago
in the exam

https://t.me/learningnets

upvoted 4 times

Danish12 7 months ago
Answer is correct!
upvoted 1 times

kdkdk 7 months ago
in the exams
upvoted 5 times

am20 7 months, 3 weeks ago
I think the answer is D based on this https://www.youtube.com/watch?v=6R3W9T01gdE
upvoted 1 times

am20 7 months, 3 weeks ago
correction. agree with jinxie. Answer B is correct. you can also watch this https://www.youtube.com/watch?v=YWvl0cIilyA
upvoted 1 times

macphy 8 months ago
Barchetta's comment is correct. "on behalf of the application users.", this means, you need an application permission (A or D).
At this time, application permission requires the concent, so the answer is D.
upvoted 2 times

jinxie 7 months, 3 weeks ago
you do not need to grant admin permissions for delegated keyvault access so the given answer is correct. to replicate, create a webapp, go to authetnicaton/authorization. enable appservice Authentication and generate a new appregistration. Go to AAD, to go appregistrations, API permissions and add the keyvault permission for delegated users. you will notice that the admin permission is marked with "-" meaning it is not required.
upvoted 1 times

barchetta 1 year, 5 months ago
Wait, I think I get it "on behalf of the application users." that is the critical statement.
upvoted 5 times

barchetta 1 year, 5 months ago
Im not sure there is enough data in the question to answer.
upvoted 1 times

RupaliS 1 year, 6 months ago
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, and the app is delegated permission to act as the signed-in user when making calls to the target resource. Some delegated permissions can be consented to by non-administrative users, but some higher-privileged permissions require administrator consent.
upvoted 7 times

RupaliS 1 year, 6 months ago
Ans C also seems to be right ?
"Adding a delegated permission to an application does not automatically grant consent to the users within the tenant. Users must still manually consent for the added delegated permissions at runtime, unless the administrator grants consent on behalf of all users."
upvoted 3 times

D0yle 1 year, 5 months ago
B is correct answer.- Some higher-privileged permissions require administrator consent - here we need just access to key vault.
upvoted 5 times

https://t.me/learningnets

Question #22 *Topic 4*

DRAG DROP -

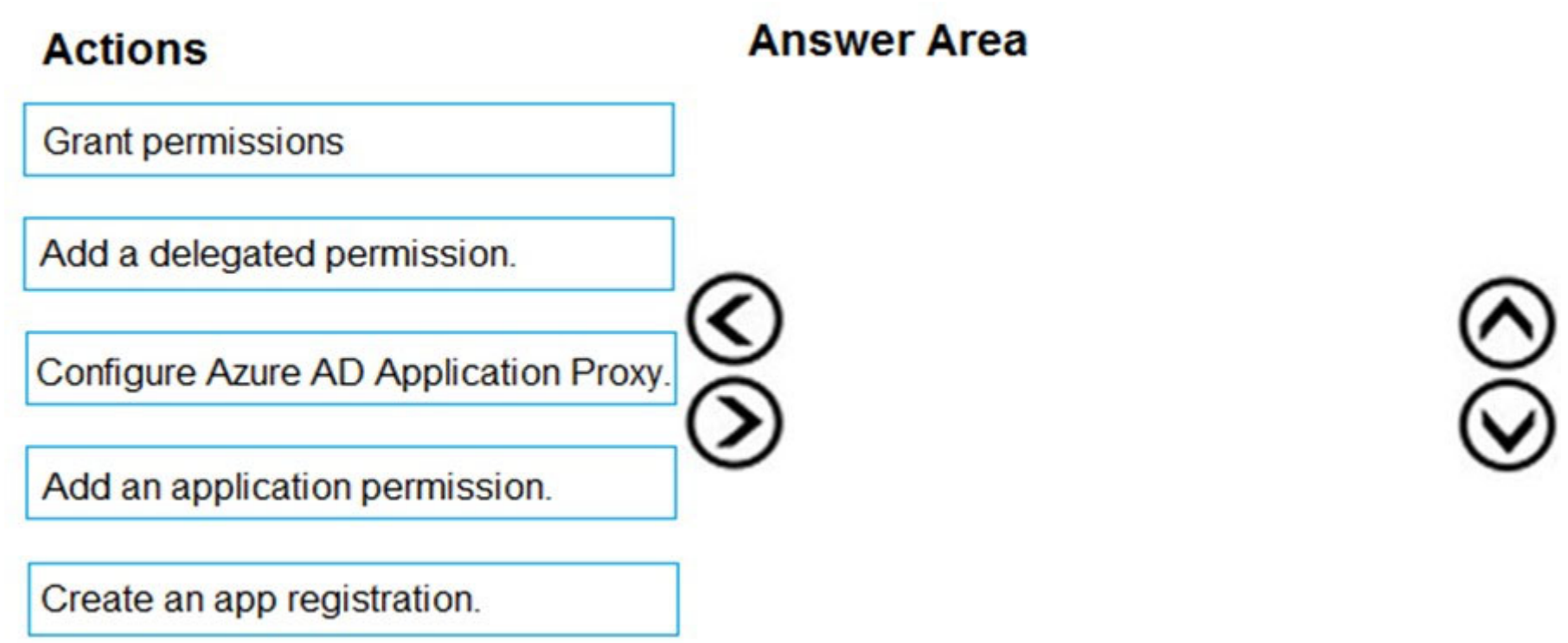
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

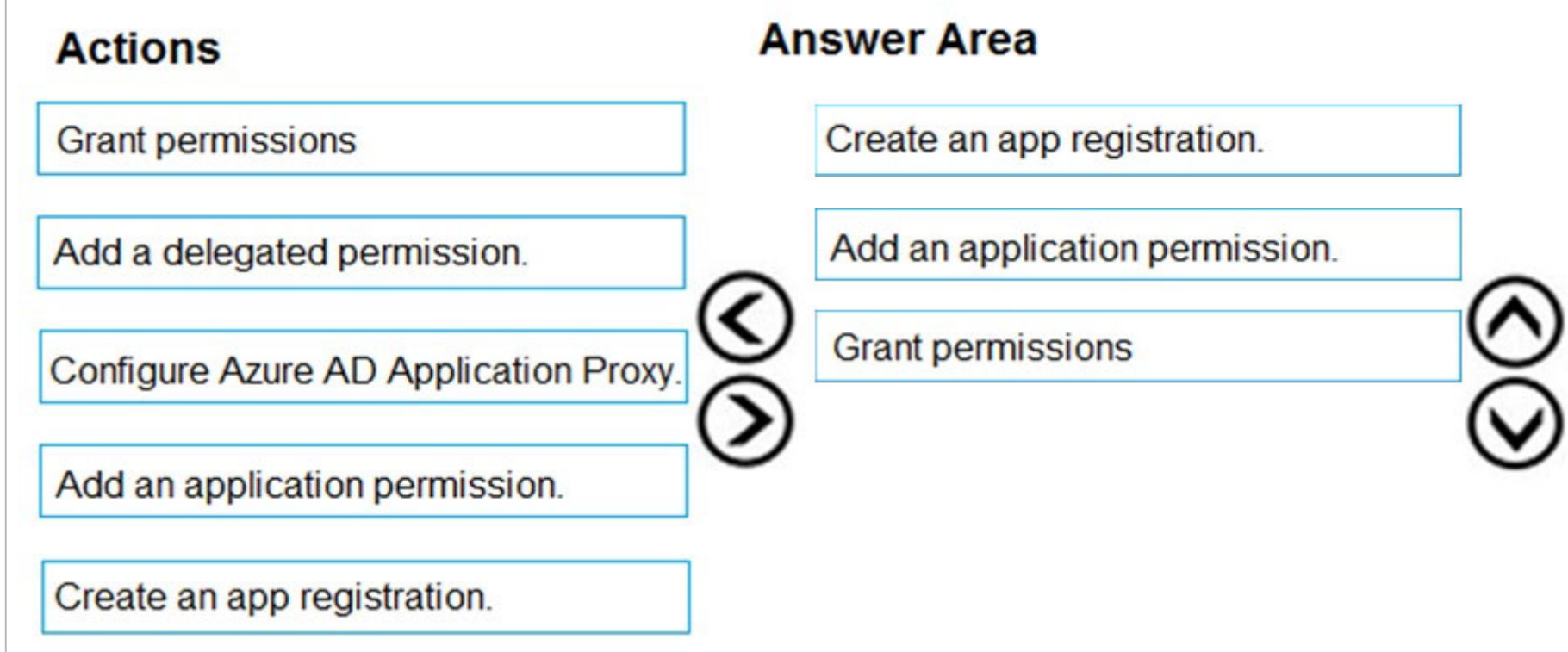
You need to delegate the minimum required permissions to App1.

Which three actions should you perform in sequence from the Azure portal? 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:



Correct Answer:



Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present.

Step 3: Grant permissions -

Incorrect Answers:

Delegated permission -

Delegated permissions are used by apps that have a signed-in user present.

Application Proxy:

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent

https://t.me/learningnets

gfhbox0083 Highly Voted 1 year ago

Correct Answers
Application permissions allow an application in Azure Active Directory to act as it's own entity, rather than on behalf of a specific user. Delegated permissions allow an application in Azure Active Directory to perform actions on behalf of a particular user

upvoted 19 times

Loga 7 months, 3 weeks ago

Agreed, for sure.

upvoted 1 times

AS007 Highly Voted 1 year, 2 months ago

Correct Answers

upvoted 10 times

peacegrace Most Recent 2 months, 2 weeks ago

When the question says "You need to delegate the minimum required permissions to App". So delegate would be the minimum permisssion right ? Application is too much. We alwasy use delegate and never application in my projects.

upvoted 2 times

DCarma 2 weeks, 2 days ago

Disagree, personally. If you use application permissions then you are just granting the application access to Microsoft Graph which is as about as minimal as you can ask for. It doesn't say anything about users using this application themselves and having the need for the app querying Microsoft Graph to do so on behalf of a user or anything.

Provided answer is correct.

upvoted 1 times

sensa 4 months, 2 weeks ago

in exam

upvoted 5 times

mayenite 5 months ago

In exam

upvoted 4 times

Adamantium 9 months, 3 weeks ago

Specific supporting documentation
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

upvoted 1 times

Andy998 1 year ago

Correct. This is on the exam.

upvoted 5 times

kristiann21 1 year, 1 month ago

correct answer

upvoted 1 times

https://t.me/learningnets

Question #23 *Topic 4*

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.
The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.
You need to register App1 in Azure AD.
What information should you obtain from the developer to register the application?

A. a redirect URI

B. a reply URL

C. a key

D. an application ID

Correct 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

AS007 Highly Voted 1 year, 2 months ago
Correct Answer
upvoted 17 times

gfhbox0083 Highly Voted 1 year ago
A, for sure.
upvoted 10 times

kumax Most Recent 3 weeks, 3 days ago
On exam, May 2021.
upvoted 1 times

Fred64 2 months, 3 weeks ago
Does Azure make a difference between reply and redirect url? It is called redirect when creating and reply later
upvoted 1 times

PM2 4 months, 1 week ago
in the exam
upvoted 4 times

Thi 5 months, 2 weeks ago
Answer: A. A redirect URI
When using OAuth2 implicit grant type, the access tokens are sent to the client using the redirect URI.
upvoted 1 times

hstorm 10 months ago
Correction: Sorry my answer was to "request authorization code" but original question is "register app in AD"
Answer is correct
upvoted 2 times

hstorm 10 months ago
The provided link
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

100% States that the answer is wrong, and should be Application_id
upvoted 1 times

cloudycloud 9 months, 2 weeks ago
the application ID is provide by AAD
upvoted 1 times

kristiann21 1 year, 1 month ago
correct answer
upvoted 2 times

D_PaW 1 year, 1 month ago
Validated in Azure Portal. Correct Answer
upvoted 2 times

https://t.me/learningnets

gekvprasad 1 year, 2 months ago
Correct Answer
upvoted 3 times

Question #24 *Topic 4*

From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.
Which effect requires a managed identity for the assignment?

A. AuditIfNotExist

B. Append

C. DeployIfNotExist

D. Deny

Correct 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

AS007 Highly Voted 1 year, 2 months ago
Correct
upvoted 12 times

kdkdk Highly Voted 7 months ago
in the exams
upvoted 9 times

tuta 7 months ago
any more pointers ? seating exam next week skimming though for last minute hints
upvoted 2 times

deegadaze1 5 months, 3 weeks ago
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.
upvoted 1 times

Deepmindx Most Recent 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 1 times

kumax 3 weeks, 3 days ago
On exam, May 2021.
upvoted 1 times

PM2 4 months, 1 week ago
in the exam
upvoted 2 times

mayenite 5 months ago
In exam
upvoted 3 times

gfhbox0083 1 year ago
C, for sure.
upvoted 5 times

kristiann21 1 year, 1 month ago
correct answer
upvoted 4 times

https://t.me/learningnets

Question #25 *Topic 4*

HOTSPOT -

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to implement an application that will consist of the resources shown in the following table.

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.

You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.

Which task should you identify for each resource? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

CosmosDB1: [▼]
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

WebApp1: [▼]
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

Answer Area

Correct Answer:

CosmosDB1: [▼]
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens. ✓

WebApp1: [▼]
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens. ✓
- Create database users and generate resource tokens.

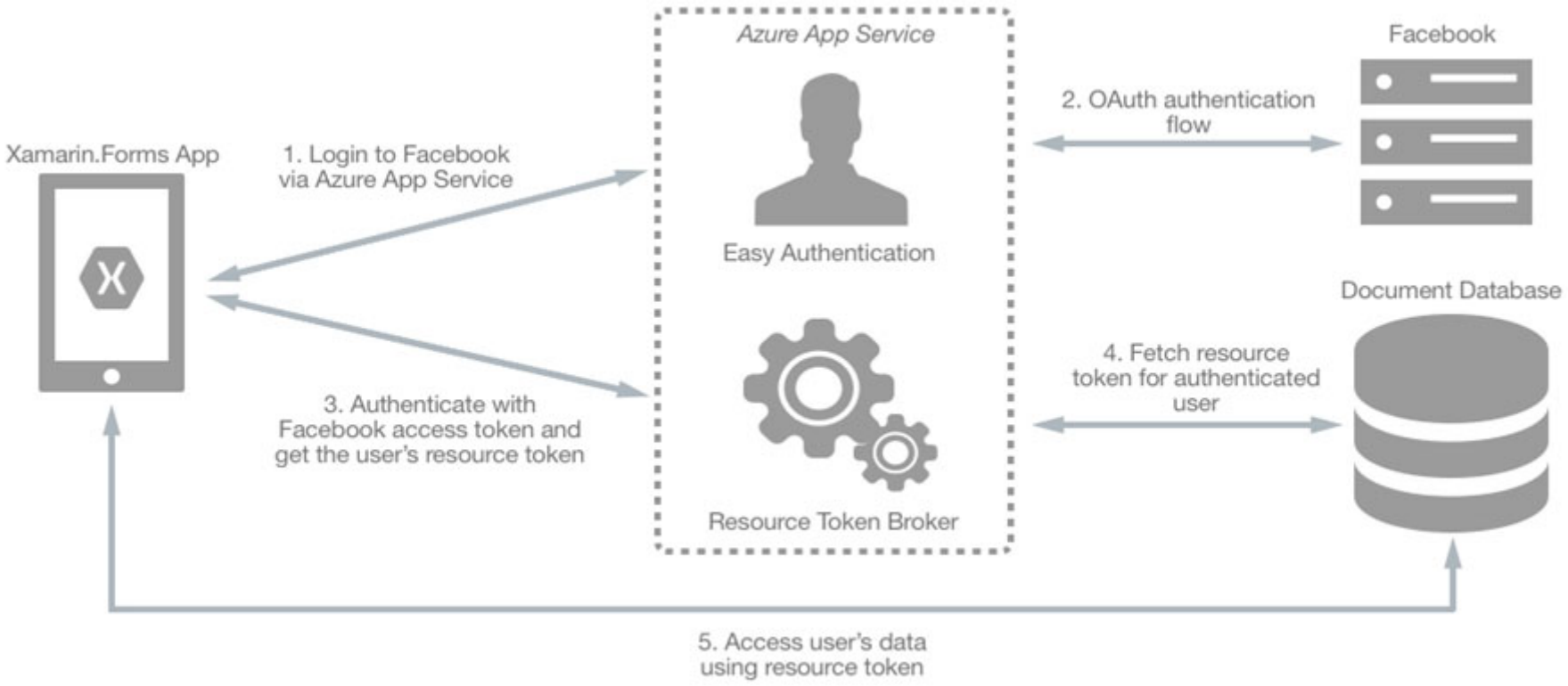
CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:

https://t.me/learningnets



Reference:

https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

AS007 Highly Voted 1 year, 2 months ago

Correct Answers

upvoted 12 times

gfhbox0083 Highly Voted 1 year ago

The provided is correct.

upvoted 6 times

PM2 Most Recent 4 months, 1 week ago

in the exam

upvoted 5 times

jbuenoo 10 months, 1 week ago

Answers seem to be correct: https://docs.microsoft.com/en-us/azure/cosmos-db/media/secure-access-to-data/resourcekeyworkflow.png

upvoted 4 times

Exam_Master_Me 12 months ago

Correct:
The mid-tier service is also responsible for authenticating the client (for example, by using Azure Active Directory). Once the client successfully authenticates, the mid-tier service requests a resource token associated with the authenticated user from the Cosmos DB account and relays the token back to the client. At that point, the client can use the token to access Cosmos DB resources directly.
https://mobilemonitoringsolutions.com/introduction-to-azure-cosmos-db-security/

upvoted 5 times

maj79 1 year ago

no mention of 'mobile application' in question

upvoted 1 times

P0d 1 year, 1 month ago

I am not sure that CosmosDB generates token. As it's acting as backend db for webapp I guess it's also relays on token.

upvoted 1 times

kristiann21 1 year, 1 month ago

same question in exam

upvoted 5 times

https://t.me/learningnets

Question #26 *Topic 4*

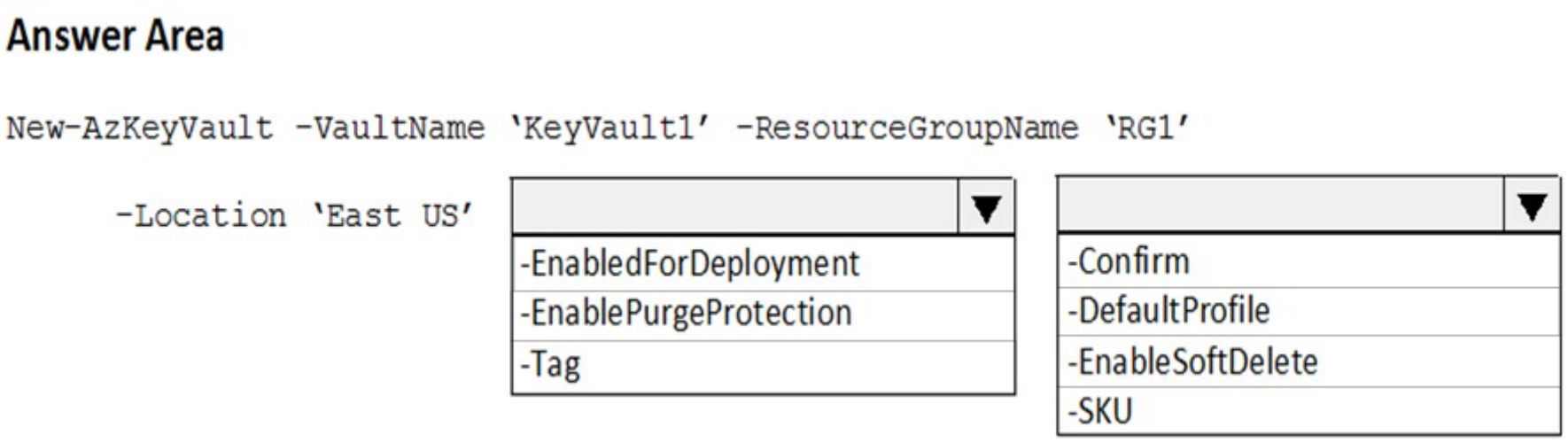
HOTSPOT -

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.

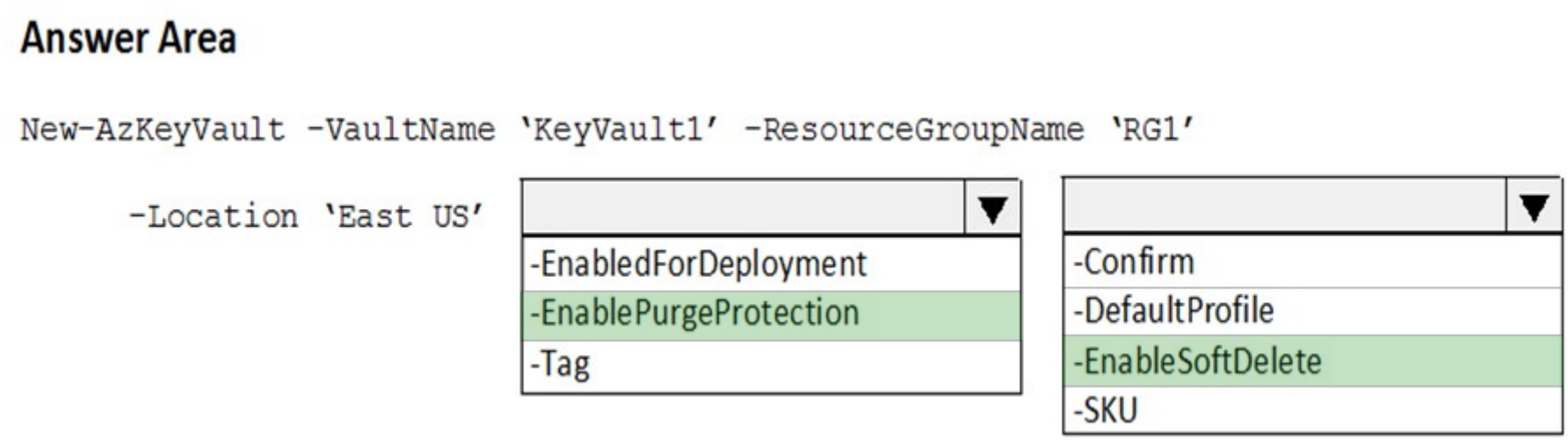
How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: -EnablePurgeProtection -

If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

Box 2: -EnableSoftDelete -

Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

Reference:

https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

macco455 3 months, 2 weeks ago

Outdated, Soft delete is enabled by default so you don't need to use that command anymore and you can't even turn it off.

upvoted 4 times

Fred64 2 months, 3 weeks ago

yes but you still need EnablePurgeProtection

upvoted 2 times

badaboom 3 months, 3 weeks ago

YES Correct answers !

upvoted 2 times

https://t.me/learningnets

Question #27 *Topic 4*

You have an Azure subscription that contains an Azure key vault named Vault1.
In Vault1, you create a secret named Secret1.
An application developer registers an application in Azure Active Directory (Azure AD).
You need to ensure that the application can use Secret1.
What should you do?

A. In Azure AD, create a role.

B. In Azure Key Vault, create a key.

C. In Azure Key Vault, create an access policy.

D. In Azure AD, enable Azure AD Application Proxy.

Correct Answer: *A* C
Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them.
Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active
Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.
Example: How a system-assigned managed identity works with an Azure VM
After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Oz Highly Voted 1 year, 7 months ago
Ref: https://docs.microsoft.com/en-us/azure/key-vault/tutorial-net-create-vault-azure-web-app

The correct answer is "set access policy" to the managed identity that app will use.
Example:
az keyvault set-policy --name '<YourKeyVaultName>' --object-id <PrincipalId> --secret-permissions get list
This command gives the identity (MSI) of the app service permission to do get and list operations on your key vault.
upvoted 77 times

gfhbox0083 Highly Voted 1 year ago
C, for sure.
Access Policy for Azure KeyVault
upvoted 22 times

Deepmindx Most Recent 2 weeks, 1 day ago
IN EXAM ### 29/6/2021
upvoted 1 times

rgullini 2 months, 1 week ago
Right now, both methods are available (RBAC, still in "preview") and Access Policies. So, either one of the other would make it. However, the question is old so, I think the correct answer more than 1 year ago was "Access policies"
upvoted 2 times

rgullini 2 months, 1 week ago
@Examtopics, please, correct this question answer and justification
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
Create a system-assigned managed identity for your application.
upvoted 1 times

Prod 3 months ago

https://t.me/learningnets

I am confused and worried after reading all the discussions. why did I spend my hard earned money on this site!! It looks like "No one knows what is correct answers". God knows even these questions are true or not! :(

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

The true purpose of this site is to make you think and research - resulting in learning. Not to just give you answers to memorize to pass an exam. Make the effort

upvoted 18 times

DCarma 2 weeks, 2 days ago

Then why provide 'answers' at all if they are incorrect 50% of the time? Surely you agree that it doesn't seem right that you pay for something and you have to find out from other paying members that what you paid for is incorrect?

upvoted 1 times

PaulMD 4 months, 1 week ago

Reading the reasoning, Option A should be managed identity

upvoted 1 times

seconazure 4 months, 2 weeks ago

Tested
Ans is C : In Azure Key Vault, create an access policy.

upvoted 6 times

sureshatt 4 months, 3 weeks ago

As everyone in here says, the correct answer is C. Managed identity only ease the authentication part, but the authorisation part still needs to be done. You need to use create an Access Policy in Key-vault (Since the RBAC is not still possible for data plane). See tutorial with the exact use-case as in the question: https://docs.microsoft.com/en-us/azure/key-vault/secrets/quick-create-net

upvoted 1 times

sureshatt 3 months, 2 weeks ago

Either we have to use Azure RBAC or an Access Policy to allow access to the Key Vault. In the case of managed identity, then you need to assign the Azure RBAC role "Key Vault Secret User" role to the managed identity. Therefore the given answer A has no meaning. You dont have to create any role new.

upvoted 1 times

milind8451 4 months, 3 weeks ago

"Set Access Policy" is the right answer

upvoted 2 times

Thi 5 months, 2 weeks ago

Answer is C:
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

upvoted 2 times

Iliyasm 5 months, 3 weeks ago

Answer is A, You need to create a managed identity role in order to give access to keyvault.

Please refer to troubleshooting area in this article where the developer is trying to give access to keyvault to an app

upvoted 1 times

zic04 5 months, 3 weeks ago

C for me !!!

upvoted 1 times

init2winit 6 months ago

Correct Answer is "Create an Access Policy"

upvoted 1 times

AzureGurl 6 months, 1 week ago

It should be create Access Policy. that is required for the application to get the key from KV.

upvoted 1 times

https://t.me/learningnets

Question #28 *Topic 4*

You have an Azure SQL database.
You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a stored access policy

B. a shared access signature (SAS)

C. the column encryption key

D. user credentials

E. the column master key

Correct Answer: *CE*
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

AS007 Highly Voted 1 year, 2 months ago
Correct ones
upvoted 15 times

gfhbox0083 Highly Voted 1 year ago
C, E, for sure.
upvoted 11 times

dfernandes Most Recent 3 days, 17 hours ago
also in AZ-301/304 exam
upvoted 1 times

kumax 3 weeks, 3 days ago
On exam, May 2021.
upvoted 1 times

sureshatt 4 months, 3 weeks ago
I think you only need the column master key and required permissions to read key metada from the database.
"Assuming your application has the required database permissions and can access the column master key, the Microsoft .NET Data Provider for SQL Server will encrypt any query parameters that target encrypted columns, and will decrypt data retrieved from encrypted columns, returning plaintext values of .NET types corresponding to the SQL Server data types set for the columns in the database schema."
https://docs.microsoft.com/en-us/sql/connect/ado-net/sql/sqlclient-support-always-encrypted?view=sql-server-ver15
upvoted 2 times

AzureGurl 6 months, 1 week ago
Answer is correct.
upvoted 3 times

aceking 6 months, 2 weeks ago
correct answer, for those who wants to visually see how it configured, go here (around 23min): https://www.youtube.com/watch?v=8sLeFgmjcc8
upvoted 4 times

PM2 6 months, 3 weeks ago
in the exam
upvoted 4 times

kdkdk 7 months ago
in the exams
upvoted 7 times

hstorm 10 months ago
I don't get it. Keys has to be stored in a key-vault, thus what we need is to provide access to the key-vault to retrieve the keys ??? Can anybody explain this Please ?
upvoted 2 times

DeepMoon 9 months, 1 week ago

https://t.me/learningnets

Read this article: Then You Will be Enlightened My Son
https://www.pass.org/PASS-Blog/introducing-always-encrypted-with-secure-enclaves-in-sql-server-2019-1

Stay Away From the Brahamins at Microsoft Doc For They Would Lead You Astray My Son
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15

upvoted 5 times

juselasmc 10 months, 1 week ago

IN THE EXAM

upvoted 7 times

kristiann21 1 year, 1 month ago

correct answer

upvoted 4 times

https://t.me/learningnets

Question #29 *Topic 4*

You have a hybrid configuration of Azure Active Directory (Azure AD).
All users have computers that run Windows 10 and are hybrid Azure AD joined.
You have an Azure SQL database that is configured to support Azure AD authentication.
Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises
Active Directory account.
You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.
Which authentication method should you instruct the developers to use?

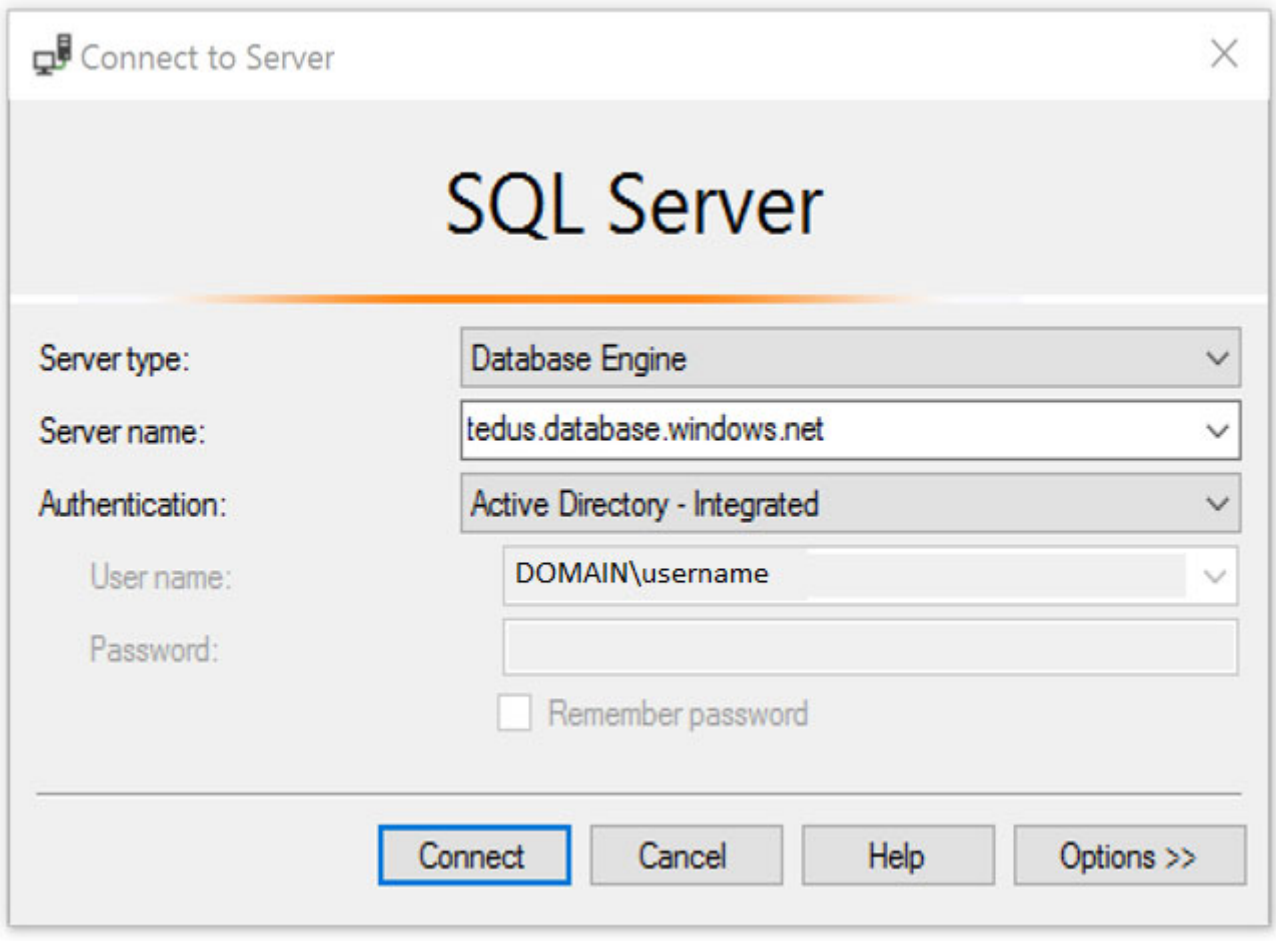
A. SQL Login

B. Active Directory ג€" Universal with MFA support

C. Active Directory ג€" Integrated

D. Active Directory ג€" Password

Correct 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.



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 IDג€ option is only supported for Universal with MFA connection options, otherwise it is greyed out.)
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell

kristiann21 Highly Voted 1 year, 1 month ago

https://t.me/learningnets

correct.

Hybrid AD, and workstations are domain joined. Hence integrated authentication will use a kerberos ticket to authenticate itself to the SQL server using the logged in user of the workstation.

upvoted 19 times

AS007 Highly Voted 1 year, 2 months ago

Correct Ans

upvoted 15 times

kumax Most Recent 3 weeks, 3 days ago

On exam, May 2021.

upvoted 1 times

PM2 4 months, 1 week ago

in the exam

upvoted 3 times

danwr81 4 months, 2 weeks ago

Since device is Hybrid AAD joined, PTA/PHS with SSO or Federation is required for that feature to work, therefore Integrated would work.

upvoted 1 times

Kinanke 5 months ago

Password Auth. See this source has same question : https://www.exam4training.com/which-authentication-method-should-you-recommend/

upvoted 1 times

HCL 5 months, 1 week ago

It is not a federated domain, nor managed domain (AAD DS). It is hybrid AD only.
So answer should be:
D. AD Password authentication

upvoted 3 times

B1T3X 6 months ago

It doesn't state there's any federation. The Azure AD Connect authentication isn't even specified. Therefore without any speculating the answer should be "Password"

upvoted 3 times

deegadaze1 5 months, 3 weeks ago

D- is the correct answer !!!

upvoted 2 times

AzureGurl 6 months, 1 week ago

Answer is correct. This is a tricky question, if the workstation is not in domain then it could be userid/password . since in this its a domain joined hence its integrated authentication.

upvoted 4 times

https://t.me/learningnets

Question #30 *Topic 4*

DRAG DROP -

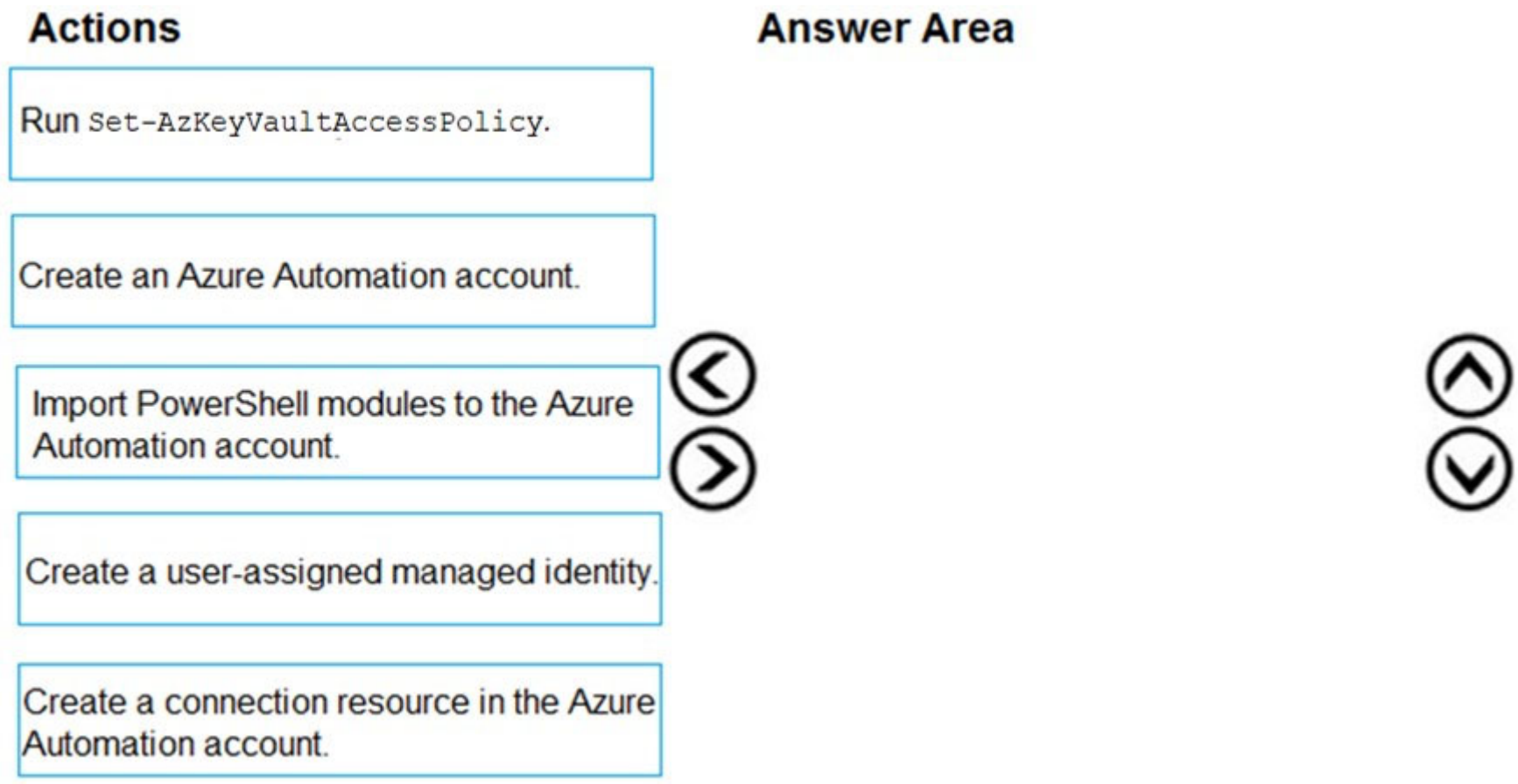
You have an Azure subscription named Sub1 that contains an Azure Storage account named contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of contosostorage1 and store them in Contosokeyvault1.

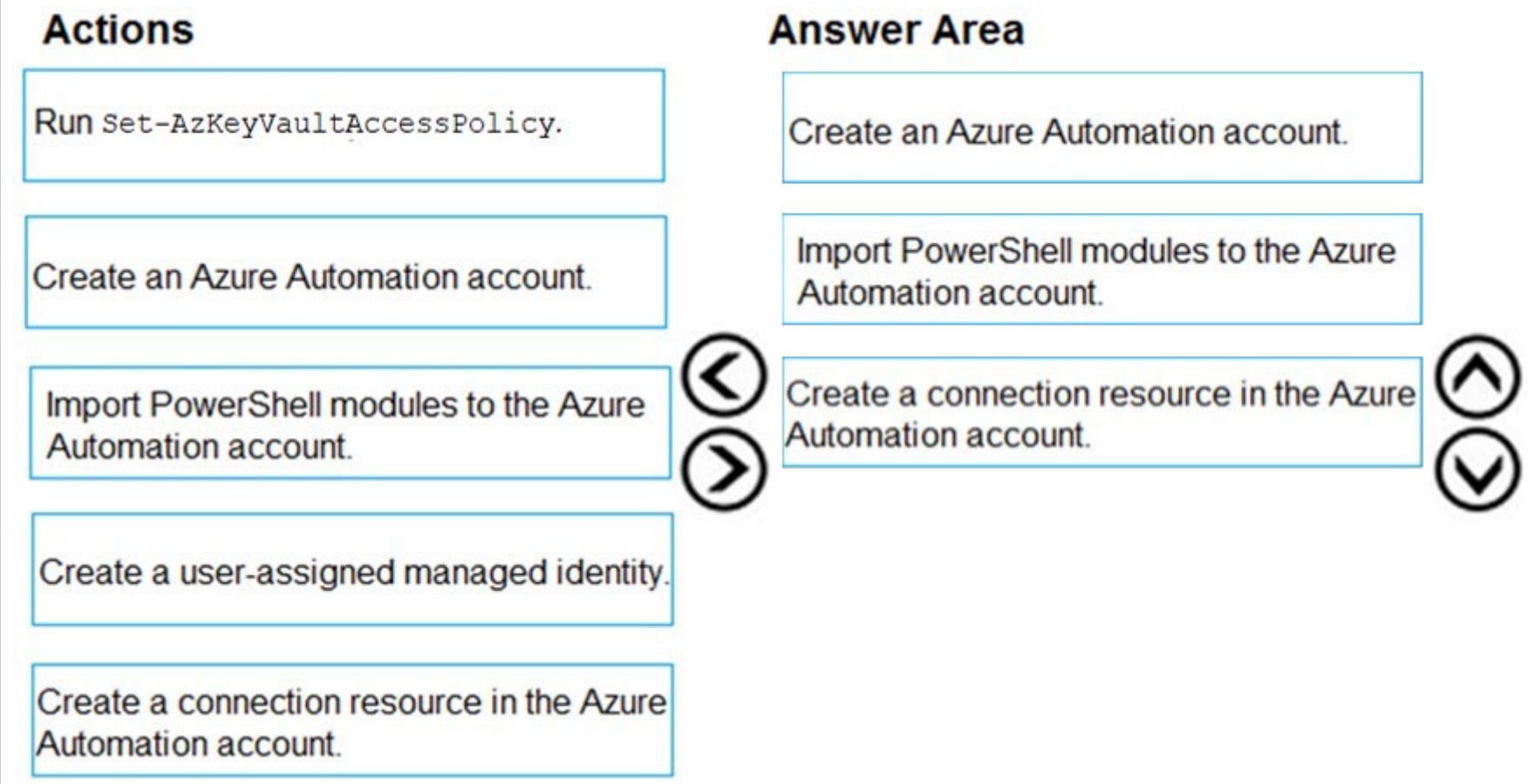
You need to implement prerequisites to ensure that you can implement the runbook.

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:



Correct Answer:



Step 1: Create an Azure Automation account

Runbooks live within the Azure Automation account and can execute PowerShell scripts.

Step 2: Import PowerShell modules to the Azure Automation account

Under ג€˜Assetsג€™ from the Azure Automation account Resources section select ג€˜to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Create a connection resource in the Azure Automation account

You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage

Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created ג€˜run as accountsג€™ above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get

https://t.me/learningnets

all the keys from the vault.
$connectionName = "AzureRunAsConnection"
try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName
"Logging in to Azure..."
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
Reference:
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

Pinto Highly Voted 3 months, 3 weeks ago
It should be:
Box1: Create azure automation account
Box2: Run Set-AzKeyVaultAccessPolicy.
Box3: Import powershell modules

A connection resource cannot function till access is set.

Also found this blog which agrees with what I believe is correct - https://kasunkodagoda.com/2018/05/07/key-rotation-made-easy-with-azure-key-vault-and-azure-automation/
upvoted 10 times

macco455 3 months, 2 weeks ago
Agree based on this article from 2 1/2 years ago, but things might have changed since then although I am not able to find anything else besides the article in the answer which is from almost 5 years ago. SO this is better than that and I will go with this as well.
upvoted 2 times

canonigo 3 months, 3 weeks ago
I agree.
upvoted 2 times

sureshatt 3 months, 2 weeks ago
I agree.
upvoted 2 times

kumax Most Recent 3 weeks, 3 days ago
On exam, May 2021.
upvoted 2 times

ZakS 1 month, 3 weeks ago
My thinking is that the given answers for boxes 1 and 2 are correct.
3rd box should be Run Set-AzKeyVaultAccessPolicy.

So, answers should be:
Box 1 - Create Azure Automation account (This step automatically creates the Azure Run As account)
Box 2 - Import PowerShell modules (Adds the required modules to the Automation account)
Box 3 - Run Set-AzKeyVaultAccessPolicy (Gives the Azure Run As account access to the Key Vault)
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
given answer seems correct - run set-az* could be the fourth step.
upvoted 3 times

souvik123 2 months, 1 week ago
I think the given answer is correct. Run Set-AzKeyVaultAccessPolicy can be the next step.
upvoted 1 times

https://t.me/learningnets

Question #31 *Topic 4*

HOTSPOT -

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

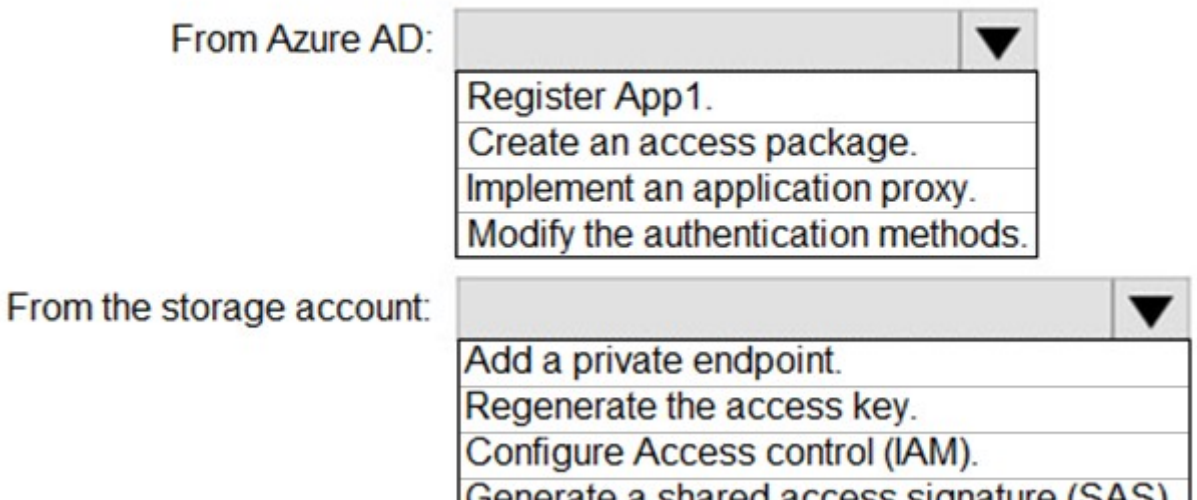
You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

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

NOTE: Each correct selection is worth one point.

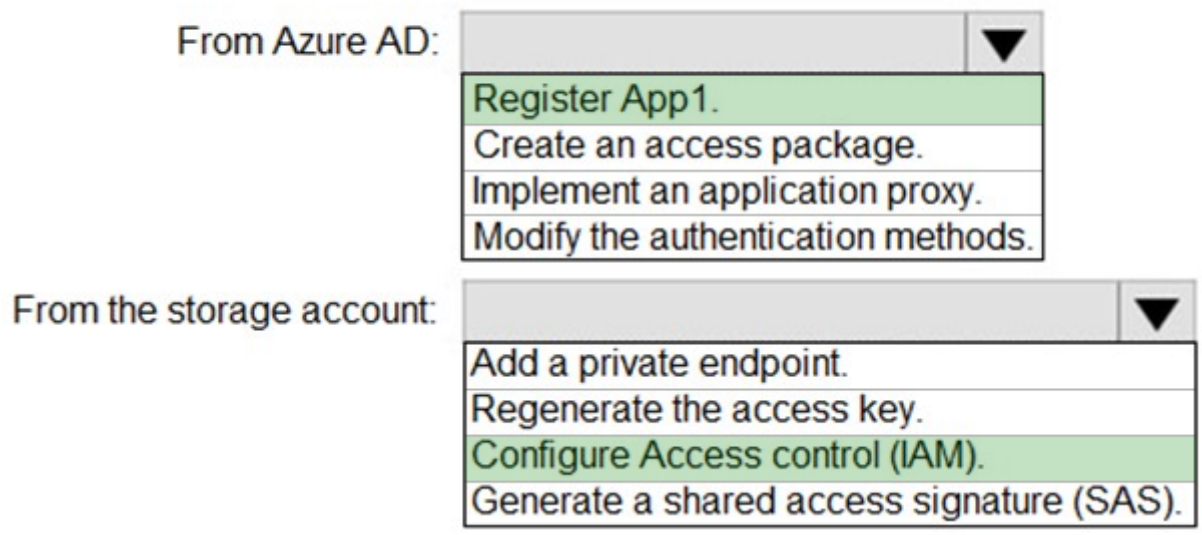
Hot Area:

Answer Area



Answer Area

Correct Answer:



Reference:

https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/ https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md

badaboom Highly Voted 3 months, 3 weeks ago

Correct !

upvoted 5 times

Pinto Most Recent 3 months, 3 weeks ago

seems correct.

upvoted 4 times

https://t.me/learningnets

Question #32 *Topic 4*

HOTSPOT -

You have an Azure subscription that contains an Azure key vault named ContosoKey1.

You create users and assign them roles as shown in the following table.

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	*None*
User2	Security Admin	*None*
User3	*None*	User Access Administrator
User4	*None*	Key Vault Contributor

You need to identify which users can perform the following actions:

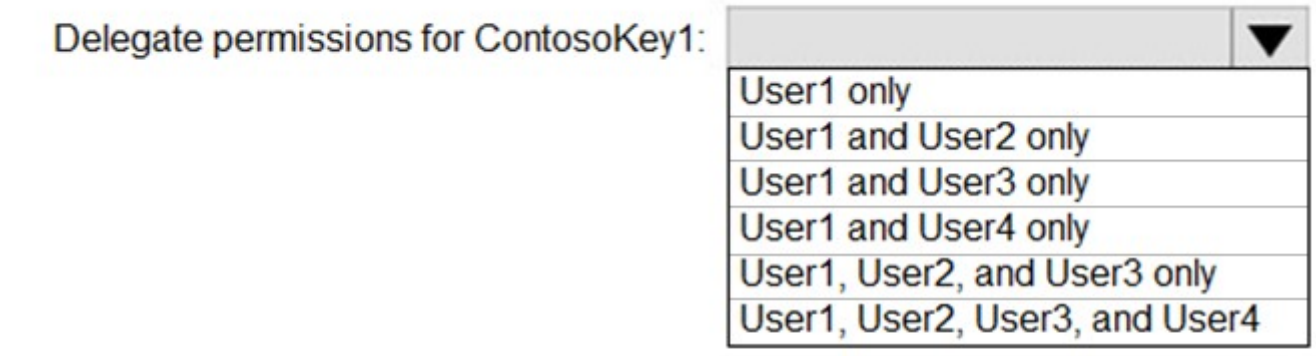
- Delegate permissions for ContosoKey1.
- Configure network access to ContosoKey1.

Which users should you identify? To answer, select the appropriate options in the answer area.

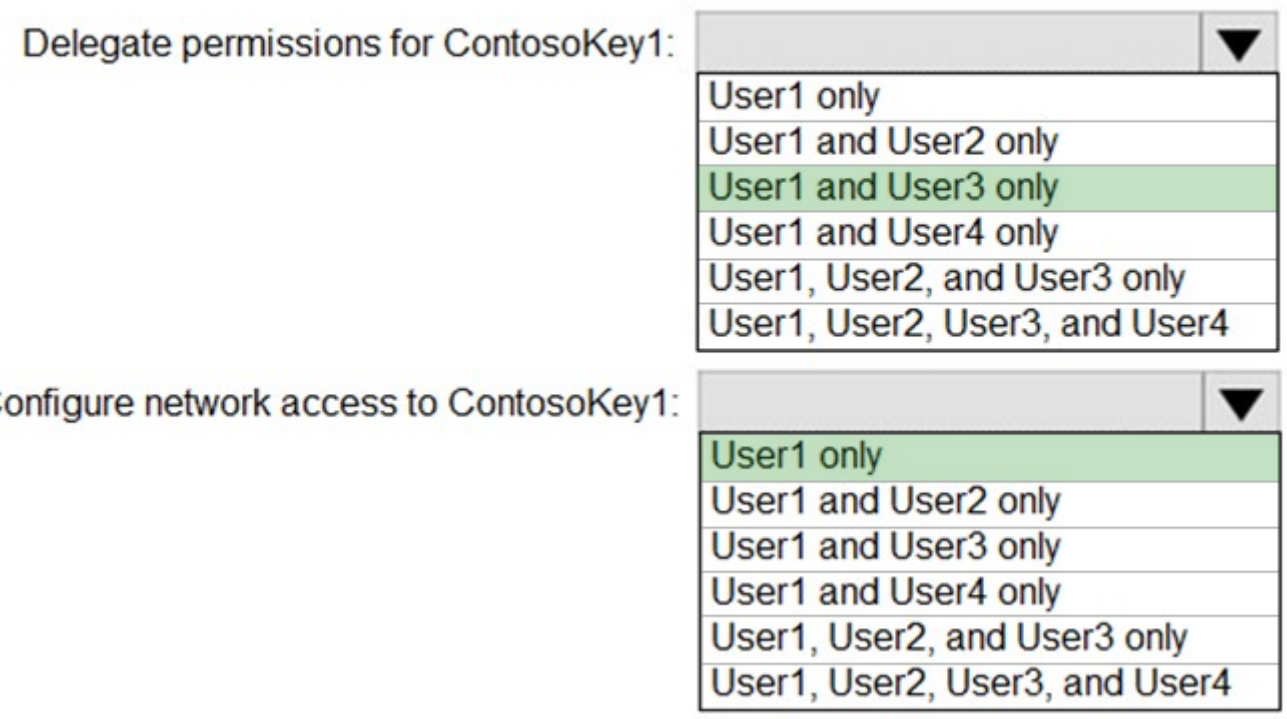
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Answer Area



Correct Answer:

Reference:

https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

cvarl Highly Voted 3 months, 4 weeks ago

Delegate permissions for ContosoKey1: User 1 and User 3
Configure network access to ContosoKey1: User 1 and User 4

https://t.me/learningnets

Key Vault Contributor role definition includes Microsoft.KeyVault/*, which means it has full rights and can therefore modify network access
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-contributor

upvoted 16 times

Pinto 3 months, 3 weeks ago

Not sure about box1,

Box1: User1 and User3/User4.
Box2: User1 and User4.
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault#management-plane-and-azure-rbac
https://docs.microsoft.com/en-us/azure/key-vault/general/security-overview
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

upvoted 1 times

guser99 3 months, 2 weeks ago

Tested in lab
Box1: User1,User3 and User4.
Box2: User1 and User4.

upvoted 3 times

macco455 3 months, 2 weeks ago

@guser99 Contributors on ANY blade have full right EXCEPT modifying permission which includes delegation. Therefore this is incorrect. COrrect answer are:
Box 1: User 1 and User 3
Box 2: User 1 and User 4

upvoted 1 times

russ0 2 months, 2 weeks ago

Box 2 should be User 1 only since Key Vault Contributor role is for management plane operations to manage key vaults. It does not allow access to keys, secrets and certificates.

upvoted 2 times

Cyberbug2021 Highly Voted 2 months, 2 weeks ago

A contributor does not have rights to grant permissions, check microsoft.keyvault/* does not include network access -
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkeyvault

box 1 - user 1 and user 3
box 2 - user 1

upvoted 7 times

zsedo 1 month ago

One only need Microsoft.KeyVault/vaults/accessPolicies/write which is part of the Key Vault Contributor role.
You can add a single IP range, don't need to read the network configs (vnet/subnet)

upvoted 1 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago

"Contributor" role is different than "Key Vault Contributor" Role

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

Key Vault Contributor role is for management plane operations to manage key vaults. It does not allow access to keys, secrets and certificates.

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

Contributor
Create and manage all of types of Azure resources
Create a new tenant in Azure Active Directory
Cannot grant access to others

upvoted 1 times

https://t.me/learningnets

Question #33 *Topic 4*

You have an Azure subscription that contains four Azure SQL managed instances.

You need to evaluate the vulnerability of the managed instances to SQL injection attacks.

What should you do first?

A. Create an Azure Sentinel workspace.

B. Enable Advanced Data Security.

C. Add the SQL Health Check solution to Azure Monitor.

D. Create an Azure Advanced Threat Protection (ATP) instance.

Correct Answer: *B*

ttomaszoex Highly Voted 5 months, 1 week ago

the answer is correct. see https://www.sqlshack.com/advanced-data-security-in-azure-sql-database-data-discovery-classification/ however this feature has been renamed by Microsoft to Azure Defender for SQL

upvoted 11 times

JCWF 4 months ago

https://docs.microsoft.com/en-gb/azure/azure-sql/database/azure-defender-for-sql

upvoted 2 times

sureshatt Highly Voted 4 months ago

This question is outdate. Now you can enable Azure Defender for SQL at server level or DB level.

upvoted 7 times

Super_Pun Most Recent 4 months ago

Given answer is correct
Advanced Data Security helps to detect SQL vulnerable for four Azure SQL managed instances.

upvoted 1 times

Narragr 4 months, 1 week ago

I would go for D. "Advanced Threat Protection provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Users receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access and queries patterns."

Source: https://docs.microsoft.com/en-gb/azure/azure-sql/database/threat-detection-overview

upvoted 6 times

Jul1 5 months, 1 week ago

I would go for advanced data security because it has to be enabled, not created :)

upvoted 2 times

Dolmance_ 5 months, 1 week ago

I would go for D (ATP). According to https://docs.microsoft.com/pl-pl/azure/azure-sql/database/threat-detection-overview , “Users receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks...”

upvoted 3 times

Thi 5 months, 1 week ago

As i read about articles B & D can be answer to evaluate sql injection attack if someone have correct answer then share.

upvoted 1 times

HCL 5 months, 1 week ago

Given answer seems to be correct, but couldn't find docs with the name "Advanced Data Security".
Only a YT video is found: https://www.youtube.com/watch?v=XwxIlZTNUSY (09:23)

upvoted 6 times

https://t.me/learningnets

Question #34 *Topic 4*

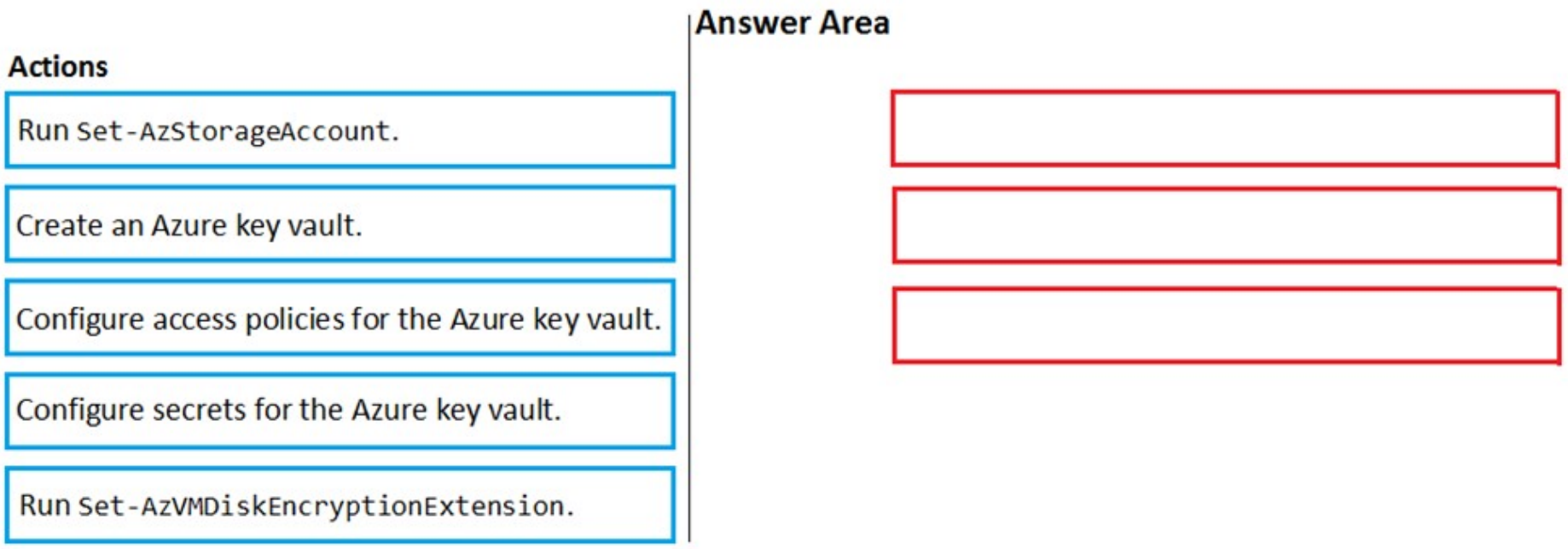
DRAG DROP -

You have an Azure subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

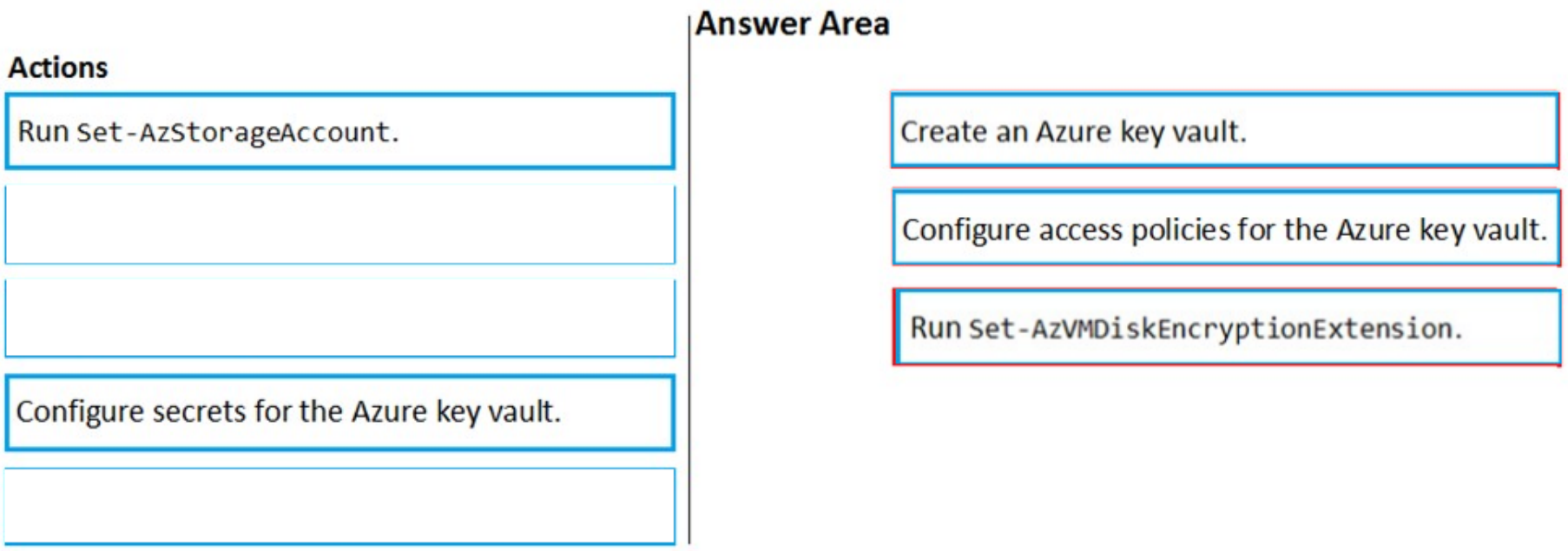
You need to encrypt VM1 disks by using Azure Disk Encryption.

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:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

badaboom Highly Voted 3 months, 3 weeks ago

Seems correct !

upvoted 12 times

https://t.me/learningnets

Question #35 *Topic 4*

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

- Name: Vault5
- Region: West US
- Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.

Which key vault settings should you configure?

A. Access policies

B. Secrets

C. Keys

D. Locks

Correct Answer: *A*

Reference:

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

gfhbox0083 Highly Voted 1 year ago

A for sure.
Access Policies.

upvoted 17 times

Prash85 Highly Voted 1 year, 4 months ago

answer is A. Access policies

upvoted 12 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 1 times

milind8451 4 months, 3 weeks ago

A) is right ans.

upvoted 2 times

milind8451 4 months, 3 weeks ago

Correct ans.

upvoted 2 times

zic04 5 months, 3 weeks ago

A agree

upvoted 2 times

AzureGurl 6 months, 1 week ago

Answer is correct, Create KV, Set Access Policy (advance), use the KV for VM

upvoted 4 times

GayanWK 7 months ago

https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-encryption#provide-permissions

upvoted 2 times

Stuudent 7 months, 3 weeks ago

You need that for the VM to be able to access the KeyVault.

upvoted 2 times

kristiann21 1 year, 1 month ago

correct answer.

upvoted 7 times

D0yle 1 year, 5 months ago

Hmmm,. it is a tricky one - we need to have access policy for Backup Services but in my case it was created atomatically during the enabling backup of the VM. We still need to have keys in Key Vault and keys come first - then the access policy.

upvoted 3 times

azurearch 1 year, 4 months ago

https://t.me/learningnets

question is which key vault setting you would configure for backing up VM, not what is the first activity to do this.

upvoted 11 times

https://t.me/learningnets

Question #36 *Topic 4*

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Type	Region	Resource group
sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.
What should you do?

A. Enable a managed identity on VM1.

B. Create a secret in KV1.

C. Configure a service endpoint on SQL1.

D. Create a key in KV1.

Correct Answer: *B*
A

benito_nepomuceno Highly Voted 4 months ago
A. Enable a managed identity on VM1.
upvoted 16 times

rgullini 2 months, 3 weeks ago
Isn´t it the B option as the request is tosecure access to a database on SQL1 by using a contained database user?
upvoted 2 times

rgullini 2 months, 3 weeks ago
Dismiss my comment. VM and keyvault should be in the same region.
upvoted 1 times

maxstv 4 months ago
Agree here.

A. Enable a managed identity on VM1.

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql
upvoted 8 times

Super_Pun Highly Voted 4 months ago
Given answer is correct
The question is "secure access to a database on SQL1 by using a contained database user"
by using contained database user... it means no need to enable manage identity
upvoted 8 times

sureshatt 3 months, 2 weeks ago
I disagree. contained database user does not mean/or nothing to do with managed identity. Contained database user can be mapped to Azure AD identity.

"However, using Azure Active Directory authentication with SQL Database and Azure Synapse requires using contained database users based on an Azure AD identity. A contained database user does not have a login in the master database, and maps to an identity in Azure AD that is associated with the database. The Azure AD identity can be either an individual user account or a group." https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

Therefore, a managed identity should also be possible to mapped to a contained user similar to a user identity in azure ad.
upvoted 2 times

sureshatt 3 months, 2 weeks ago
See https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql
"Create a contained user in the database that represents the VM's system assigned identity"
upvoted 1 times

Rume Most Recent 1 week, 6 days ago
Answer is A - Managed Identity
upvoted 1 times

ysm 1 month, 2 weeks ago

https://t.me/learningnets

Since it's contained user so no need for storing passwords nor users since they already are in the db.
answer should be about the network access which is service endpoint.

upvoted 2 times

besha 2 weeks, 3 days ago

No! That should be private endpoint not service endpoint!

upvoted 1 times

kra96 2 months ago

Option C. thats secure way of configuring access to SQL service instances.

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

Answer A would apply to regular SQL database but not to Contained Database User, https://docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable?view=sql-server-ver15

upvoted 1 times

JOKERO 2 months, 3 weeks ago

the key vault is in a different region (not possible)

upvoted 1 times

JOKERO 2 months, 3 weeks ago

why not service endpoint ? https://docs.microsoft.com/fr-fr/azure/virtual-network/virtual-network-service-endpoints-overview
it's a secure connection

upvoted 1 times

JOKERO 2 months, 3 weeks ago

ignore; For Azure SQL, a service endpoint applies only to Azure service traffic within a virtual network's region.

upvoted 1 times

dadageer 4 months ago

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql

upvoted 5 times

https://t.me/learningnets

Question #37 *Topic 4*

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:

- Name: VM1
- Size: DS2v2
- Resource group: RG1
- Region: West Europe
- Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

A. Vault1 or Vault3 only

B. Vault1, Vault2, Vault3, or Vault4

C. Vault1 only

D. Vault1 or Vault2 only

Correct Answer: *A*

In order to make sure the encryption secrets donλ€™t cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites

kristiann21 Highly Voted 1 year, 1 month ago

correct answer.

upvoted 22 times

gfhbox0083 Highly Voted 1 year ago

A, for sure

Same Azure Region for KeyVault

upvoted 15 times

Cyberbug2021 Most Recent 2 months, 2 weeks ago

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away, but within the same geography to maintain high durability of your keys and secrets.

upvoted 1 times

PM2 4 months, 1 week ago

in the exam

upvoted 5 times

sureshatt 4 months, 2 weeks ago

Correct answer.

"Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don't cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be co-located in the same region."

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

upvoted 1 times

mayenite 5 months, 2 weeks ago

correct answer. Resource Group is irrelevant.

Azure Disk Encryption requires an Azure Key Vault to control and manage disk encryption keys and secrets. Your key vault and VMs must reside in the same Azure region and subscription.

upvoted 2 times

btxy4 9 months, 1 week ago

"Azure Disk Encryption requires an Azure Key Vault to control and manage disk encryption keys and secrets. Your key vault and VMs must reside in the same Azure region and subscription."

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

upvoted 1 times

https://t.me/learningnets

Exam_Master_Me 12 months ago

Correct.

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-key-vault
states: Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don't cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same subscription and region as the VMs to be encrypted.

upvoted 3 times

gboyega 1 year ago

A is correct

upvoted 8 times

certifiedgeek 1 year ago

Based on https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview#encryption-key-storage-requirements. "Azure Disk Encryption requires an Azure Key Vault to control and manage disk encryption keys and secrets. Your key vault and VMs must reside in the same Azure region and subscription." - So this should be Vault1 only

upvoted 3 times

Appyfiz 11 months, 3 weeks ago

All vaults are in same subscription and region but different resource group. Hence, answer A stands true.

upvoted 8 times

https://t.me/learningnets

Question #38 *Topic 4*

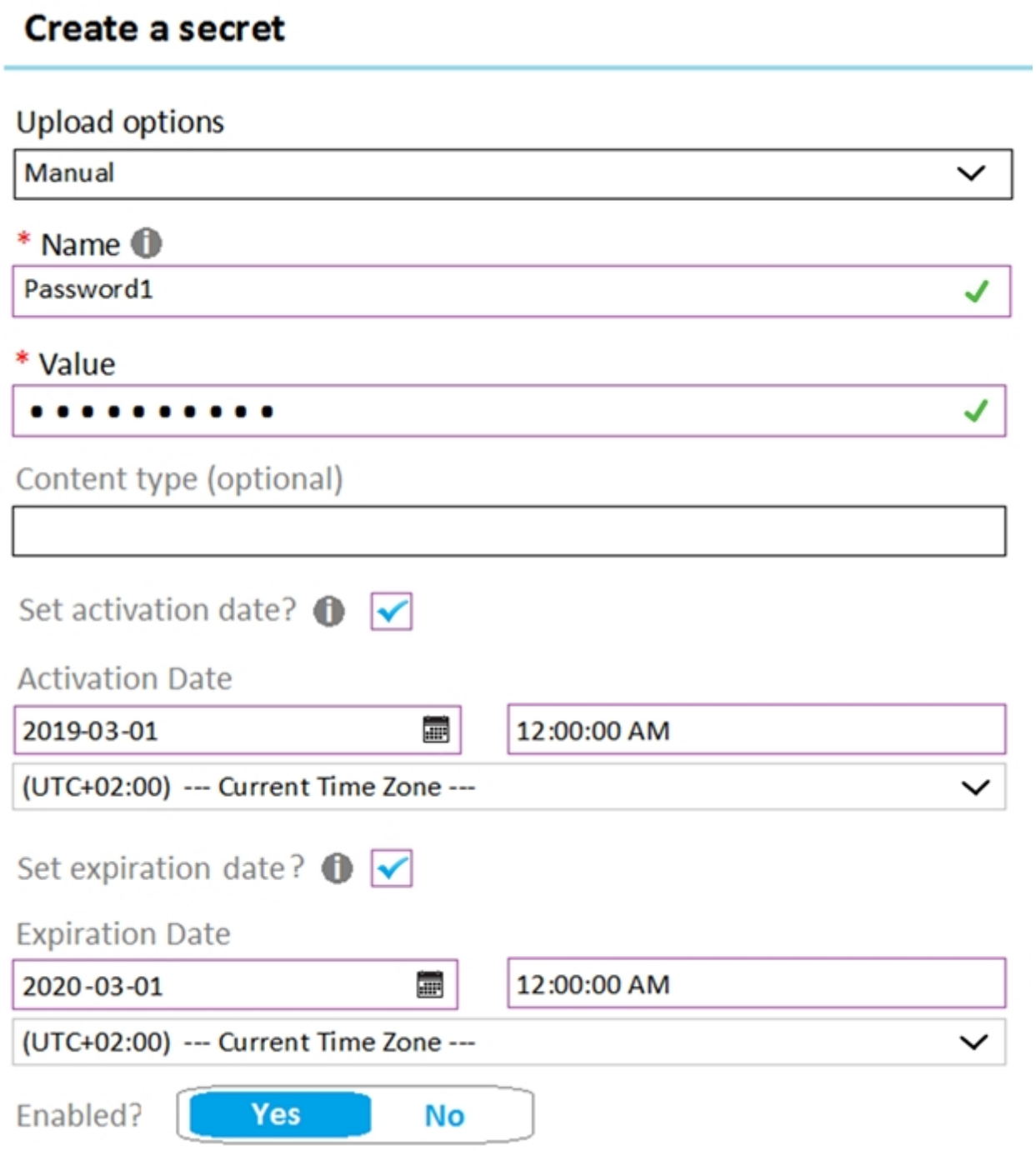
HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
User1	Azure Active Directory (Azure AD) user
User2	Azure Active Directory (Azure AD) user
Group1	Azure Active Directory (Azure AD) group
Vault1	Azure key vault

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. The date format YYYY-MM-DD is used on the exhibit. (Click the Exhibit tab.)



User2 is assigned an access policy to Vault1. The policy has the following configurations:

- Key Management Operations: Get, List, and Restore
- Cryptographic Operations: Decrypt and Unwrap Key
- Secret Management Operations: Get, List, and Restore

Group1 is assigned an access policy to Vault1. The policy has the following configurations:

- Key Management Operations: Get and Recover
- Secret Management Operations: List, Backup, and Recover

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

https://t.me/learningnets

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	○	○
On June 1, 2019, User2 can view the value of Password1.	○	○
On June 1, 2019, User1 can view the value of Password1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	○	●
On June 1, 2019, User2 can view the value of Password1.	●	○
On June 1, 2019, User1 can view the value of Password1.	○	●

dadageer Highly Voted 4 months ago

Tested answers:

1) On Jan 1 2019 User 1 can view the password 1 - No (Error: Either this secret is disabled or you do not have the "Get" secret permission.)

2) On June 1 2019 User2 can view the password1 - YES

3) On June 1 2019 User1 can view the Password1 - No

User 2 can see the Value no issues regardless of date because he has GET Secret Permission

upvoted 12 times

Sethoo 3 months, 4 weeks ago

Group 1 , which user 1 belongs to does not have the "Get" permission so that must explain your results in 1. I am surprised the result tested No for 3, i was expecting a yes because of the dates or because Group 1 does not have the "Get" permission, they don't have access to the password irrespective of the date. thank you for running the test

upvoted 1 times

dadageer 3 months, 3 weeks ago

Yes "Get" permission is must to see the password. Even if Secret is enabled and within valid date you get error "Either this secret is disabled or you do not have the "Get" secret permission"

upvoted 2 times

kumax Most Recent 3 weeks, 3 days ago

On exam, May 2021.

upvoted 2 times

gwin 1 month, 1 week ago

Good everyone, i have an issue navigating with the simulation section environment during exams Az 500 can anyone put me through ?

upvoted 1 times

davidkerr7 2 months ago

Though #3 should have been yes, since Group 1 has the "Get"

upvoted 1 times

BalderkVeit 1 month, 3 weeks ago

it doesn't. It's a secret, not a key.

upvoted 2 times

Cyberbug2021 2 months, 2 weeks ago

https://t.me/learningnets

Secret Management Operations: Get

upvoted 1 times

Fred64 2 months, 3 weeks ago

activation and expiration date are just declarative. They involve no constraint in practice. So the only question is to have permission to decrypt key. The proposed answer is OK

upvoted 2 times

https://t.me/learningnets

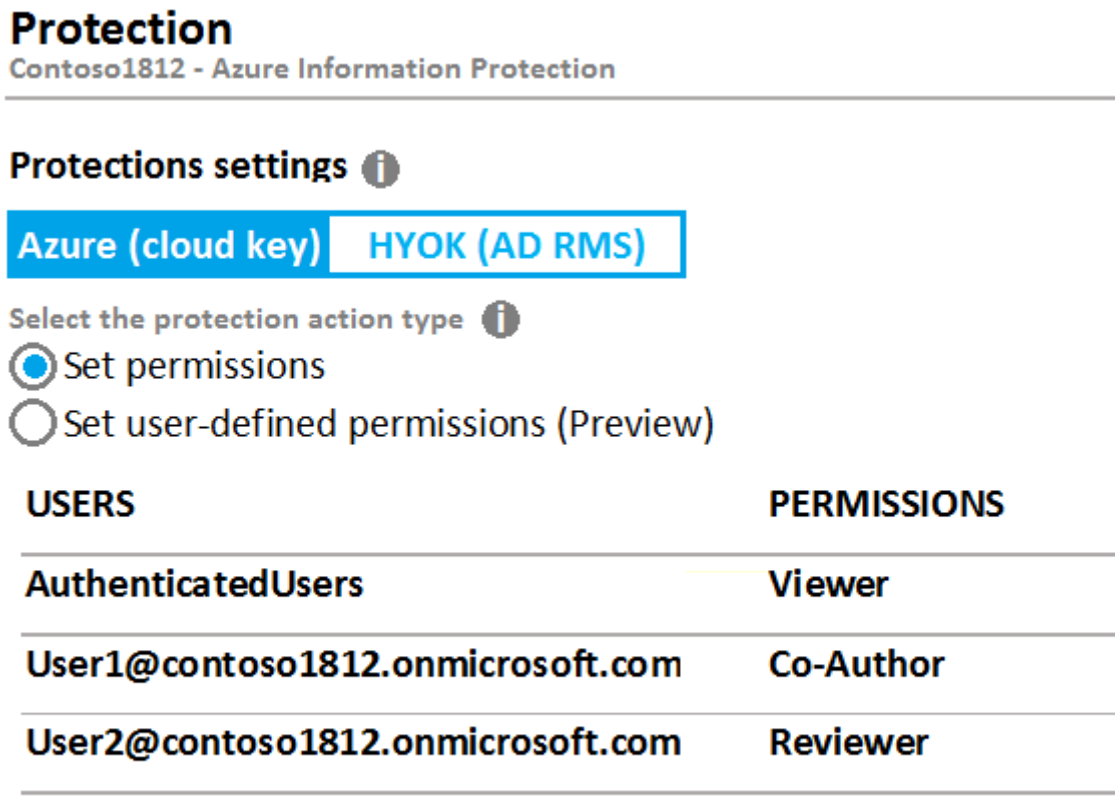
Question #39 *Topic 4*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

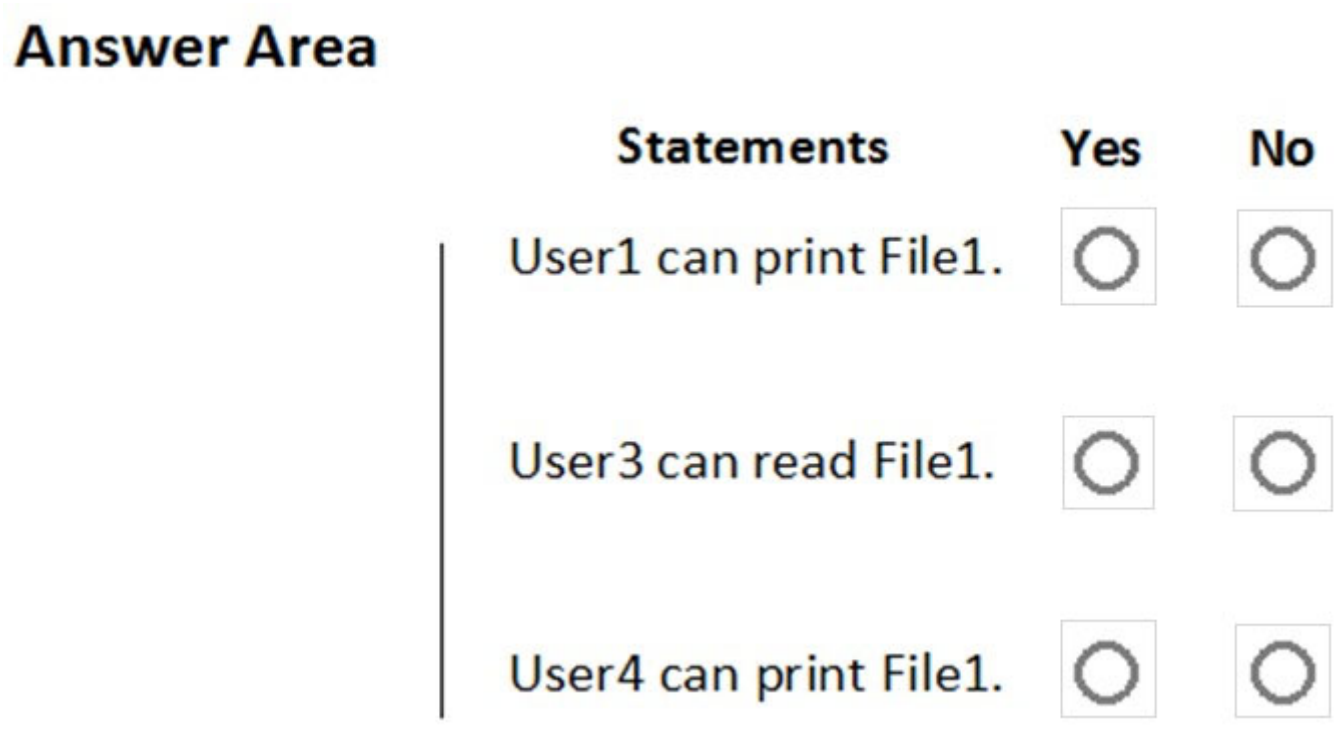


Label1 is applied to a file named File1.

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

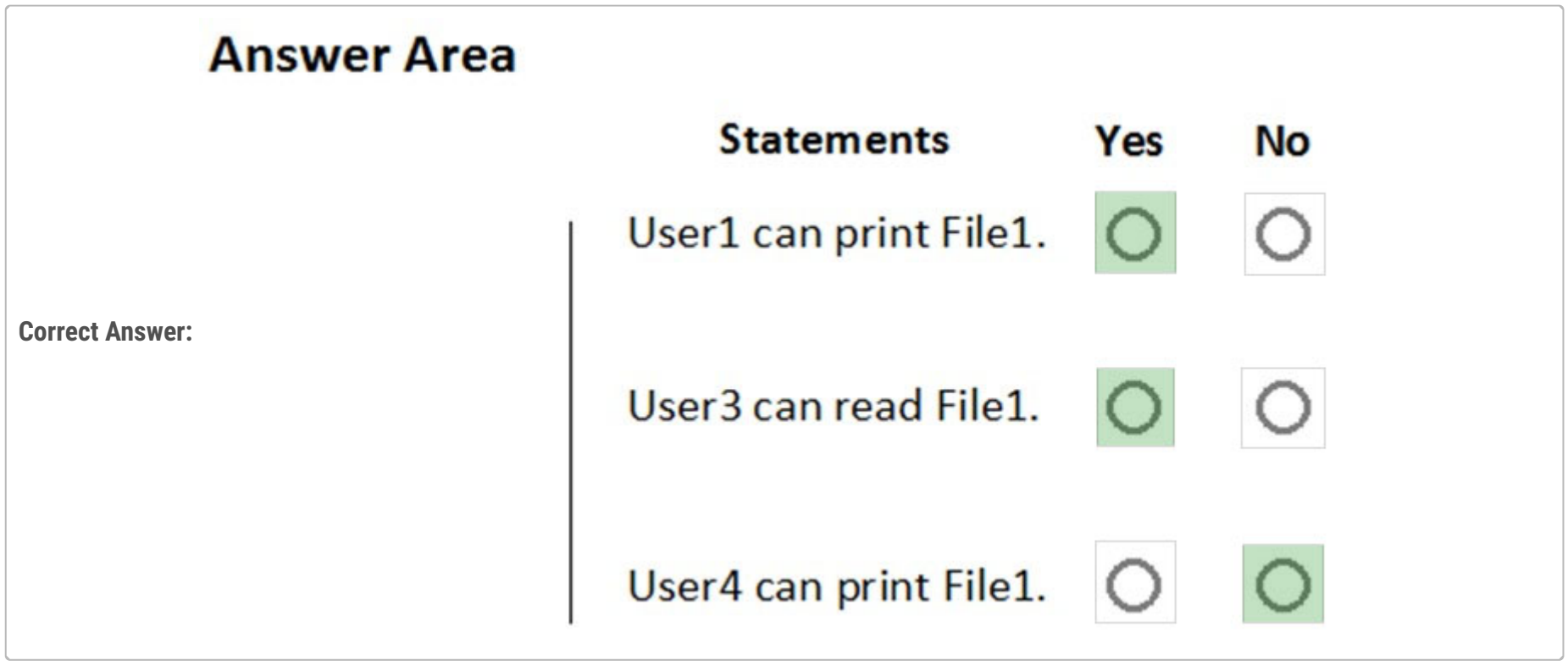
NOTE: Each correct selection is worth one point.

Hot Area:



https://t.me/learningnets

Correct Answer:



AcTiVeGrEnAdE Highly Voted 3 months, 4 weeks ago

Given answer is correct.

upvoted 6 times

Cyberbug2021 Highly Voted 2 months, 2 weeks ago

Tip- don't forget the first line authenticateduser - viewer

upvoted 5 times

DCarma Most Recent 2 weeks, 3 days ago

1) YES - User 1 is a co-author, therefore can: View, Open, Read; Save; Edit Content, Edit; Copy; View Rights; Allow Macros; Save As, Export; Print; Repy; Reply All; Forward.

2) YES - User 3 is an AuthenticatedUser and therefore a viewer, so can: View, Open, Read; View Rights; Reply; Reply All; Allow Macros.

3) NO - User 4 is a guest, and has no permissions to this file.

https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights

upvoted 1 times

Sethoo 3 months, 4 weeks ago

My first take is a YES, YES, No as well.

upvoted 4 times

https://t.me/learningnets

Question #40 *Topic 4*

SIMULATION -

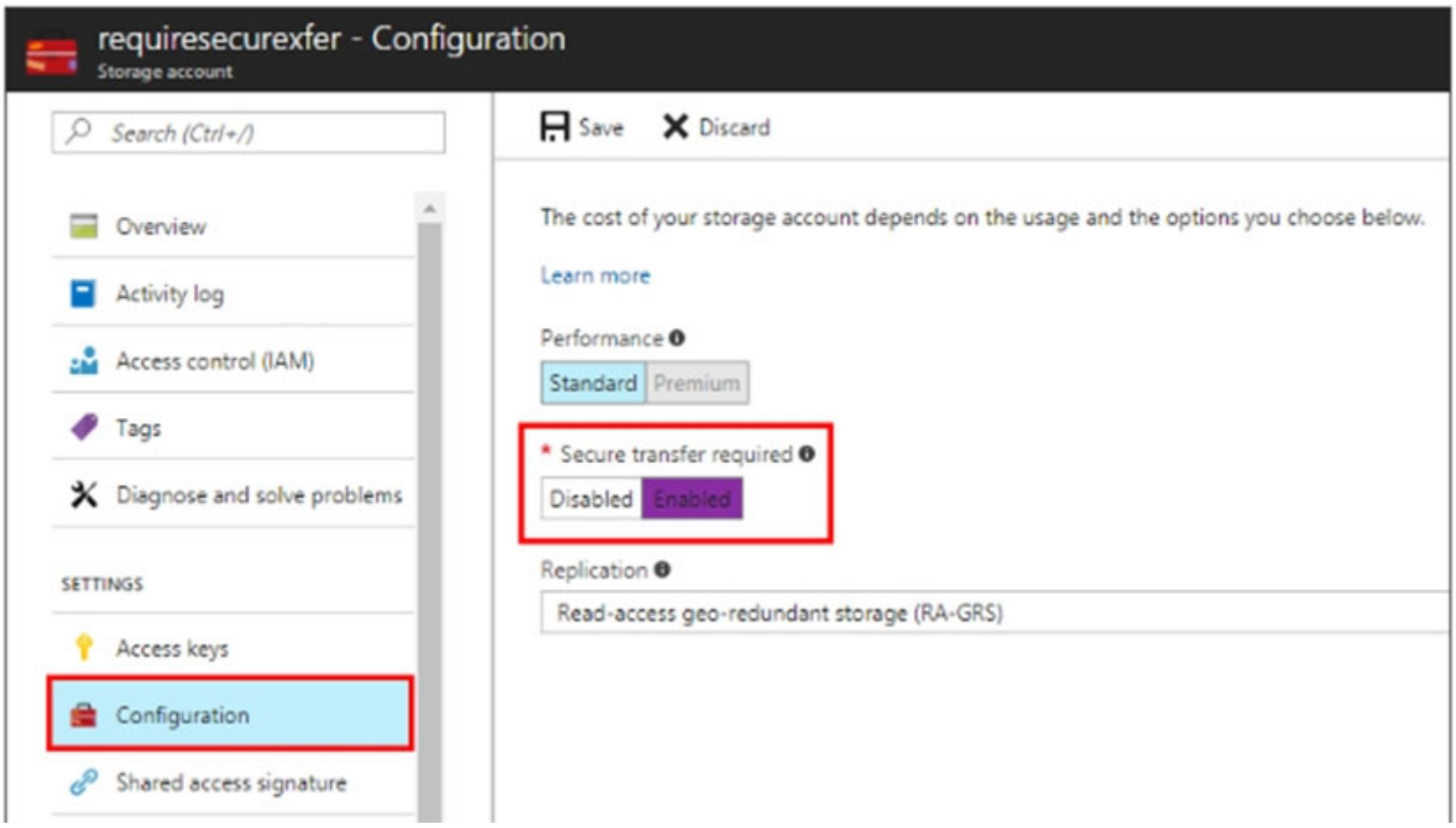
You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account.

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
2. Select Configuration, and Secure Transfer required.



Reference:

https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storage/m-p/82475

gwin 1 month, 1 week ago

Good everyone, i have an issue navigating with the simulation section environment during exams Az 500 can anyone put me through ?

upvoted 1 times

https://t.me/learningnets

Question #41 *Topic 4*

DRAG DROP -

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

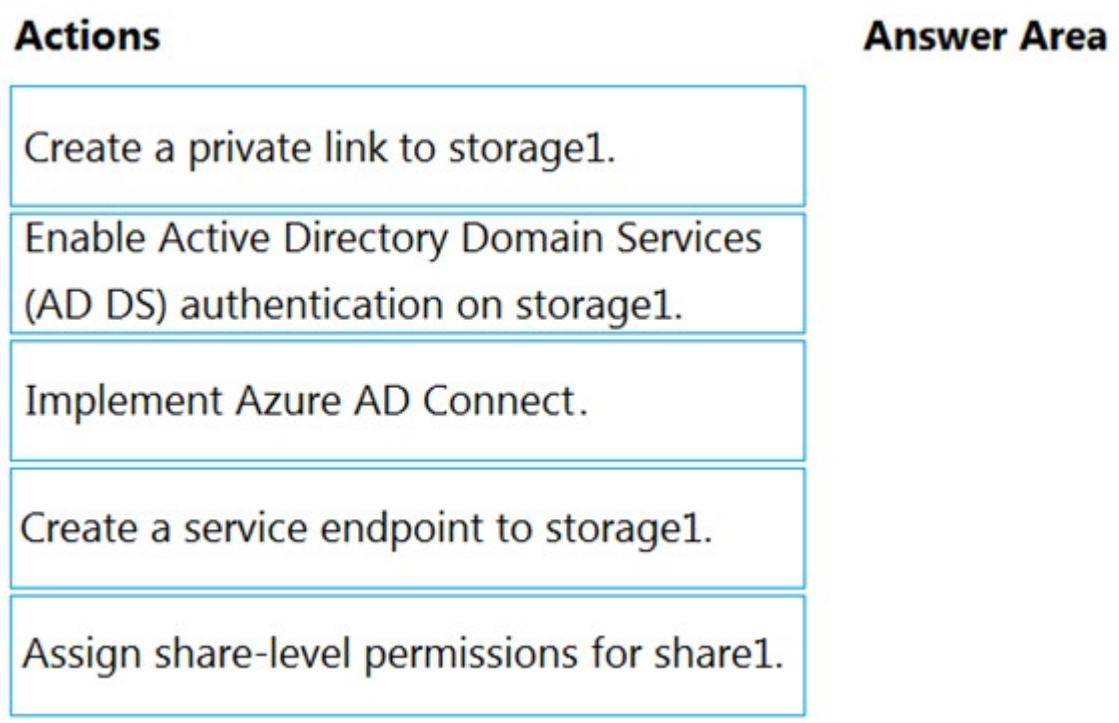
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

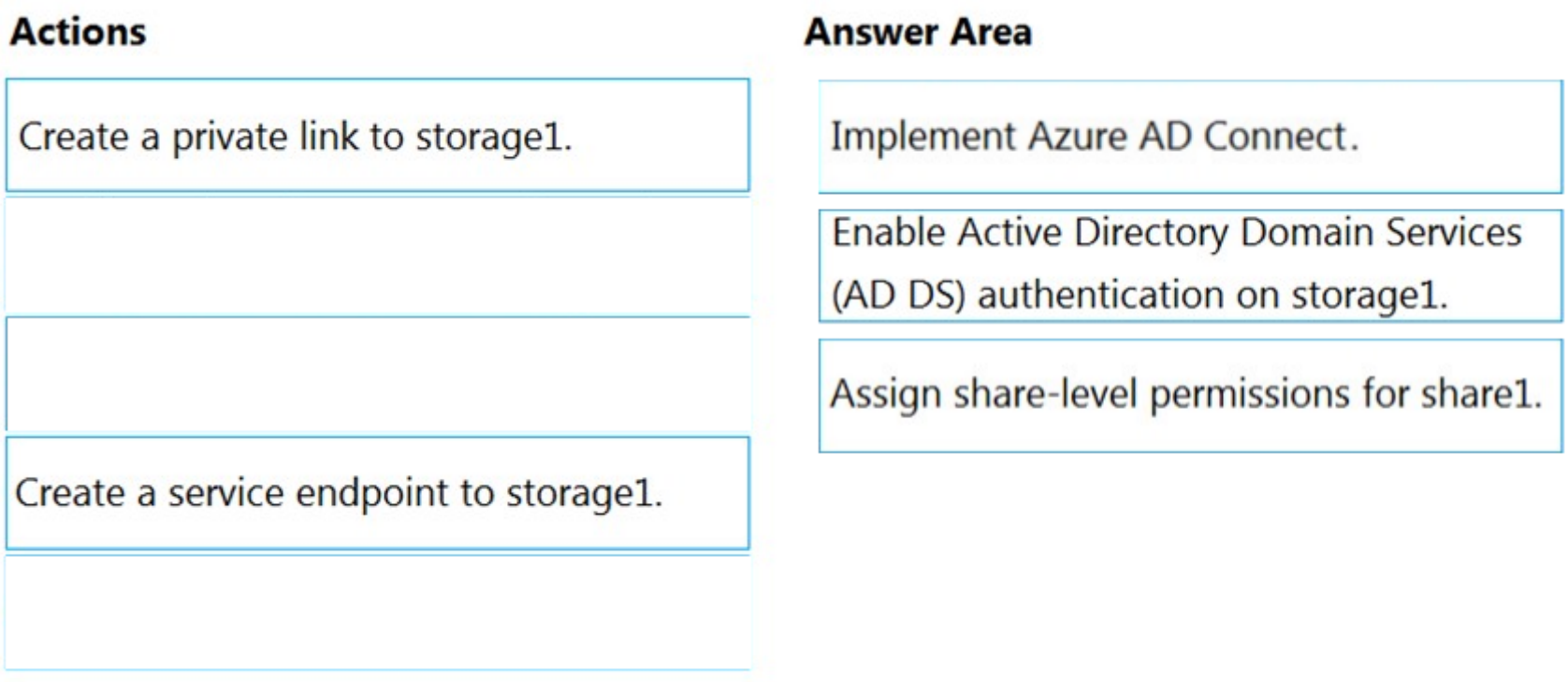
You need to ensure that User1 can access share1 by using his domain credentials.

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.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable

macco455 Highly Voted 3 months, 2 weeks ago

Looks good to me

upvoted 5 times

hendry781 Most Recent 3 months, 1 week ago

wrong. answer to (2) should be create a private link to storage1

upvoted 1 times

OhBee 3 months ago

The answer is correct.

Ref: https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable?tabs=azure-portal

upvoted 12 times

https://t.me/learningnets

https://t.me/learningnets

Question #42 *Topic 4*

SIMULATION -

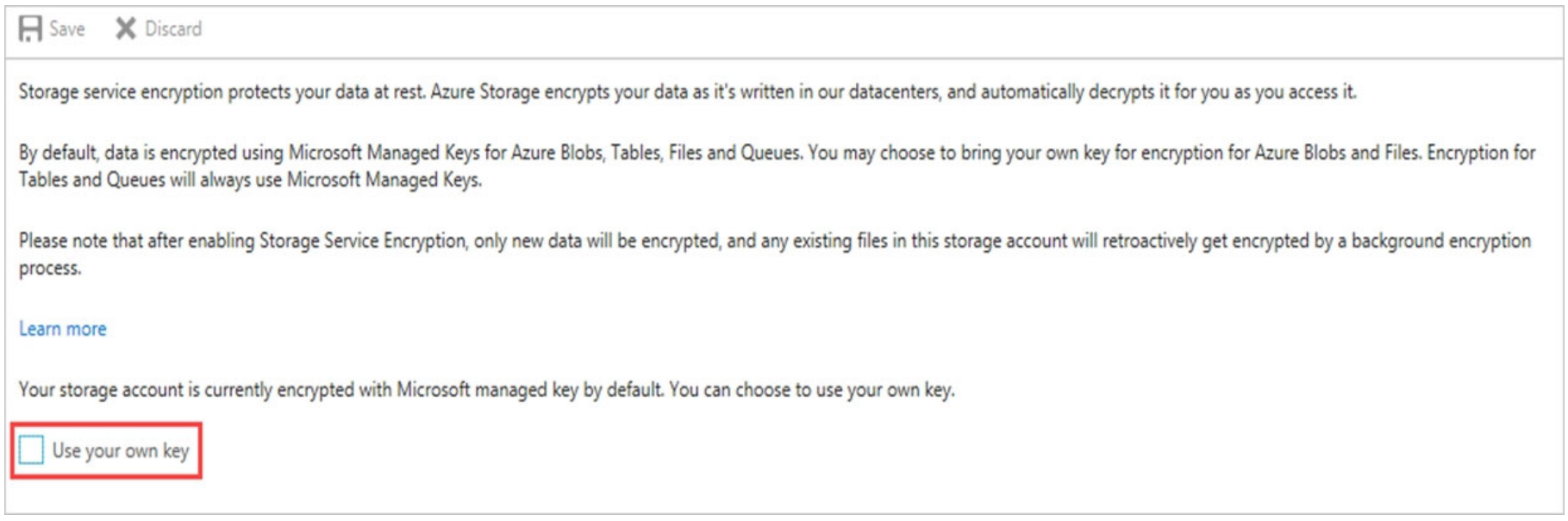
You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.

To complete this task, sign in to the Azure portal.

Correct Answer: *See the explanation below.*

Step 1: To enable customer-managed keys in the Azure portal, follow these steps:

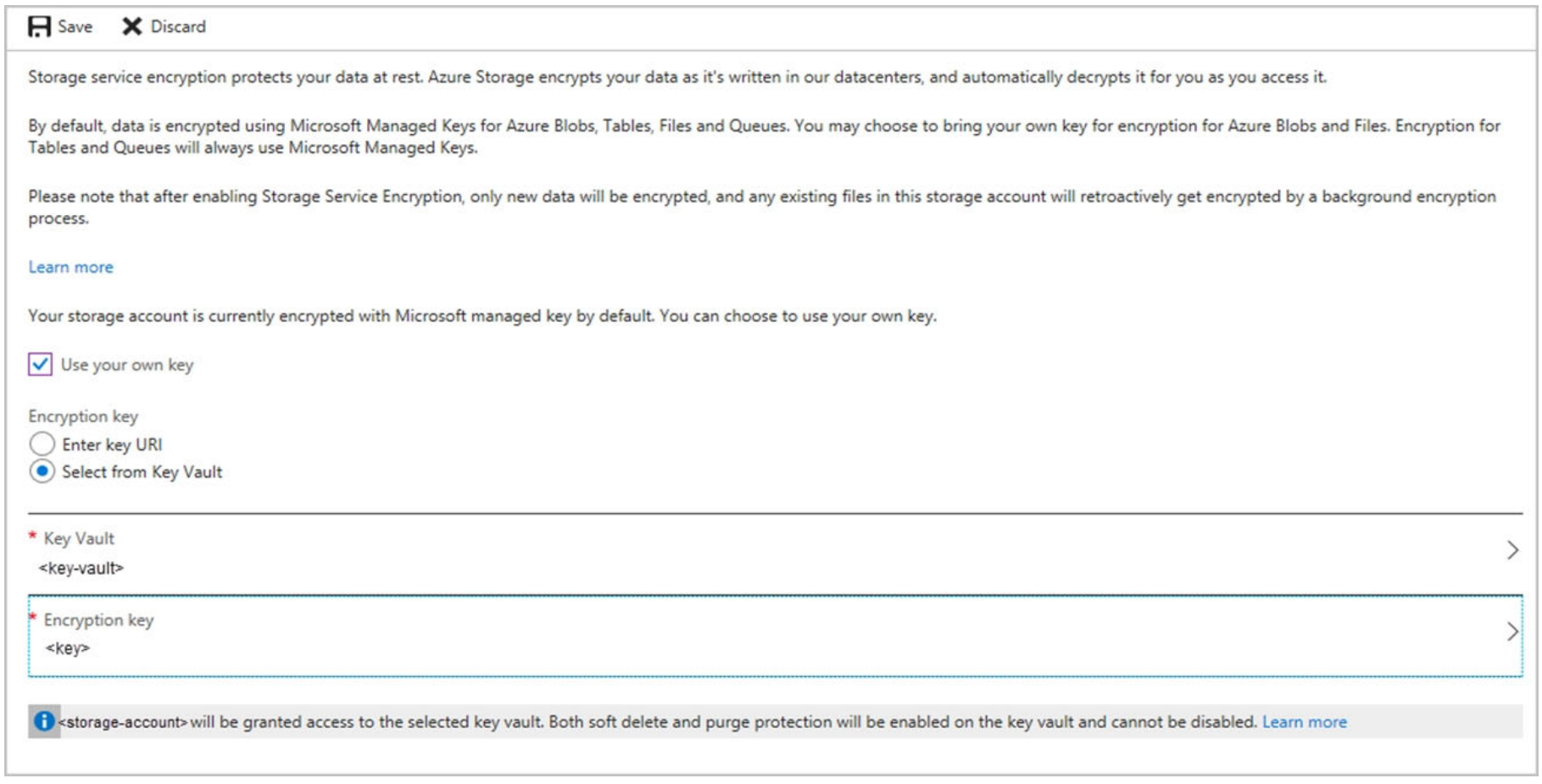
1. Navigate to your storage account rg1lod10598168n1
2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.



Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

4. Choose the Select from Key Vault option.
5. Choose the key vault KeyVault10598168 containing the key you want to use.
6. Choose the key from the key vault.



Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal

gwin 1 month, 1 week ago

Good everyone, i have an issue navigating with the simulation section environment during exams Az 500 can anyone put me through ?

upvoted 1 times

macco455 3 months, 2 weeks ago

Concept is right but the terminology changed on the page. Now you have to choose Customer managed keys instead of use your own

upvoted 2 times

https://t.me/learningnets

Question #43 *Topic 4*

You have a web app named WebApp1.
You create a web application firewall (WAF) policy named WAF1.
You need to protect WebApp1 by using WAF1.
What should you do first?

A. Deploy an Azure Front Door.

B. Add an extension to WebApp1.

C. Deploy Azure Firewall.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

kristiann21 Highly Voted 1 year, 1 month ago
Correct answer.

WAF is supported by Application Gateway and FrontDoor both.
upvoted 18 times

gboyega Highly Voted 1 year ago
Answer is CORRECT
upvoted 8 times

Exam_Master_Me Most Recent 12 months ago
Supported service
WAF can be deployed with Azure Application Gateway, Azure Front Door, and Azure Content Delivery Network (CDN) service from Microsoft.
WAF on Azure CDN is currently under public preview.

https://docs.microsoft.com/nl-nl/azure/web-application-firewall/overview
upvoted 5 times

https://t.me/learningnets

Question #44 *Topic 4*

You have an Azure subscription that contains an Azure SQL database named sql1.

You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:

- Support querying events by using the Kusto query language.
- Minimize administrative effort.

What should you configure?

A. an event hub

B. a storage account

C. a Log Analytics workspace

Correct Answer: *C*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

kumax 3 weeks, 3 days ago

On exam, May 2021.

upvoted 2 times

bmanu 1 month, 4 weeks ago

correct

upvoted 4 times

Topic 5 - Question Set 5

Question #1 *Topic 5*

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.

Correct 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

https://t.me/learningnets

Question #2 *Topic 5*

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

Correct 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

Jacquesvz 1 day, 13 hours ago
No other auth gives you control over password policies and user logon restrictions, I feel answer should be A: Yes
upvoted 1 times

https://t.me/learningnets

Question #3 *Topic 5*

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

Correct 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

Rume 1 week, 6 days ago
must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant .... This point to PTA

amount of necessary servers are reduced...Suggest to use PHS.

My vote would be B: NO.

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

However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead
upvoted 1 times

https://t.me/learningnets

Question #4 *Topic 5*

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

Correct 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

Question #5 *Topic 5*

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. B. 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.

Correct 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

https://t.me/learningnets

Question #6 *Topic 5*

You have been tasked with applying conditional access policies for your companyג€™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

Correct 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/

https://t.me/learningnets

Question #7 *Topic 5*

You have been tasked with applying conditional access policies for your companyλ€™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

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

thienvupt 1 week, 4 days ago
The same with Sign-ins from IP addresses with suspicious activity
so B is correct
upvoted 1 times

Ucy 1 week, 5 days ago
Correct Answer is B
IP addresses with suspicious/dubious activity risk level is LOW
upvoted 1 times

Deboe07 1 week, 6 days ago
Answer is incorrect. Per the referenced article sign-ins from suspicious (dubious) ip addresses is risk level low. Right answer is B
upvoted 1 times

https://t.me/learningnets

Question #8 *Topic 5*

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?

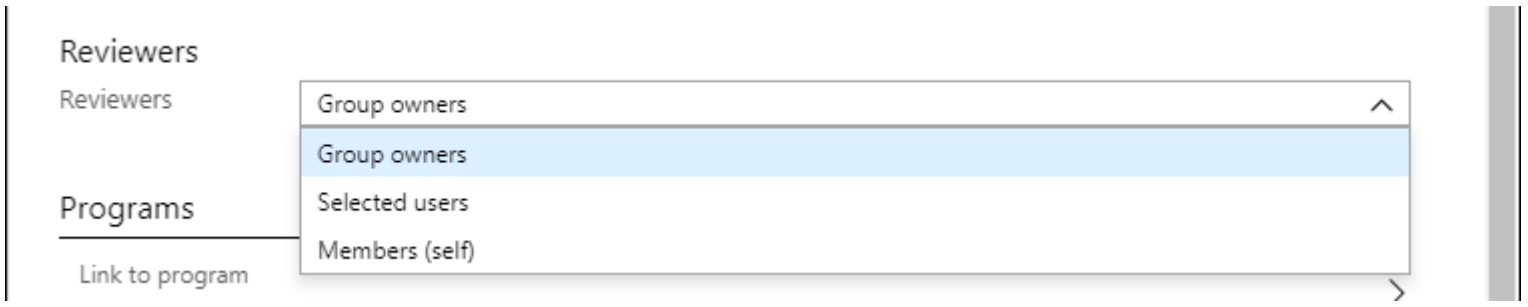
A. Selected users.

B. Members (Self).

C. Group Owners.

D. Anyone.

Correct 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

IRINI 1 week, 1 day ago
The reference shows the Answer is D
upvoted 2 times

Jacquesvz 1 day, 12 hours ago
The question states "You also have to make sure that the reviews can be reviewed by resource owners." so C = Group Owners, is the correct answer here.
upvoted 1 times

https://t.me/learningnets

Question #9 *Topic 5*

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.

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

Rume 2 weeks 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 1 times

https://t.me/learningnets

Question #10 *Topic 5*

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 companyλ€™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 λ€No adjustment requiredλ€ 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

Correct Answer: *A* B
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

Rume 2 weeks ago
B. Azure Blueprints
upvoted 3 times

ChinkSantana 1 week, 3 days ago
Yes Azure Blueprints
upvoted 1 times

Question #11 *Topic 5*

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

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

Rume 1 week, 6 days ago
given answer is correct
upvoted 2 times

https://t.me/learningnets

Question #12 *Topic 5*

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

Correct Answer: *A* D
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles
Topic 2, Implement platform protection

Lyonel 1 day, 10 hours 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

Madball 2 days, 19 hours ago
The correct answer is D, this has the least privileges in accordance with the following Microsoft article.

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli
upvoted 1 times

Vanht 4 days, 15 hours ago
The correct answer should be D
upvoted 1 times

nicejob 6 days, 20 hours ago
reader role has AcrPull and Access Resource Manager
upvoted 1 times

nicejob 6 days, 20 hours ago
Which of the following is the role you should assign?
AcrPull is permission not role.
upvoted 1 times

ChinkSantana 1 week, 3 days ago
If the question asked for Download Image then AcrPull
upvoted 2 times

Ucy 1 week, 5 days ago
Answer is Wrong....
Correct answer is D AcrPull
upvoted 3 times

Rume 2 weeks ago
ACR Pull?
upvoted 2 times

perkarelei 1 week, 5 days ago
ACR Pull seems the better option considering "least privileges":
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli#pull-image
upvoted 1 times

https://t.me/learningnets

Question #13 *Topic 5*

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 Companyג€™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

Correct Answer: *B*

Question #14 *Topic 5*

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 Companyג€™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

Correct Answer: *B*

https://t.me/learningnets

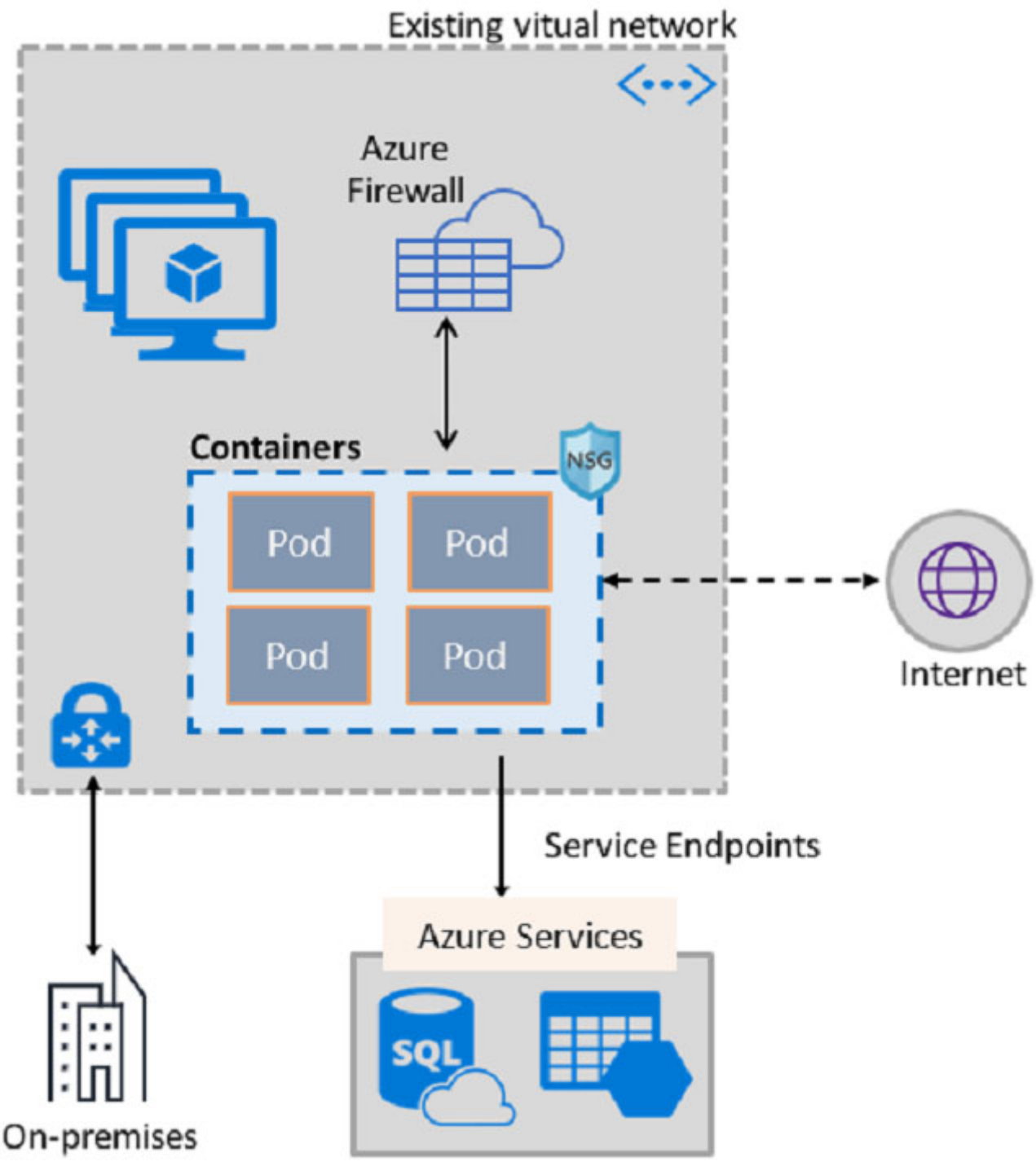
Question #15 *Topic 5*

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 Companyزâ€™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

Correct 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 doesnزâ€™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

https://t.me/learningnets

Question #16 *Topic 5*

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.

Correct 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

adsdadasdad 1 week, 2 days ago
answer is correct
upvoted 1 times

Rume 2 weeks ago
B is correct.
upvoted 2 times

Question #17 *Topic 5*

Your companyλ€™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

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

Rume 2 weeks ago
D is correct.
upvoted 2 times

https://t.me/learningnets

Question #18 *Topic 5*

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 a secret in Azure Key Vault.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

nicejob 6 days, 20 hours ago
When you create an AKS cluster in the Azure portal or using the az aks create command, Azure can automatically generate a service principal. In the following Azure CLI example, a service principal is not specified. In this scenario, the Azure CLI creates a service principal for the AKS cluster. To successfully complete the operation, your Azure account must have the proper rights to create a service principal.
Azure CLI

Copy
az aks create --name myAKSCluster --resource-group myResourceGroup
upvoted 1 times

Question #19 *Topic 5*

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 a conditional access policy.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

https://t.me/learningnets

Question #20 *Topic 5*

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

Correct 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

romaso82 5 days, 11 hours ago
correct answer
upvoted 1 times

https://t.me/learningnets

Question #21 *Topic 5*

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.

Correct Answer: *BC* BD
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

SajjadKarim 6 days, 23 hours 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

adsdadasdad 1 week, 2 days ago
No , its b and d. i tested c and i could not deploy a vm with the lock thats on the resource group. the correct answer is b and d
upvoted 1 times

sdahiya4 1 week, 5 days ago
Answers are correct
Read-Only lock on VM will not allow that to be powered on
Read only lock on Resource Group will allow virtual machine creation
upvoted 1 times

Rume 1 week, 6 days ago
i think the right answer is:
B. (Read only lock)and
D.(Read-Only lock on RG2)
upvoted 1 times

perkarelei 1 week, 5 days ago
From the reference link: "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."

Meaning resources can be added to the RG as long as they are not locked.
upvoted 1 times

https://t.me/learningnets

Question #22 *Topic 5*

You have been tasked with delegate administrative access to your companyλ€™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

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

Question #23 *Topic 5*

You have been tasked with delegate administrative access to your companyλ€™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

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

secisfun 5 days, 6 hours ago
correct
upvoted 1 times

https://t.me/learningnets

Question #24 *Topic 5*

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).

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

perkarelei 1 week, 5 days 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 1 times

Question #25 *Topic 5*

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.

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

https://t.me/learningnets

Question #26 *Topic 5*

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 ג€No adjustment requiredג€ 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

Correct 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
Topic 3, Manage security operations

Question #27 *Topic 5*

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

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

Rume 2 weeks ago
repeat question - however, answer is correct
upvoted 1 times

https://t.me/learningnets

Question #28 *Topic 5*

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

Correct Answer: *B*

Question #29 *Topic 5*

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

Correct Answer: *B*

Question #30 *Topic 5*

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

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

https://t.me/learningnets

Question #31 *Topic 5*

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.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

Rume 2 weeks ago
too many repeat questions -
Answer is correct.
upvoted 2 times

Question #32 *Topic 5*

You have been tasked with altering a current security playbook via Azure Security Center.
You want make sure that the playbook sends email messages to a distribution group, instead of a user.
Which of the following options should you use to achieve your goal?

A. Azure Blueprints

B. Activity Log

C. Azure Log Analytics

D. Azure Logic Apps Designer

Correct Answer: *D*
You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

Rume 1 week, 6 days ago
Given answer is correct.
upvoted 1 times

https://t.me/learningnets

Question #33 *Topic 5*

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.

Correct 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

Question #34 *Topic 5*

Your companyλ€™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.

Correct 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

https://t.me/learningnets

Question #35 *Topic 5*

Your companyλ€™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

Correct Answer: *C*
Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as λ€audit logsλ€ or
λ€operational logs,λ€ because they report control-plane events for your subscriptions.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

Question #36 *Topic 5*

Your companyλ€™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

Correct 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

https://t.me/learningnets

Question #37 *Topic 5*

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

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing
Topic 4, Secure data and applications

Question #38 *Topic 5*

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 companyλ€™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 usersλ€™ behalf.
Solution: You configure a delegated permission with admin consent.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

https://t.me/learningnets

Question #39 *Topic 5*

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 companyλ€™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 usersλ€™ behalf.
Solution: You configure a delegated permission with no admin consent.
Does the solution meet the goal?

A. Yes

B. No

Correct 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

Question #40 *Topic 5*

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 λ€No adjustment requiredλ€ 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

Correct 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

Rume 1 week, 6 days ago
given answer is correct. "No adjustment required"
upvoted 1 times

https://t.me/learningnets

Question #41 *Topic 5*

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

Correct 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

secisfun 5 days, 6 hours ago
answer is correct
upvoted 1 times

Rume 2 weeks ago
C- :DeployIfNotExist" - Correct anwer
upvoted 1 times

Question #42 *Topic 5*

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

Correct 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

Rume 2 weeks ago
repeted question - and the answers are correct
upvoted 2 times

https://t.me/learningnets

Question #43 *Topic 5*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company has an Azure subscription that includes an Azure key vault. You have previously created a secret in the key vault.
After an application developer registers an application in Azure Active Directory (Azure AD), you are instructed to make sure that the application is able to use the secret you created.
Solution: You should create a DLP policy.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

Question #44 *Topic 5*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company has an Azure subscription that includes an Azure key vault. You have previously created a secret in the key vault.
After an application developer registers an application in Azure Active Directory (Azure AD), you are instructed to make sure that the application is able to use the secret you created.
Solution: You should create a key in Azure Key Vault.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

Rume 1 week, 6 days ago
AZ Key Vault, already exist, why to create an additional one?
Answer is NO.
upvoted 1 times

https://t.me/learningnets

Question #45 *Topic 5*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Azure subscription that includes an Azure key vault. You have previously created a secret in the key vault.
After an application developer registers an application in Azure Active Directory (Azure AD), you are instructed to make sure that the application is able to use the secret you created.
Solution: You should create a role in Azure AD.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *Answer: <map><m x1="28" x2="317" y1="132" y2="223" ss="0" a="0" /><m x1="27" x2="319" y1="234" y2="316" ss="0" a="0" /> <m x1="27" x2="320" y1="324"*
Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them.
Managed identities for Azure resources overview make solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active
Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.
Example: How a system-assigned managed identity works with an Azure VM
After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Q46 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.

https://t.me/learningnets

Options	Answer
The column encryption key	
A DLP policy	
A shared access signature (SAS)	
A key vault access policy	
The column master key	

y2="406" ss="0" a="0" /><m x1="29" x2="320" y1="414" y2="500" ss="0" a="0" /><m x1="28" x2="320" y1="510" y2="597" ss="0" a="0" /><m x1="397" x2="740" y1="129" y2="220" ss="1" a="0" /><m x1="397" x2="740" y1="228" y2="312" ss="1" a="0" /><c start="0" stop="0" /><c start="4" stop="1" /></map>

Options	Answer
A DLP policy	The column encryption key
A shared access signature (SAS)	The column master key
A key vault access policy	

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

sheva370 1 week, 4 days ago

https://t.me/learningnets

Question #46 *Topic 5*

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?

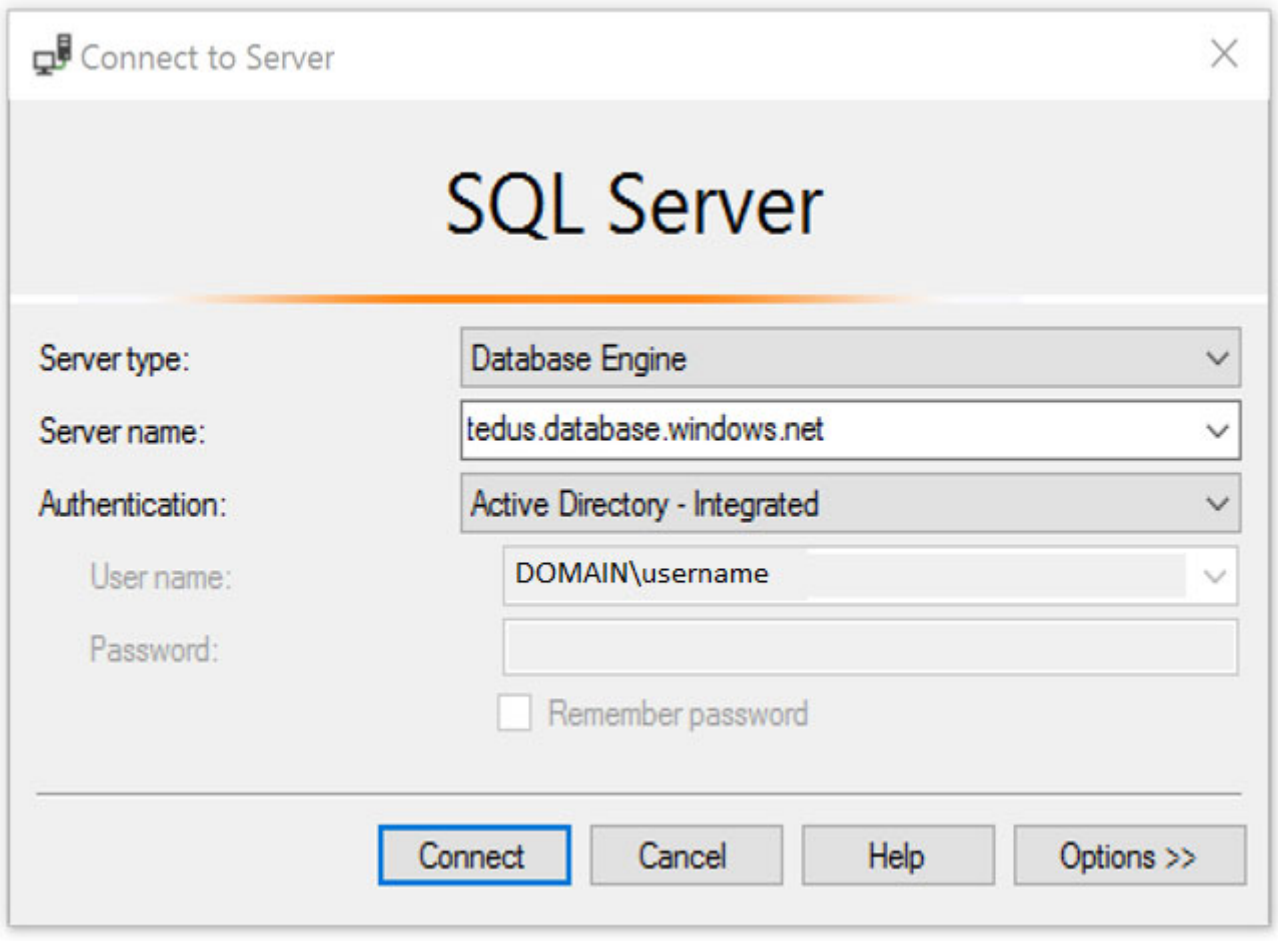
A. Azure AD token.

B. Azure Multi-Factor authentication.

C. Active Directory integrated authentication.

D. Active Directory integrated authentication.

Correct 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.



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 IDλ€ option is only supported for Universal with MFA connection options, otherwise it is greyed out.)
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md

Madball 2 days, 19 hours ago

https://t.me/learningnets

Both C and D are the correct answer, however, I suspect one of those is meant to have multi-factor authentication as an answer, but the correct answer is Active Directory Integrated Authentication.

upvoted 1 times

thienvupt 1 week, 2 days ago

C&D the same answer

upvoted 1 times

Question #47 *Topic 5*

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.

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

Rume 2 weeks 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 1 times

Question #48 *Topic 5*

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.

Correct 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

Topic 6 - Testlet 1

https://t.me/learningnets

Question #1 *Topic 6*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



The Azure subscription contains the objects shown in the following table.



Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.



Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersג€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication

https://t.me/learningnets

WebApp1 must enforce mutual authentication.

General Requirements -
Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.



Question

You need to meet the identity and access requirements for Group1.
What should you do?

A. Add a membership rule to Group1.

B. Delete Group1. Create a new group named Group1 that has a group type of Microsoft 365. Add users and devices to the group.

C. Modify the membership rule of Group1.

D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Correct Answer: *B*

Incorrect Answers:
A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.
D: For assigned group you can only add individual members.
Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal

Madball 2 days, 18 hours ago
Unable to answer these questions confidently because the pictures are missing.
upvoted 1 times

Rume 1 week, 6 days ago
All the previous comments have been removed. The correct answer is D.
https://www.examtopics.com/discussions/microsoft/view/6782-exam-az-500-topic-5-question-1-discussion/
upvoted 4 times

https://t.me/learningnets

Question #2 *Topic 6*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



The Azure subscription contains the objects shown in the following table.



Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.



Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersג€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

https://t.me/learningnets

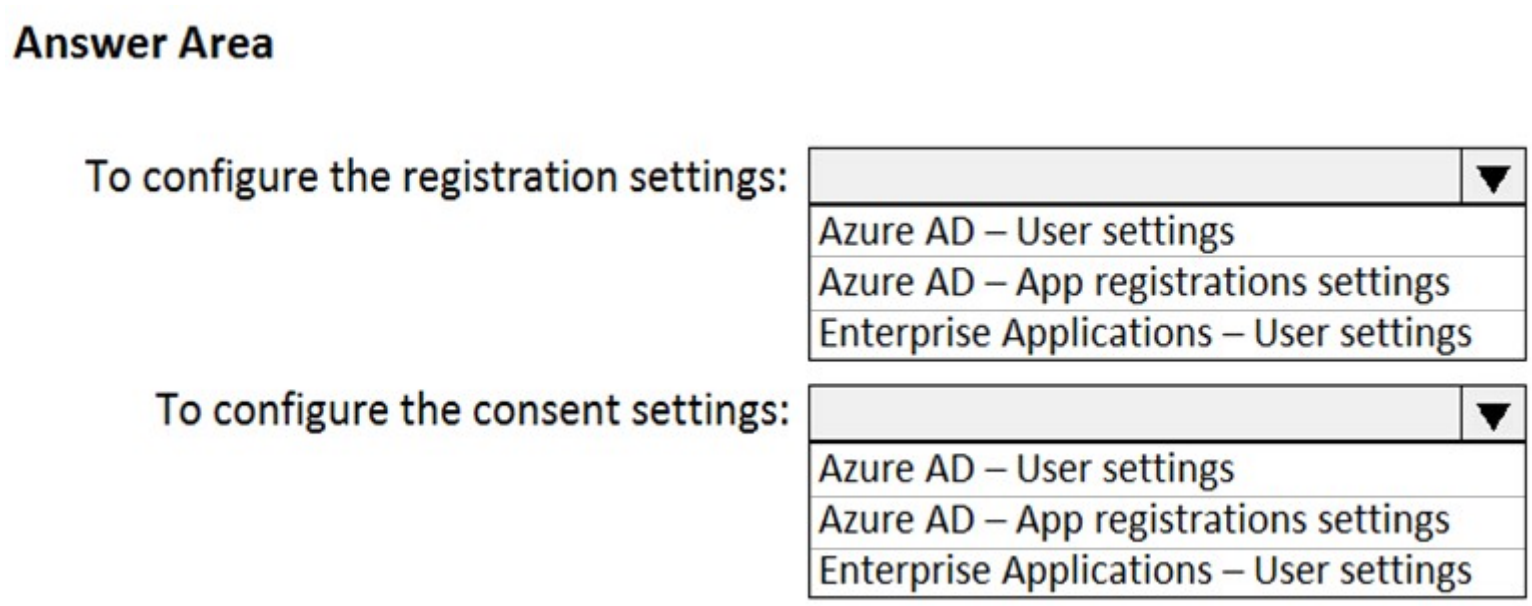
WebApp1 must enforce mutual authentication.

General Requirements -
Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

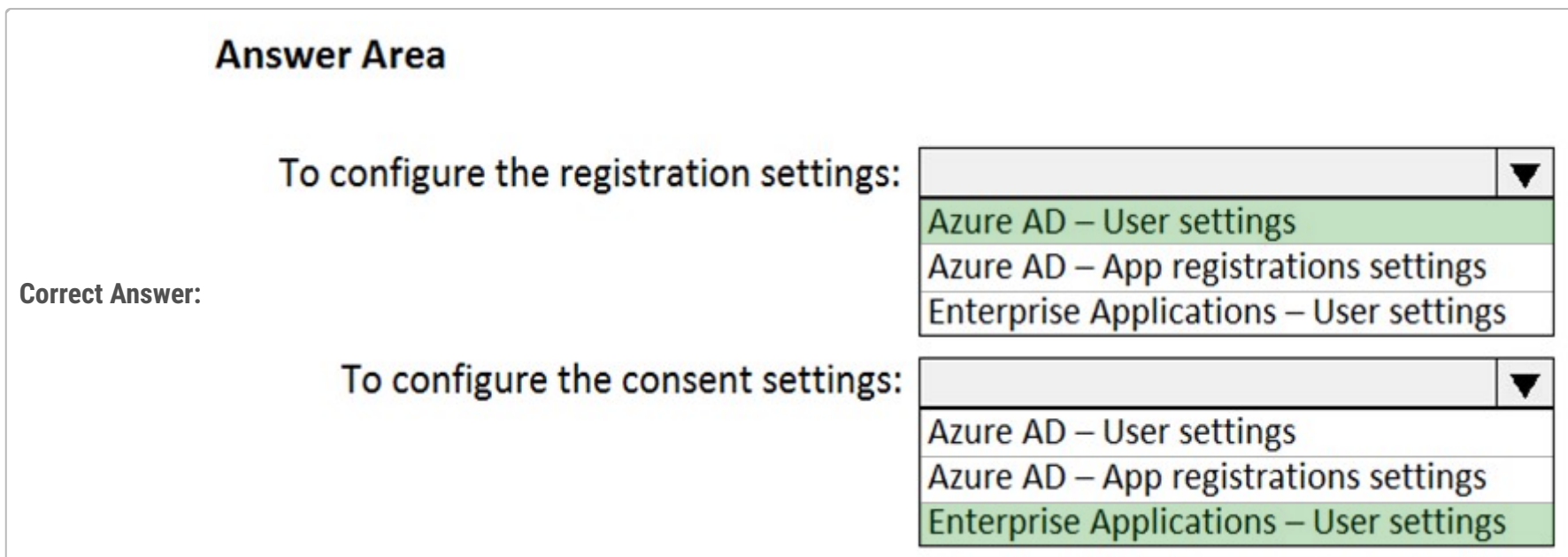


Question

HOTSPOT -
You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.
What should you use in the Azure portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

Jacquesvz 1 week, 1 day ago

Given answers are correct:
Box1:
Sign in to the Azure portal as a Global Administrator.
Select Users blade (either users blade directly or AD , then select users)> User Settings > App registrations.
Users can reigster aplications (yes/no)
Select Save to save your settings.

Box2:
Sign in to the Azure portal as a Global Administrator.
Select Azure Active Directory > Enterprise applications > Consent and permissions > User consent settings.
Under User consent for applications, select which consent setting you'd like to configure for all users.
Select Save to save your settings.

upvoted 2 times

https://t.me/learningnets

Topic 7 - Testlet 2

https://t.me/learningnets

Question #1 *Topic 7*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Question

You need to ensure that User2 can implement PIM.

What should you do first?

A. Assign User2 the Global administrator role.

B. Configure authentication methods for contoso.com.

C. Configure the identity secure score for contoso.com.

D. Enable multi-factor authentication (MFA) for User2.

Correct 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

kristiann21 Highly Voted 1 year, 1 month ago

Global Administration rights required.

I was thinking MFA, but then the question does not mention MFA, or MFA status it only mentions user 2 has Security Administrator Role. So obviously if User2 needs to implement PIM, PIM needs to be enabled, and it requires Global Administrator role.

upvoted 31 times

juselasmc Highly Voted 10 months ago

I think Correct Answer is A. This is is the Exam

upvoted 9 times

Ed2learn Most Recent 3 weeks, 3 days ago

Global Admin is the correct answer. Its not horribly clear but this article has the answer on how to deploy PIM. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

"Only owners of subscriptions and management groups can bring these resources under management by Privileged Identity Management. After it is under management, the PIM functionality is available for owners at all levels including management group, subscription, resource group, and resource. If you're a Global Administrator trying to deploy Privileged Identity Management for your Azure resources, you can elevate access to manage all Azure subscriptions to give yourself access to all Azure resources in the directory for discovery. "

upvoted 1 times

kumax 3 weeks, 3 days ago

On exam, May 2021.

This is a scenario that contains multiple (less than 5) questions.

upvoted 1 times

MarioMK 1 month, 3 weeks ago

answer is correct. When you are first configuring PIM you will need Global Admin rights within Microsoft Azure. The first user to enable and configure PIM will automatically be assigned the Privileged Role Administrators and Security Administrators role groups.

upvoted 1 times

macco455 3 months, 2 weeks ago

In order to activate PIM, you need to consent to PIM which requires a Global Admin to do so. Once you do so, it will automatically prompt you for MFA thus making the answer A.

upvoted 1 times

https://t.me/learningnets

teamaws 3 months, 2 weeks ago

Answer is A, Global Administrator required to implement PIM as user2 was Security Administrator

upvoted 2 times

sureshatt 4 months, 2 weeks ago

MFA is also required to do PIM, however there I have to assume Azure Security Defaults are activated by default (unless disabled manually), therefore MFA is there for all admin users. Then assigning the Global Administrator role allows the user to perform PIM tasks such as assignments.

upvoted 1 times

Thi 5 months, 1 week ago

Global Admin
https://practical365.com/azure-ad/getting-started-privileged-identity-management/#:~:text=When%20you%20are%20first%20configuring,to%20consent%20to%20use%20it.

upvoted 1 times

Stuudent 7 months, 3 weeks ago

This seems off to me:

First:
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
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

Secondly:
Sign in to the Azure portal with a user who is in the Privileged role administrator role.
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?tabs=new

So no Global Administrator Role seems necessary?

upvoted 4 times

3abmula 1 month, 2 weeks ago

But none of the other answers make any sense also.

upvoted 1 times

deegadaze1 5 months, 3 weeks ago

Supported, I don't see any reason why this answer should be A...

upvoted 1 times

kristiann21 1 year, 1 month ago

In the exam, would it be possible to go back to the case study information after viewing the question?

upvoted 1 times

jd1 1 year ago

Yes, you can see the case study information and question at the same time. I usually read the question/questions before I even look at the case study, since questions like these don't even require the case study saves time.

upvoted 16 times

Topic 8 - Testlet 3

https://t.me/learningnets

Question #1 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Identity and Access Requirements

Azure Security Center is set to the Standard tier.

Requirements -

https://t.me/learningnets

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersג€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

Question

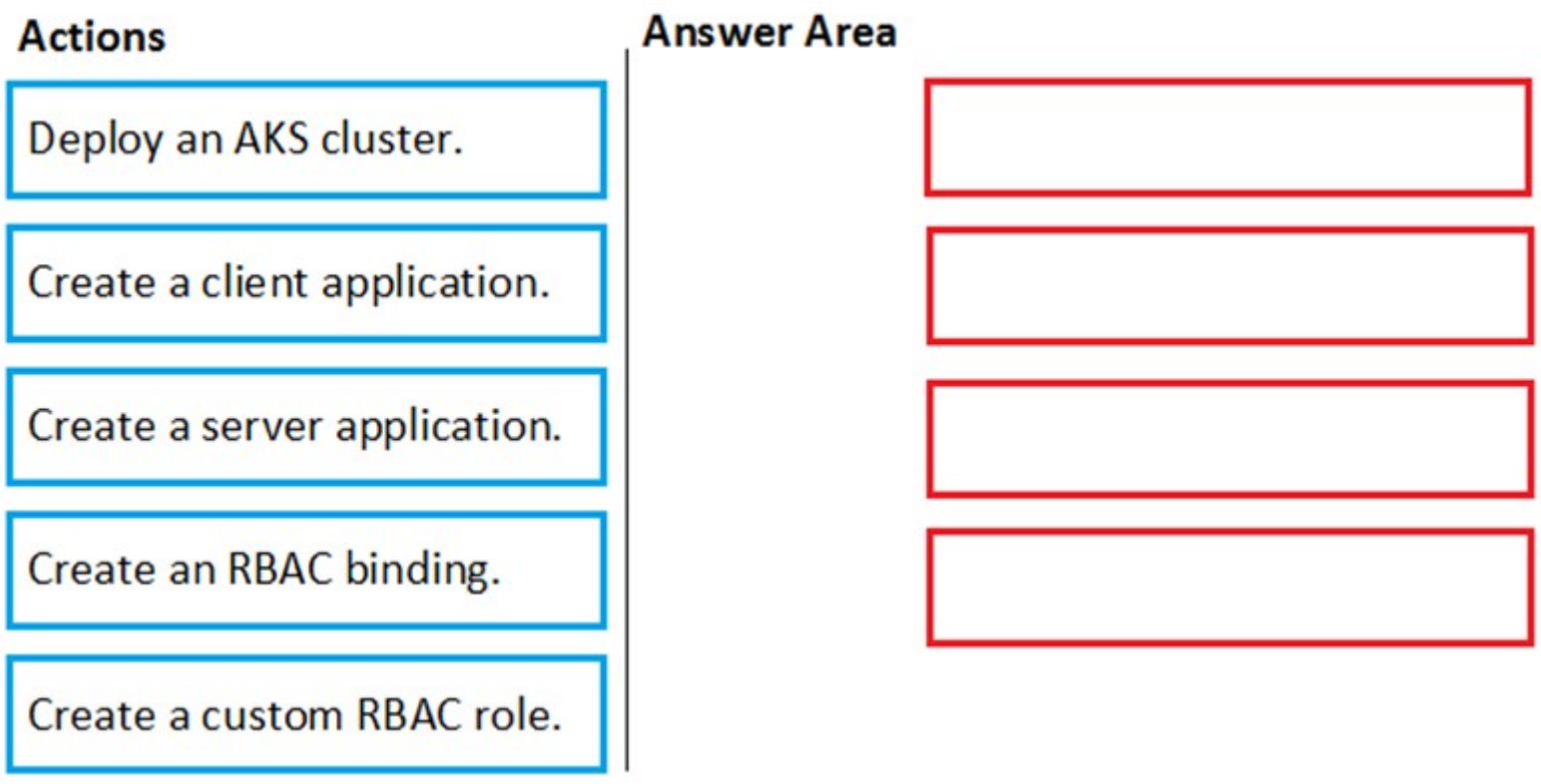
DRAG DROP -

You need to deploy AKS1 to meet the platform protection requirements.

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

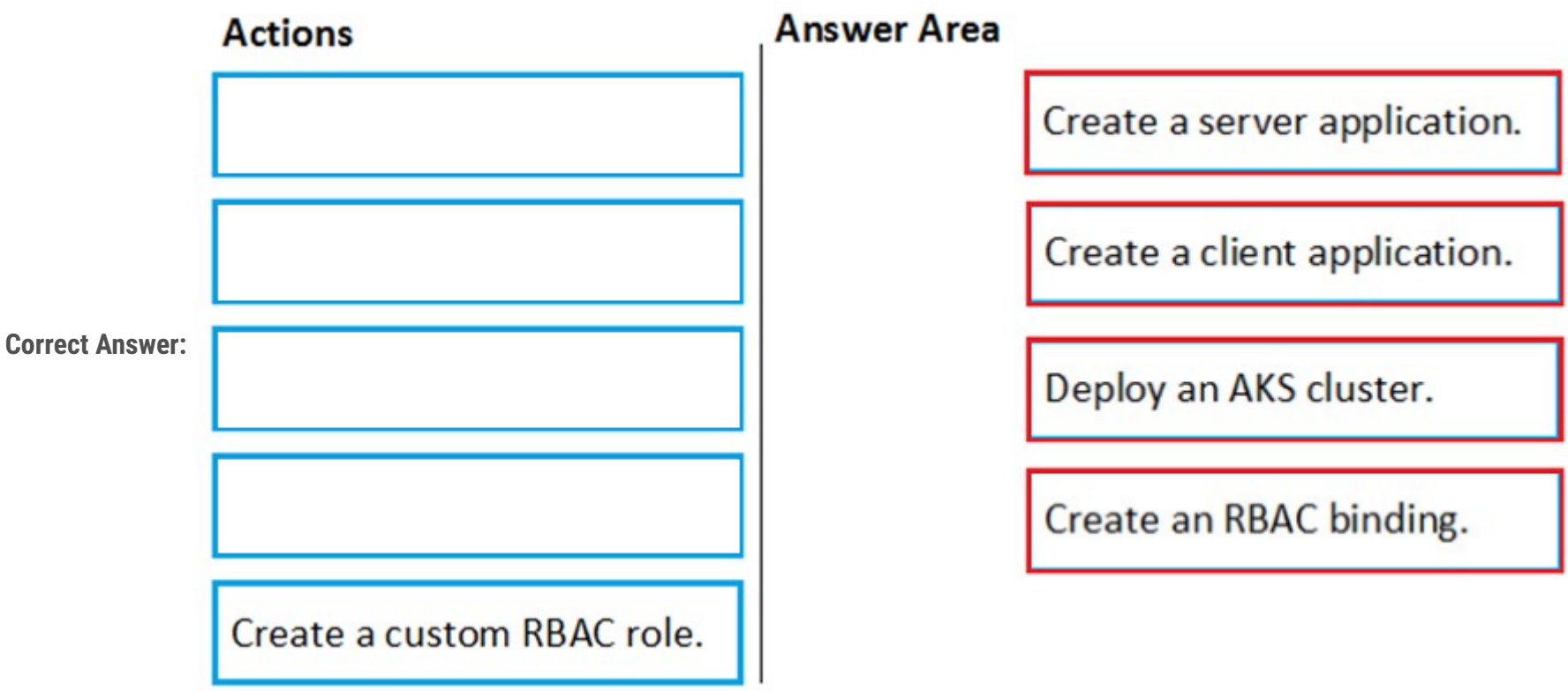
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:



https://t.me/learningnets

Correct Answer:



Scenario: Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Litware plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.

Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.

Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster.

Use the az aks create command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.

Reference:

https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

dadageer Highly Voted 4 months ago

Correct answer
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

upvoted 8 times

kumax Most Recent 3 weeks, 3 days ago

On exam, May 2021.
This is a scenario that contains multiple (less than 5) questions.

upvoted 1 times

bmanu 1 month, 3 weeks ago

seems like an outdated question "AKS has a new improved AKS-managed Azure AD experience that doesn't require you to manage server or client application. If you want to migrate follow the instructions here." https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

upvoted 2 times

sureshatt 3 months, 2 weeks ago

Current AKS version has AAD integration out of the box, hence it is no longer required to configure the AAD server and client apps.

upvoted 3 times

https://t.me/learningnets

https://t.me/learningnets

Question #2 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Identity and Access Requirements

Azure Security Center is set to the Standard tier.

Requirements -

https://t.me/learningnets

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersλ€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

Question

You need to ensure that users can access VM0. The solution must meet the platform protection requirements.

What should you do?

A. Move VM0 to Subnet1.

B. On Firewall, configure a network traffic filtering rule.

C. Assign RT1 to AzureFirewallSubnet.

D. On Firewall, configure a DNAT rule.

Correct Answer: *A*

Azure Firewall has the following known issue:

Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.

If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesnλ€™t work.

This is a result of asymmetric routing λ€" a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.

Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesnλ€™t have a user-defined route to the firewall.

Scenario:

VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

https://t.me/learningnets

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.

References:

https://docs.microsoft.com/en-us/azure/firewall/overview

dadageer Highly Voted 4 months ago

Not sure if this question is still valid as it is no longer an issues with JIT/FW:
https://azure.microsoft.com/en-us/updates/just-in-time-access-now-supports-azure-firewall/

upvoted 5 times

dadageer 4 months ago

it use to be a manual creation of DNAT rule but now JIT will create it for you!

upvoted 3 times

Fitama Most Recent 1 day, 16 hours ago

So what is the correct one? I think that it is the B. Why VM0 it has to be change to Subnet1? I don´t understand. Thanks

upvoted 1 times

https://t.me/learningnets

Question #3 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Identity and Access Requirements

Azure Security Center is set to the Standard tier.

Requirements -

https://t.me/learningnets

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersג€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

Question

HOTSPOT -

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

Create a custom policy definition that has effect set to: [▼]

- Append
- Deny
- DeployIfNotExists

Create a policy assignment and modify: [▼]

- The Create a Managed Identity setting
- The exclusion settings
- The scope

https://t.me/learningnets

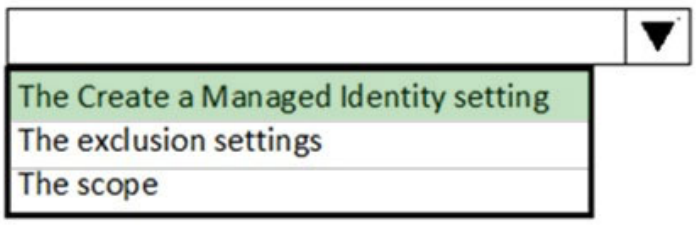
Correct Answer:

Answer Area

Create a custom policy definition that has effect set to:



Create a policy assignment and modify:



Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.
RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists -
DeployIfNotExists executes a template deployment when the condition is met.
Azure policy definition Antimalware
Incorrect Answers:
Append:
Append is used to add additional fields to the requested resource during creation or update. A common example is adding tags on resources such as costCenter or specifying allowed IPs for a storage resource.
Deny:
Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
Box 2: The Create a Managed Identity setting
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

benito_nepomuceno Highly Voted 4 months ago
BOX 2 is SCOPE
upvoted 12 times

thienvupt Most Recent 1 week, 3 days ago
Correct,
Box 2: The Create a Managed Identity setting
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.
upvoted 1 times

kumax 3 weeks, 3 days ago
On exam, May 2021.
This is a scenario that contains multiple (less than 5) questions.
upvoted 2 times

alexk0 1 month, 3 weeks ago
For me box2 is Scope.
When you're assigning the create policy, the first row of the first screen asks you about scope. Also, the "Create Manages Identity" checkbox is checked by default for DeployIfNotExists.
upvoted 1 times

vijeet 2 months, 3 weeks ago
doesn't DeployIfNotExists require a managed identity.
I understand the scope is important but following the order what comes first?
1. DeployIfNotExists
2. Managed Identity
3. Scope
upvoted 3 times

dadageer 4 months ago
Box 2 scope as generally it will be applied on Sub but you need to change it to RG as per requirements
upvoted 3 times

https://t.me/learningnets

Topic 9 - Testlet 4

https://t.me/learningnets

Question #1 *Topic 9*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

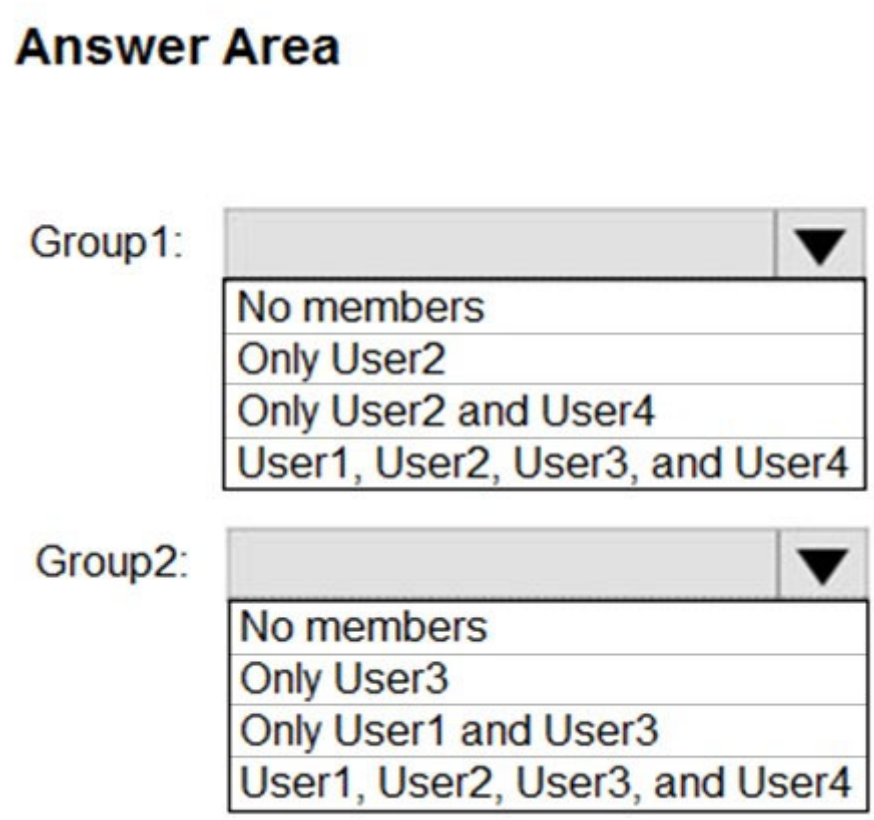
Question

HOTSPOT -

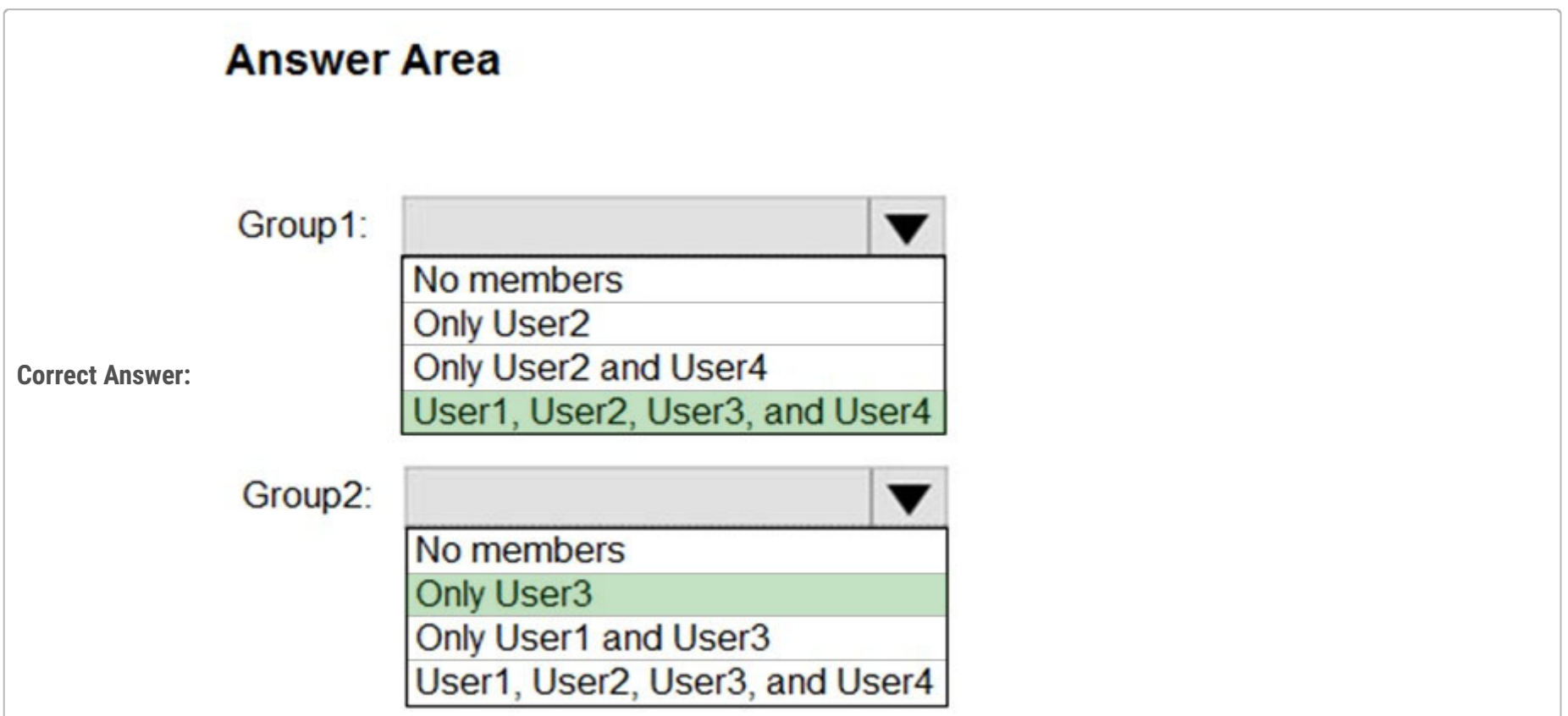
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: User1, User2, User3, User4

Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3 -

Match "*on" is only true for London (User3) as ג€˜Londonג€™ is the only word that ends with ג€˜onג€™.

Scenario:

https://t.me/learningnets

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city –contains "ON"`
Group2	Dynamic user	`user.city –match "*on"`

References:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

AdnanEzzi Highly Voted 1 year, 2 months ago

The answer is correct. Group 1 - U1, U2, U3 & U4 AND for Group 2 - U3.

upvoted 29 times

AS007 Highly Voted 1 year, 2 months ago

Given answers are correct - reason "the rules are different, one says match and other says contain"

upvoted 11 times

kumax Most Recent 3 weeks, 3 days ago

On exam, May 2021.
This is a scenario that contains multiple (less than 5) questions.

upvoted 2 times

justinp 3 weeks, 1 day ago

this question still avaliable in exam?

upvoted 1 times

CASGTI 2 months, 2 weeks ago

Tested in lab..
>>> -match "*on" >>> is an incorrect expression, it will not allow you to save the this, so the group will not contain any members.
... valid expression could be ".*on" (with a dot in front) ... so make sure in exam you see the dot, if no dot ... then, no members.

upvoted 7 times

dorinh 2 months ago

you're right, the syntacx is evaluated only on this format (user.displayName -match ".*as")

upvoted 1 times

vijeet 2 months, 3 weeks ago

this is from MS Docs
Using the -match operator
The -match operator is used for matching any regular expression. Examples:

user.displayName -match "Da.*"
Da, Dav, David evaluate to true, aDa evaluates to false.

user.displayName -match ".*vid"
David evaluates to true, Da evaluates to false.

upvoted 2 times

TJO 3 months, 2 weeks ago

Took the test today and the membership rule for Group2 IS listed at shown in this sample question: user.city -match "*on"
Not sure if their typo is by design, so up to you on how you treat this question should it come up on your test.

upvoted 2 times

hang10z 4 months, 1 week ago

The answer is
1: User1-4
2: No users, you cannot even create a group with user.city - match "*on" it fails. That is an invalid expression

upvoted 4 times

dadageer 4 months, 1 week ago

No idea what are these Powershell comments about? answer is right!

upvoted 1 times

Narragr 4 months, 1 week ago

user.city -match "*on" will have 0 member since the syntax is wrong. The correct syntax would be user.city -match ".*on", in this case London would have been the only solution

https://t.me/learningnets

upvoted 2 times

milind8451 4 months, 3 weeks ago

Right answer, people testing in powershell, this is for "Dynamic Group".

upvoted 1 times

AshTac 5 months, 3 weeks ago

For group 2, if we are getting invalid syntax (I also go the same in my test), shouldn't the answer be no members?

upvoted 2 times

inf 5 months, 3 weeks ago

Answer:
BOX 1: User1, User2, User3, User4
BOX 2: User1, User2, User3, User4

Azure Dynamic Group (validation testing)
4 x Users: Admin01, Admin02, User01, User02
(Green tick = member, Red cross = not member)

BOX 1: TEST 1: 4 x Matches
Validate Rules (Preview)
- City Contains ON
(user.city -contains "ON")

User: Admin01
- (user.city -contains "ON")
- user.city -contains "ON" [city = "LONDON"]
- Green Tick!
User: Admin02
- (user.city -contains "ON")
- user.city -contains "ON" [city = "MONTREAL"]
- Green Tick!
User: User01
- (user.city -contains "ON")
- user.city -contains "ON" [city = "London"]
- Green Tick!
User: User02
- (user.city -contains "ON")
- user.city -contains "ON" [city = "Montreal"]
- Green Tick!

upvoted 4 times

inf 5 months, 3 weeks ago

BOX 2: TEST 2: 4 x Matches
Validate Rules (Preview)
- City Match *on
(failed - irregular expression - i.e. does not work)

- City Match .*on
(improvised, assume .*on, rather than *on)
(.* is an arbitrary string of any length)
(-match .*on is similar to -contains on)
(.*on search term can exist anywhere in the string)
(.*on$ would return London users only, that is $ looks at the End of the String)

(user.city -match ".*on")

User: Admin01
- (user.city -match ".*on")
- user.city -match ".*on" [city = "LONDON"]
- Green Tick!
User: Admin02
- (user.city -match ".*on")
- user.city -match ".*on" [city = "MONTREAL"]
- Green Tick!
User: User01
- (user.city -match ".*on")
- user.city -match ".*on" [city = "London"]
- Green Tick!
User: User02
- (user.city -match ".*on")
- user.city -match ".*on" [city = "Montreal"]
- Green Tick!

upvoted 7 times

sheva370 1 month ago

Correct answer!

upvoted 1 times

zic04 5 months, 3 weeks ago

https://t.me/learningnets

I just tested, 1234 for 1 and 2 but the syntax for the second incorrect (user.city -match ".*on")
if we have the question during a test we have to report it

upvoted 1 times

stag 7 months, 1 week ago

Contains "ON" Capital letter User 2 and match with "*on" any word does not matter start with"*" and match "on" .User 1-2-3-4

upvoted 1 times

upstirs 7 months ago

if it is not case sensitive then all Group1 and 2 is 1-2-3-4

upvoted 1 times

ufuomaolori 6 months, 3 weeks ago

It is case sensitive, I have tried out in my lab. "ON" is not the same as "on"

upvoted 2 times

B1T3X 6 months ago

It's not case sensitive. I tested.

upvoted 1 times

lvd 5 months, 3 weeks ago

the documentation says it is NOT case sensitive: String and regex operations are not case sensitive
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

upvoted 2 times

awssecuritynewbie 8 months ago

in the exam guys and i believe it should be removed but they would not listen i have already complained about this.

upvoted 1 times

Totalvibe 8 months, 3 weeks ago

Definitely answers are correct...it's a matter of the dynamic management rule and regex conditions.

upvoted 2 times

awssecuritynewbie 9 months, 1 week ago

I first didn't agree but now looking at the documentation i can see that the values are not " String and regex operations are not case sensitive."

so it would be the correct answer

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

upvoted 1 times

awssecuritynewbie 9 months, 1 week ago

look at the given aswer it says " "~London' is the only word that ends with "~on'."
but it is a * not a ~ so how is that even the correct explanation ...confused

upvoted 2 times

Thi 5 months, 1 week ago

Thanks for explanation...I got point now

upvoted 1 times

https://t.me/learningnets

https://t.me/learningnets

Question #2 *Topic 9*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city –contains "ON"`
Group2	Dynamic user	`user.city –match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Question

HOTSPOT -

You are evaluating the security of the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the private IP address of VM5.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the private IP address of VM5.	○	○

Box 1: Yes. All traffic is allowed out to the Internet so you can ping the public IP.

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes. VM3 is on Subnet12. There is no NSG attached to Subnet12 so the traffic will be allowed by default.

https://t.me/learningnets

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

Box 3: No (because VM5 is in a separate VNet).

Note: Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

nihao381 Highly Voted 3 months, 3 weeks ago

1 -- No, as traffic would be sourced from internet since it is destined to the public IP address of VM2.
2 -- Yes, as VM3 has no NSGs interfering and traffic is contained within the same vnet.
3 -- No, as VM5 is in a separate vnet and there is no mention of any peering going on.

upvoted 21 times

benito_nepomuceno Highly Voted 4 months ago

1. [No] because VM1 is trying to reach VM2 with VM2's PUBLIC IP address which should be blocked by NSG1.
2. [Yes] because VM1 and VM3 are in the same VNET and you can reach each other with the private IP address.
3. [Yes] VM5 has NSG4 which allows internet traffic. VM1 can reach VM5 through internet using the public IP.

upvoted 7 times

ChinkSantana 1 week, 5 days ago

Question asked for Privet IP..and not Public IP of VM5

upvoted 1 times

longtech 1 month, 2 weeks ago

The ping to the private ip address of VM5 is No . Because, VM5 do not have application security group, it only true if VM5 configure that.

upvoted 2 times

milad123 3 months, 3 weeks ago

For question 1: i think that the traffic will be filtred by NSG2 (not NSG1 as you said) because as we ping the public IP address of VM2, it's related to subnet 11 --> NSG2

upvoted 1 times

NoMeHo 3 months, 4 weeks ago

3. it states private IP, not public IP. Plus, VM5 is on a different network. 3 is No IMO.

upvoted 5 times

Pinto 3 months, 3 weeks ago

good observation. The question does not tell anything about peering and routing between the 2 vnets. So, No for sure for 3rd box.

upvoted 1 times

Deepmindx Most Recent 2 weeks, 1 day ago

IN EXAM ### 29/6/2021

upvoted 2 times

kumax 3 weeks, 3 days ago

https://t.me/learningnets

On exam, May 2021.
This is a scenario that contains multiple (less than 5) questions.
upvoted 2 times

MarioMK 1 month, 1 week ago
My point of view:
N: The NSG1 i.e. the NSG for the VM2 will block this.
Y: They are on the same Vnet, so this traffic is allowed as VM3 does not have an NSG associated with it.
N: No because in order to be able to ping the private IPs, the Vnets must be peered which is not the case here.
upvoted 2 times

Andreu 2 months, 1 week ago
I think answer should be NO, YES, NO.
For question 1, VM2 has 2 NSGs associated, one for the subnet (NSG2) and one for the NIC (NSG1)

As referenced in https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works, inbound traffic will first be filtered by the NSG associated to the subnet.

So, traffic will be filtered by NSG2, which allows source from the Internet but only if it's protocol TCP. As a ping would be ICMP, it is not allowed, and the last rule of NSG2 denies and drops the packet.

So, VM1 cannot ping VM2 through its public address.
upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago
Given Answers YES, YES and NO are correct.

Looked at it again - don't forget Any. Any to Internet is allowed, so VM1 to public VM2 would be allowed

VM1 to VM3 are both on the same vnet so allowed VM1 to private ip VM3

VM5 is different vnet and no nsg so can't private can't be reach. public could be reached
upvoted 3 times

Cyberbug2021 2 months, 2 weeks ago
In NSG2 (Q1) icmp is not allowed only port 80 is allowed, so vm1 trying to reach public ip of vm2 via icmp will not work
upvoted 1 times

vijeet 2 months, 3 weeks ago
1. NO: Because for incoming even if SUBNET-NSG allows traffic but NIC-NSG denies, the traffic will be denied.
2. YES
3. NO, because no VNET PEERING
upvoted 1 times

JAGUDERO 3 months ago
1 - No, Ping is not internet traffic which is only thing allowed by rule
2 - Yes, VMs are in same VNET
3 - By default, it is not allowed to "ping" cloud services
https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-connectivity-and-networking-faq#can-i-ping-a-cloud-service
upvoted 2 times

macco455 3 months, 2 weeks ago
NO, Ping is not internet traffic which is only thing allowed by rule
Yes, VMs are in same VNET
No, Different VNETS and no peering
upvoted 3 times

Sethoo 3 months, 4 weeks ago
I will go with the given answers
upvoted 1 times

https://t.me/learningnets

Question #3 *Topic 9*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city –contains "ON"`
Group2	Dynamic user	`user.city –match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Question

HOTSPOT -

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer area

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	○	○
From VM2, you can successfully ping the private IP address of VM4.	○	○
From VM1, you can connect to the web server on VM4.	○	○

Correct Answer:

Answer area

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	○	○
From VM2, you can successfully ping the private IP address of VM4.	○	○
From VM1, you can connect to the web server on VM4.	○	○

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.

VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or

TCP 443.

barchetta Highly Voted 1 year, 5 months ago

q1: dont forget ping is not tcp.. I know better but forgot.

https://t.me/learningnets

upvoted 33 times

Stuudent 7 months, 2 weeks ago

Well excuse me...:
Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of corresponding echo Reply messages are displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.

and

This command is available only if the Internet Protocol (TCP/IP) is installed as a component in the properties of a network adapter in Network Connections.

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping

sounds to me like icmp is operating within TCP and therefore the answer to Q1 should be YES in my opinion.

upvoted 2 times

ckochhar 5 months, 2 weeks ago

No ICMP itself is a protocol just like TCP, UDP. Dont confuse them with ports, hence it does not fall under TCP.

upvoted 4 times

gills 7 months, 2 weeks ago

ICMP is a network-layer protocol. There is no TCP or UDP port number associated with ICMP packets as these numbers are associated with the transport layer above. So comparing to HTTP, which has a port 80 or 443 , there for the underlying protocol tcp is mapped to that protocol as well. ICMP is different.

SS

upvoted 4 times

swip 1 year, 2 months ago

lol, I was about to kick off, until I read your comment. Face palmed myself and thought I'm an idiot, I also know better

upvoted 4 times

ccarlton Highly Voted 1 year ago

lol.. ping is not tcp. I also forgot. ;)

upvoted 9 times

longtech Most Recent 1 month, 2 weeks ago

The answer is totally right. As we can see that, NSG 3 just only allow asg1 with connection is TCP, in here we connect to by using UDP, so that is fails.

upvoted 1 times

souvik123 2 months ago

NO - Yes - Yes
Logic is VM4 has Subnet 13 which is associated with NSG 3. The rules on NSG3 allow Ping traffic (any) from ASG 2. The ASG 2 is associated for VM2 and hence only VM2 can ping VM4. Similarly Web traffic allowed from ASG1 on NSG3. ASG1 associated with VM1 & VM4 , hence only these can reach via web traffic to VM4.

upvoted 1 times

Cyberbug2021 2 months, 2 weeks ago

NO, YES and YES - you may have to spend some time on it but if you do it right - given answer is correct

upvoted 2 times

Fred64 4 months, 1 week ago

don't understand where some find VM3 in their answer.
The questions are about VM1, VM2 and VM4

upvoted 1 times

asdf12345a 4 months, 2 weeks ago

Answer is correct - No, Yes, Yes.

You cannot ping the private address of VM4. VM4 is in ASG1 connected to Subnet13 that is associated with NSG3. NSG3 allows only allows TCP from ASG1 and ICMP is not TCP, therefore the answer is no.

From VM2, you can ping the private IP address of VM4 as NSG3 allows inbound connections on any protocol from ASG2.

From VM1, you can connect to the web server on VM4 as NSG3 allows all TCP connections from ASG1 to ASG1, and both VM1 and VM4 are in ASG1.

upvoted 4 times

an0ny 5 months, 1 week ago

Ping uses ICMP protocol, a network-layer protocol. It is neither TCP nor UDP. So, for the first one, YES.

upvoted 1 times

Danish12 7 months ago

Given answer is absolutely correct!

upvoted 6 times

https://t.me/learningnets

CloudyTexas 7 months, 1 week ago

Box1: No. NSG3 only allows TCP traffic, TCP is not ICMP ping.
Box2: No. NSG3 only allows TCP traffic, TCP is not ICMP ping.
Box3: Yes. NSG3 allows TCP PORT 80 inbound traffic.

upvoted 1 times

B1T3X 6 months ago

Box 2 is yes since VM2 is in ASG2, therefore it answers to the rule with priority 150.

upvoted 1 times

DA0410 7 months, 2 weeks ago

Examtopics makes you brain churn and so help keep me young. Keep it up. And request to experts , which is correct answer?

upvoted 3 times

B1T3X 6 months ago

Given answer is correct.

upvoted 1 times

realname007 8 months ago

so what is the correct answer for this?

upvoted 1 times

B1T3X 6 months ago

Given answer is correct.

upvoted 1 times

DeepMoon 9 months, 1 week ago

VM1 is in Subnet 11 has NSG1 attached. Pings go through to the internet.
VM4 is in Subnet13 which has NSG3 attached to it. Inbound pings are denied.
• VM1 & VM4 are labeled as ASG1.
• NSG3 only allows TCP not ICMP for ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1.

Box 2: Yes.
VM2 is subnet 11. NSG1 allows pings out.
VM4 has a NSG3 setup. It allows any protocol from ASG2 into subnet 13(where VM4 is) so ICMP ping would be allowed.
VM2 is in ASG2 so pings from it are allowed through NSG3.

Box 2: Yes.
VM2 is subnet 11. NSG1 allows pings out.
VM4 has a NSG3 setup. It allows any protocol from ASG2 into subnet 13(where VM4 is) so ICMP ping would be allowed.
VM2 is in ASG2 so pings from it are allowed through NSG3.

Box3. Yes.
VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

upvoted 1 times

paulxyz90 6 months, 1 week ago

I was wondering though - (for #3) what if VM1 routes over its public interface to get to VM4's web server. In that case there is no inbound rule for INTERNET sourced traffic on NSG3 (which is tied to VM4 - there is an any:any DENY. If we assume it's internal then it's YES.

upvoted 1 times

kiketxu 7 months, 3 weeks ago

You miss clarify the box 1. Which is NO

upvoted 1 times

kiketxu 9 months, 3 weeks ago

Dont' forget TCP is not ICMP (protocol for ping)
NO
YES
YES

upvoted 3 times

awssecuritynewbie 9 months, 1 week ago

how is the last one is correct it is source ASG1 and distanation ASGS1 .. it is only allowing to it self.

upvoted 1 times

kiketxu 7 months, 3 weeks ago

VM4 is part of ASGS1. So, Any TCP is allowed.

upvoted 2 times

Armando997 10 months ago

Given answers are correct

upvoted 1 times

Kampo 10 months ago

https://t.me/learningnets

NO - TCP traffic doesnt allow ICMP. Hence from VM1 you cant ping VM4
YES - All traffic allowed from ASG2 to NSG3
YES - Port 80 allowed from ASG1

upvoted 5 times

publicuser55 11 months, 1 week ago

Box1: No. NSG3 only allows TCP traffic, TCP is not ICMP ping.
Box2: No. NSG3 only allows TCP traffic, TCP is not ICMP ping.
Box3: Yes. NSG4 allows all inbound traffic.

upvoted 7 times

yaling 6 months, 2 weeks ago

Don't forget for Box2, Vm2 belongs to ASG2, which matches the second rule of NSG3. So it should be YES.

upvoted 5 times

https://t.me/learningnets

Question #4 *Topic 9*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Question

You need to meet the technical requirements for VNetwork1.

What should you do first?

A. Create a new subnet on VNetwork1.

B. Remove the NSGs from Subnet11 and Subnet13.

C. Associate an NSG to Subnet12.

D. Configure DDoS protection for VNetwork1.

Correct Answer: *A*

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet.

References:

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

kristiann21 Highly Voted 1 year, 1 month ago

Indeed. VNet1 has not subnet for AzureFirewall. Create a new subnet for AzureFirewall named as exactly as AzureFirewallSubnet.

upvoted 22 times

gfhbox0083 Highly Voted 1 year ago

A, for sure.

upvoted 15 times

kiketxu Most Recent 9 months, 3 weeks ago

right!

upvoted 10 times

https://t.me/learningnets

Question #5 *Topic 9*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Question

HOTSPOT -

You are evaluating the security of VM1, VM2, and VM3 in Sub2.

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
From the Internet, you can connect to the web server on VM1 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM2 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM3 by using HTTP.	○	○

Correct Answer:

Answer area

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM2 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM3 by using HTTP.	○	○

VM1: Yes. NSG2 applies to VM1 and this allows inbound traffic on port 80.

VM2: No. NSG2 and NSG1 apply to VM2. NSG2 allows the inbound traffic on port 80 but NSG1 does not allow it.

VM3: Yes. There are no NSGs applying to VM3 so all ports will be open.

dadageer Highly Voted 4 months ago

Answers correct! Y, N, Y

upvoted 8 times

besha Most Recent 2 weeks, 3 days ago

I think it should be No, No, Yes
The first one should No, becuase it is openning HTTP from ANY but only to the VirtualNetwork. From internet you can only access the public IP which is not part of the Virtual network

upvoted 1 times

Rume 3 weeks, 5 days ago

Given answer is correct.

upvoted 1 times

MarioMK 1 month, 1 week ago

https://t.me/learningnets

I think the answer should be YNN: the first two answers are correct, but the third one is wrong from my point of view. I think it is wrong becase since there is no NSG defined for VM3, the default inbound rule will apply. In this case the incoming internet traffic is blocked.

upvoted 2 times

3abmula 1 month, 1 week ago

If there is no NSG, then there are no default inbound rules, everything is allowed. Those default rules you see in Networking section on VM are coming from NSG.

upvoted 1 times

souvik123 2 months ago

Correct Answers and Explanation : Yes, No, Yes

upvoted 1 times

macco455 3 months, 2 weeks ago

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works
For anyone who doesn't understand how multiple NSGs work. This explains it perfect
Answers are correct

upvoted 4 times

Topic 10 - Testlet 5

https://t.me/learningnets

Question #1 *Topic 10*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Question

HOTSPOT -

You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs? You must be able to connect virtual machines to deployed virtual networks. To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User8 can create virtual networks in:
- RG4 only
- RG6 only
- RG4 and RG6 only
- RG5 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:
- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- RG4, RG5, and RG6

Answer Area

User8 can create virtual networks in:
- RG4 only
- RG6 only
- RG4 and RG6 only
- RG5 and RG6 only
- RG4, RG5, and RG6

Correct Answer:

User8 can create NSGs in:
- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- RG4, RG5, and RG6

Box 1: RG6 only -

The policy does not allow the creation of virtual networks/subnets in RG5. Only NSGs can be created in RG4.

Box 2: The policy does not allow the creation of NSGs in RG5.

https://t.me/learningnets

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networksSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Reference:

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

Madball 2 days, 16 hours ago

Q: User8 can create virtual networks in?
A: RG4, RG5 and RG6

My reasoning for this is because User8 is the owner of all three resource groups, there is no Azure policy denying User8 from creating a virtual network in RG4, RG5 or RG6. Additionally there are no resource locks either.

Q: User8 can create NSGs in?
A: RG4 and RG6

My reasoning for this is because User8 is the owner of the two resource groups, there is no Azure policy denying User8 from creating NSGs in RG4 or RG6, and there is no resource locks on the resource groups.

upvoted 1 times

nicejob 6 days ago

box 1 is no answer,
Allowed Resource Type (Deny): Defines the resource types that you can deploy. Its effect is to deny all resources that aren't part of this defined list.

RG4, can't create VN

upvoted 1 times

thienvupt 1 week, 3 days ago

Not allowed resource type virtual networks on RG6 & RG5 so Only RG4 can create Virtual network

upvoted 2 times

https://t.me/learningnets

Question #2 *Topic 10*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment -

Azure AD -

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1 -

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

https://t.me/learningnets

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

https://t.me/learningnets

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements -

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

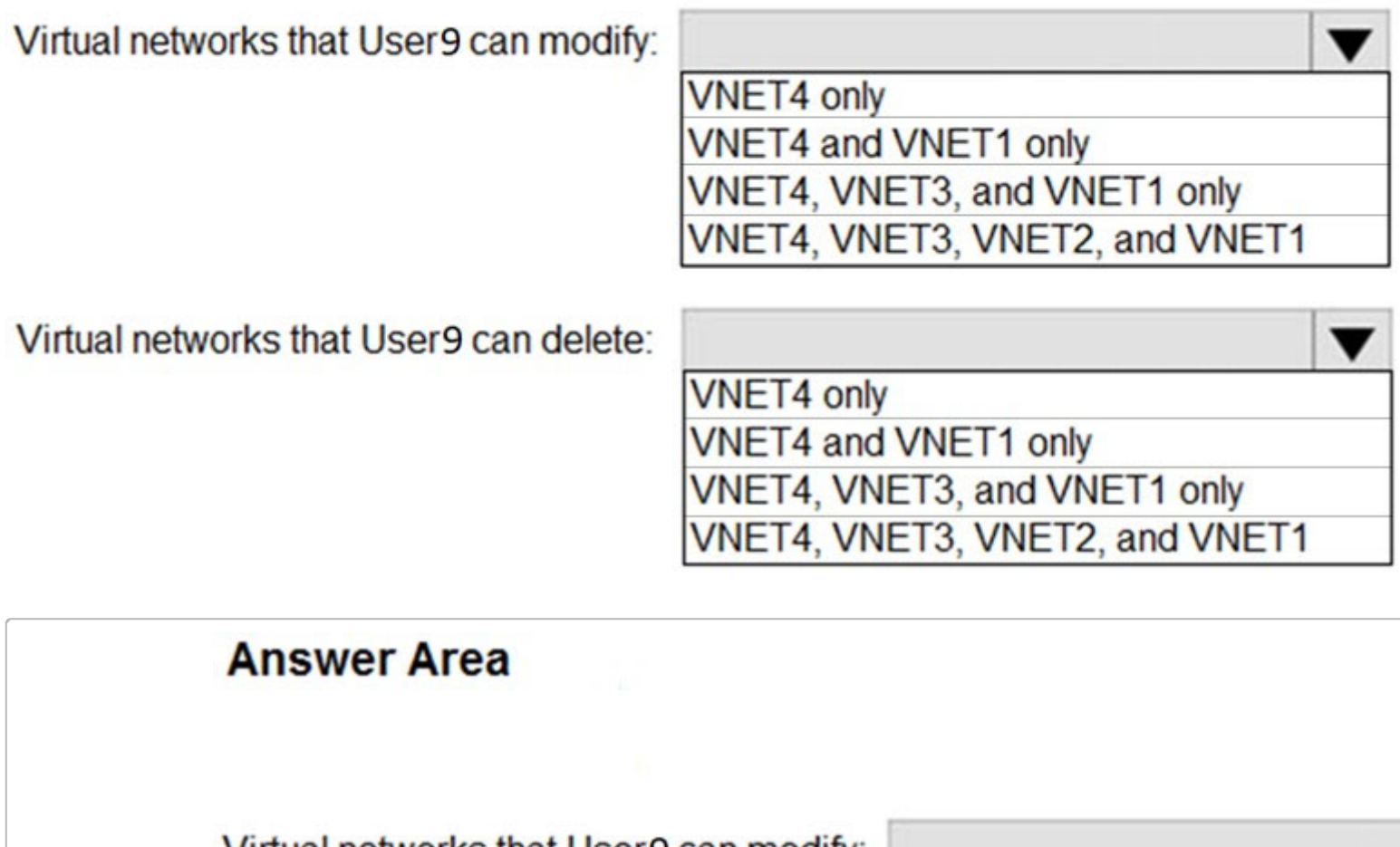
Question

HOTSPOT -

Which virtual networks in Sub1 can User9 modify and delete in their current state? To answer, select the appropriate options in the answer area.

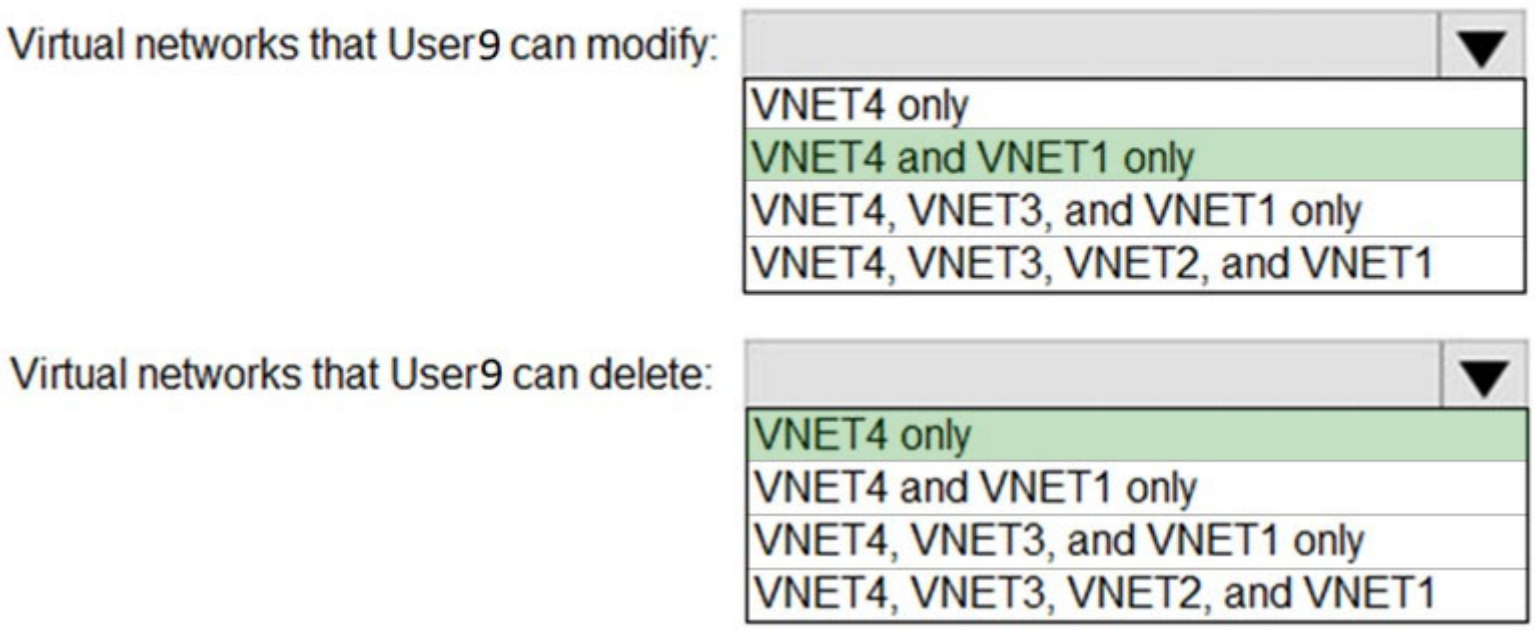
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Correct Answer:



Box 1: VNET4 and VNET1 only -

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only -

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from

https://t.me/learningnets

accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

- CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.
- 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.

Scenario:

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

dadageer Highly Voted 4 months ago

Answers are correct!

upvoted 14 times

diirn Highly Voted 3 months, 3 weeks ago

FIrst anwser: RG3 should be included as it has as well the delete lock. It should be vnet4, vnet1 and vnet3.

Second one is ok.

upvoted 6 times

macco455 3 months, 2 weeks ago

NO, RG3 has a delete AND read only lock on it(assuming thats not a typo in the question) So Answers are correct

upvoted 4 times

thienvupt Most Recent 1 week, 2 days ago

VNET1 Lock delete by RG1
Correct only VNET4

upvoted 1 times

MarioMK 1 month, 3 weeks ago

box 1 is incorrect. Vnet4 can be modifies since there is no lock applied to the RG4. There is a Delete lock on RG1 and 3 which makes them editable. Therefore, the correct answer is Vnet1,3 and 4

upvoted 2 times

3abmula 1 month, 2 weeks ago

VNET 3 is located in RG3 which has two locks, Read-only and Delete, so VNET3 can't either be modified nor deleted.

upvoted 2 times

Topic 11 - Testlet 6

https://t.me/learningnets

Question #1 *Topic 11*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.

https://t.me/learningnets

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersג€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

Question

You need to ensure that you can meet the security operations requirements. What should you do first?

A. Turn on Auto Provisioning in Security Center.

B. Integrate Security Center and Microsoft Cloud App Security.

C. Upgrade the pricing tier of Security Center to Standard.

D. Modify the Security Center workspace configuration.

Correct Answer: *C*

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 advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-days exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

dadageer Highly Voted 4 months ago

The answer which would make sense is C) but in the scenario they mentioned that ASC is Standard already? I think it is a typo and it should be 'free' which will then make answer c) more logical. Also note this is old way of MS ASC tiers (free, standard) which has now been changed to ASC Free, ASC AD ON

upvoted 6 times

dadageer 4 months ago

https://azure.microsoft.com/en-gb/blog/azure-security-center-adds-support-for-custom-security-assessments/

upvoted 1 times

https://t.me/learningnets

L_c Most Recent 1 week ago

Auto provisioning because ASC is already on standard tier

upvoted 1 times

Sethoo 3 months, 3 weeks ago

Why not use auto provisioning. If ASC is standard, then there is no need to move them to a state, in which they are already in. The answer should be A.

upvoted 2 times

Sethoo 3 months, 3 weeks ago

To add to my earlier comment, even under standard tiers, auto provision is diable by default, so they would have to change that to enable make A, the most likely answer
Any of the agents and extensions described on this page can be installed manually (see Manual installation of the Log Analytics agent). However, auto provisioning reduces management overhead by installing all required agents and extensions on existing - and new - machines to ensure faster security coverage for all supported resources.

We recommend enabling auto provisioning, but it's disabled by default.

upvoted 2 times

sureshatt 3 months, 2 weeks ago

auto provisioning only install the monitoring agents, they cannot change security configs.

upvoted 3 times

Topic 12 - Testlet 7

https://t.me/learningnets

Question #1 *Topic 12*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

https://t.me/learningnets

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersλ€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

▪

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

▪

Question

You need to configure WebApp1 to meet the data and application requirements.

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

NOTE: Each correct selection is worth one point.

A. Upload a public certificate.

B. Turn on the HTTPS Only protocol setting.

C. Set the Minimum TLS Version protocol setting to 1.2.

D. Change the pricing tier of the App Service plan.

E. Turn on the Incoming client certificates protocol setting.

Correct Answer: *AC*

A: To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.

C: Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on

Azure App Service.

Incorrect Answers:

B: We need support the http url as well.

Note:

WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.

https://t.me/learningnets

References:
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth https://azure.microsoft.com/en-us/updates/app-service-and-functions-hosted-apps-can-now-update-tls-versions/

thienvupt 1 week, 3 days ago

B. Turn on the HTTPS Only protocol setting. (x) > To force 'mutual auth' you must turn off HTTP
E. Turn on the Incoming client certificates protocol setting. (X) > must set it to 'Require'

upvoted 1 times

https://t.me/learningnets

Question #2 *Topic 12*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

https://t.me/learningnets

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersλ€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

▪

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

▪

Question

HOTSPOT -

You need to create Role1 to meet the platform protection requirements.

How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.

https://t.me/learningnets

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{
   "Name":  "Role1",
   "Id":  "11111111-1111-1111-1111-111111111111",
   "IsCustom" : true,
   "Description": "VM storage operator"
   "Actions" : [
```

["Microsoft.Compute/" | "Microsoft.Resources/" | "Microsoft.Storage/"] [disks/*", | storageAccounts/*", | virtualMachines/disks/*",]

```
   ],
   "NotActions":  [
                  ],
   "AssignableScopes":  [
```

["/" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/RG1" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"]

```
}
```

Answer Area

```
{
   "Name":  "Role1",
   "Id":  "11111111-1111-1111-1111-111111111111",
   "IsCustom" : true,
   "Description": "VM storage operator"
   "Actions" : [
```

Correct Answer:

["Microsoft.Compute/" | "Microsoft.Resources/" | "Microsoft.Storage/"] [disks/*", | storageAccounts/*", | virtualMachines/disks/*",]

```
   ],
   "NotActions":  [
                  ],
   "AssignableScopes":  [
```

["/" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/RG1" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"]

```
}
```

Scenario: A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for
RG1.
Azure RBAC template managed disks "Microsoft.Storage/"

https://t.me/learningnets

Reference:
https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/
https://blogs.msdn.microsoft.com/azure4fun/2016/10/21/custom-azure-rbac-roles-and-how-to-extend-existing-role-definitions-scope/

Rume 1 week, 6 days ago
https://www.examtopics.com/discussions/microsoft/view/6772-exam-az-500-topic-11-question-2-discussion/
upvoted 1 times

https://t.me/learningnets

Question #3 *Topic 12*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the

Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

https://t.me/learningnets

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersג€™ behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

▪

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

▪

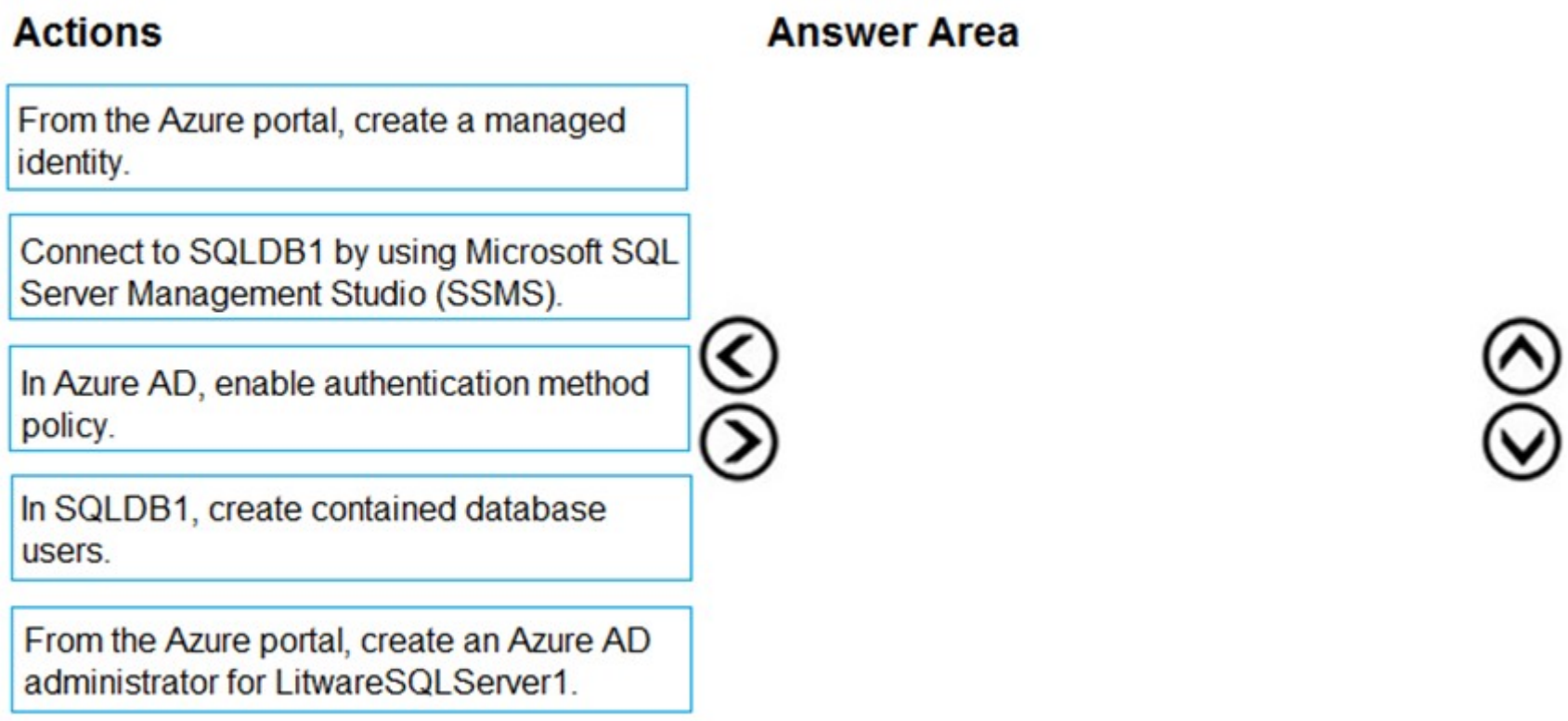
Question

DRAG DROP -

You need to configure SQLDB1 to meet the data and application requirements.

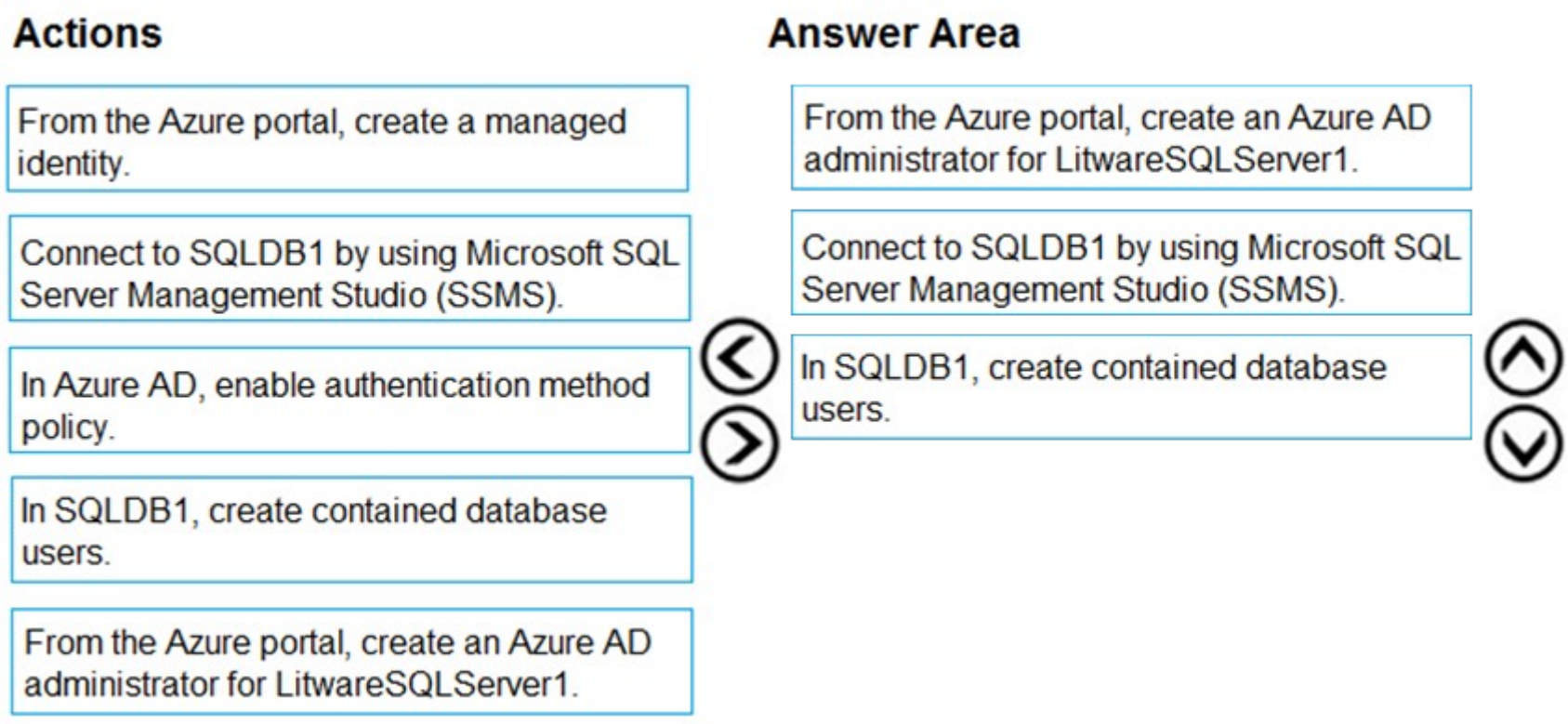
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



https://t.me/learningnets

Correct Answer:



Reference:

https://docs.microsoft.com/en-gb/azure/azure-sql/database/authentication-aad-overview

Rume 1 week, 6 days ago

https://www.examtopics.com/discussions/microsoft/view/9125-exam-az-500-topic-11-question-3-discussion/

upvoted 1 times

https://t.me/learningnets