AZ-500 Exam Topics Review Questions

Updated: 6/7/2021

https://cybersecurityhoy.files.wordpress.com/2021/06/az-500-exam-all.pdf

Updated: 6/7/2021

Contents

1. Stored access policy

You have an Azure Storage account named Sa1 in a resource group named RG1. Users and applications access the blob service and the le service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the le service and the blob service.

You need to revoke all access to Sa1.

Solution: You generate new SASs. Does this meet the goal? No

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.

References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

2. Same as 1

3. Connect HDInsight to your on-premises network

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? NO

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

4. Same as 3

5. Password hash synchronization with seamless single sign-on (SSO)

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.

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 into 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.

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.

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 trac is encrypted and limited to authentication requests.

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

6. Synchronization Rules Editor

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?

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-conguration

7. Conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

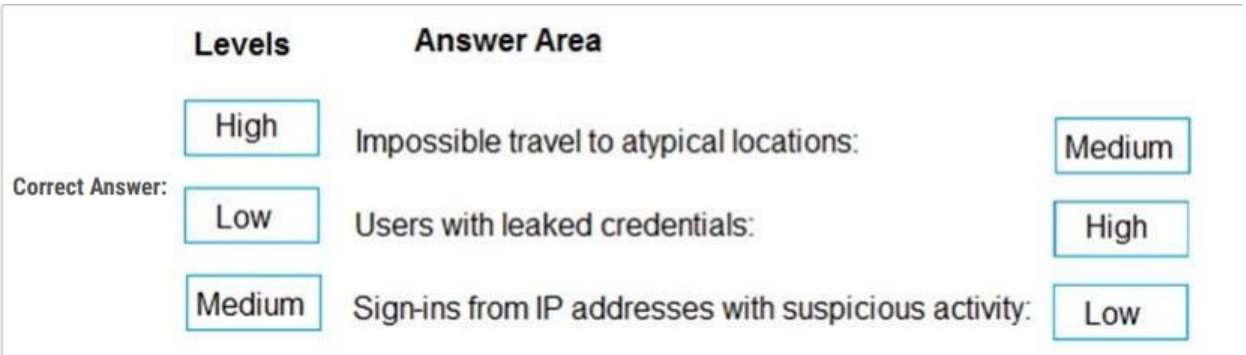
You need to identify the risk level of the following risk events:

➪ 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?

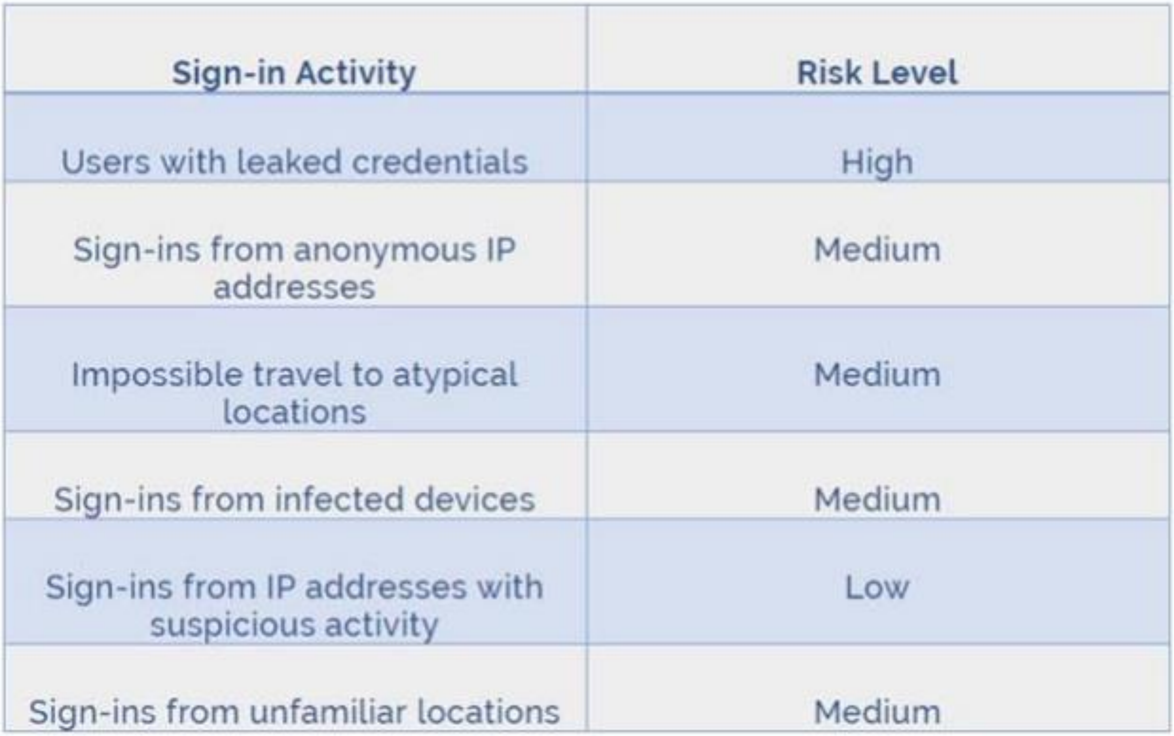


	Levels	Answer Area	
Correct Answer:	High	Impossible travel to atypical locations:	Medium
	Low	Users with leaked credentials:	High
	Medium	Sign-ins from IP addresses with suspicious activity:	Low

Azure AD Identity protection can detect six types of suspicious sign-in activities:

1. Users with leaked credentials
2. Sign-ins from anonymous IP addresses
3. Impossible travel to atypical locations
4. Sign-ins from infected devices
5. Sign-ins from IP addresses with suspicious activity
6. Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks: 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

8. Azure AD Identity Protection user risk policy

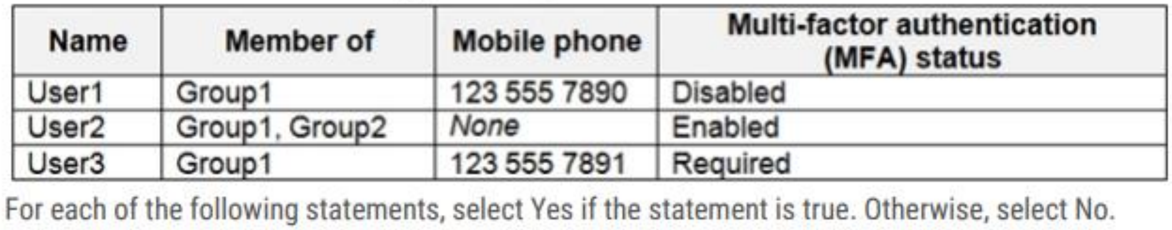
You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

⇨ Assignment: Include Group1, Exclude Group2

⇨ Conditions: Sign-in risk of Medium and above

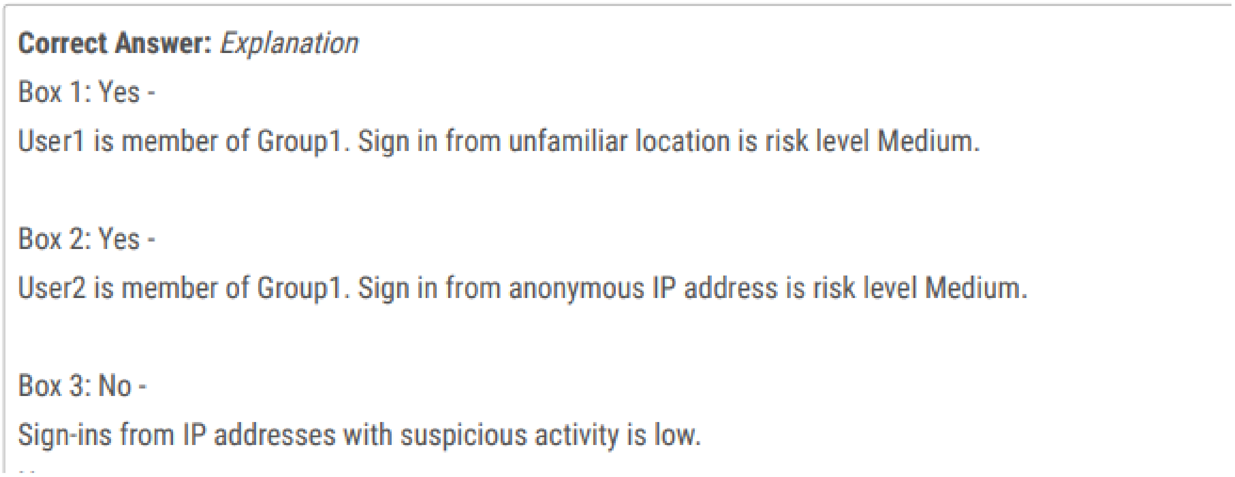
Access: Allow access, Require password change

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

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



Correct Answer: *Explanation*

Box 1: Yes -

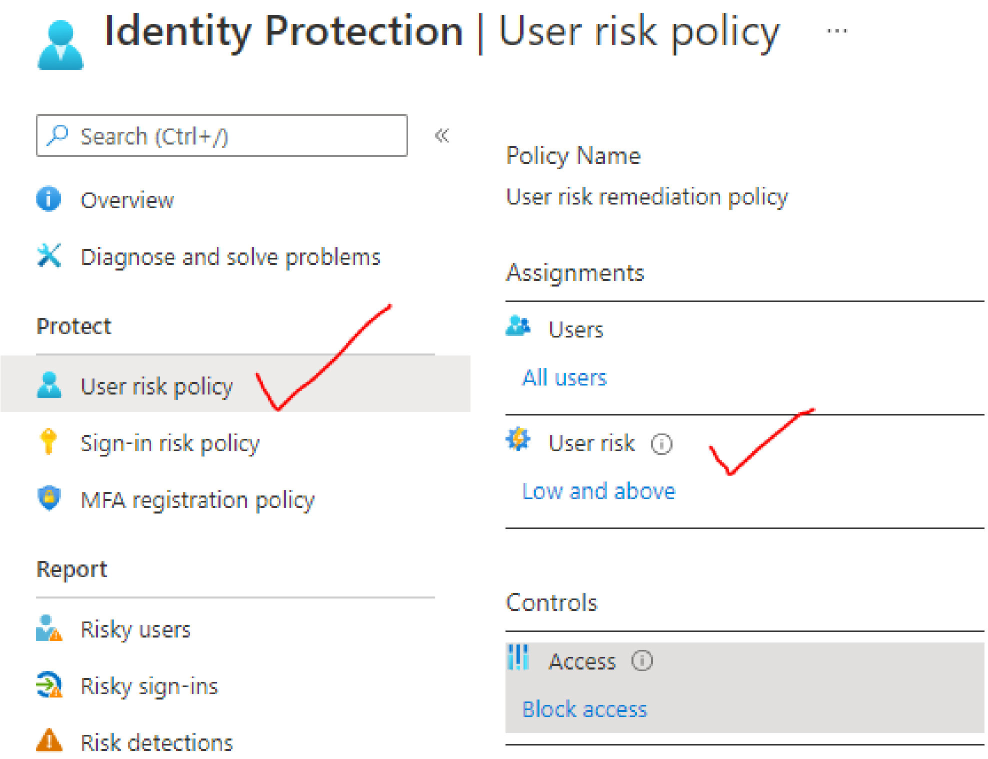
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

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.



Identity Protection | User risk policy ...

Policy Name

User risk remediation policy

Assignments

Users

All users

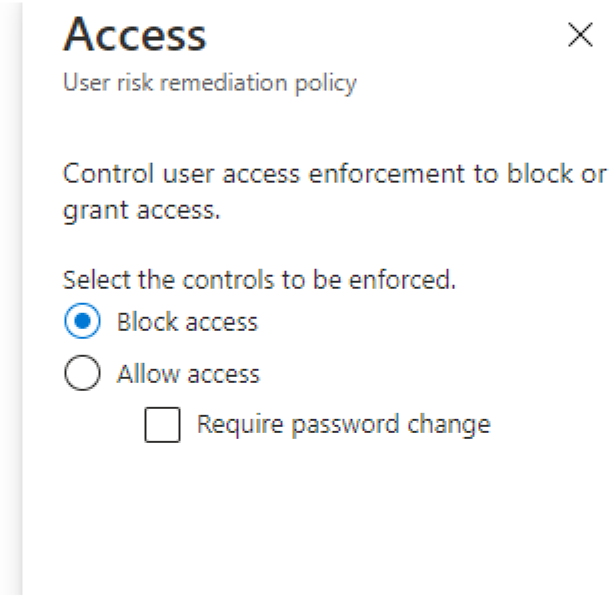
User risk ⓘ

Low and above

Controls

Access ⓘ

Block access



Access

User risk remediation policy

Control user access enforcement to block or grant access.

Select the controls to be enforced.

● Block access

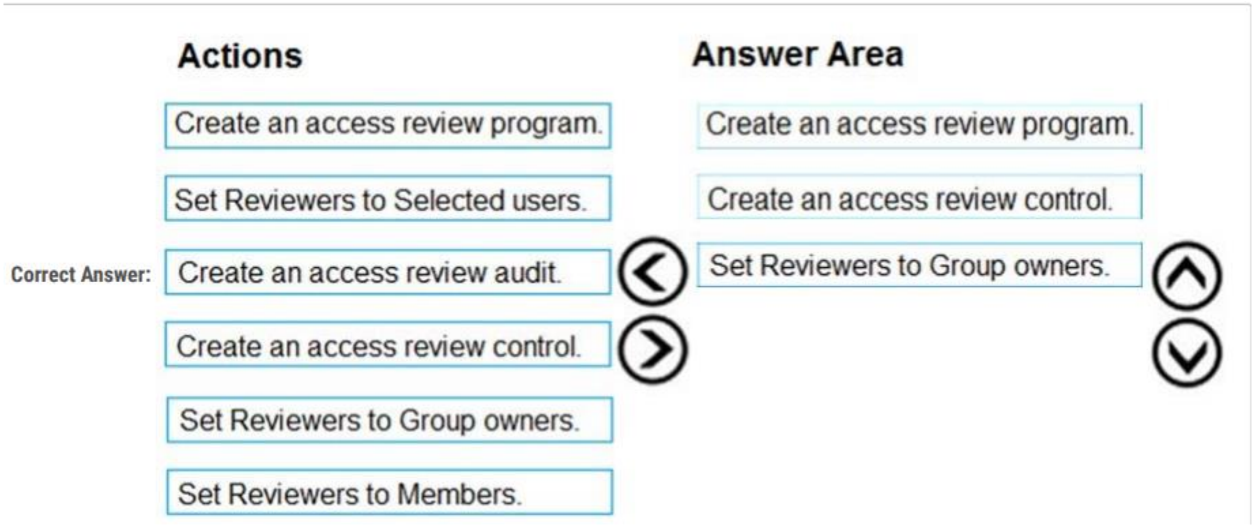
○ Allow access

□ Require password change

9. Access Review

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.



Correct Answer:

Actions

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

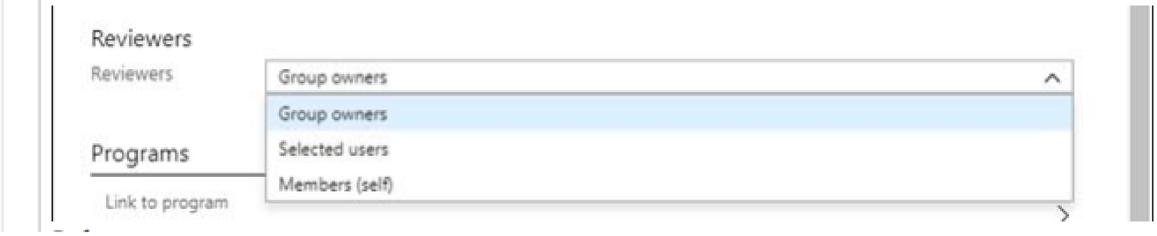
- Create an access review program.
- Create an access review control.
- Set Reviewers to Group owners.

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

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



Reviewers

Reviewers Group owners

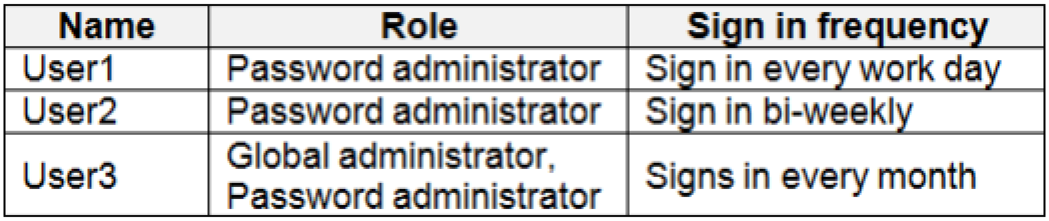
References:

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

https://docs.microsoft.com/en-us/azure/activedirectory/governance/manage-programs-controls

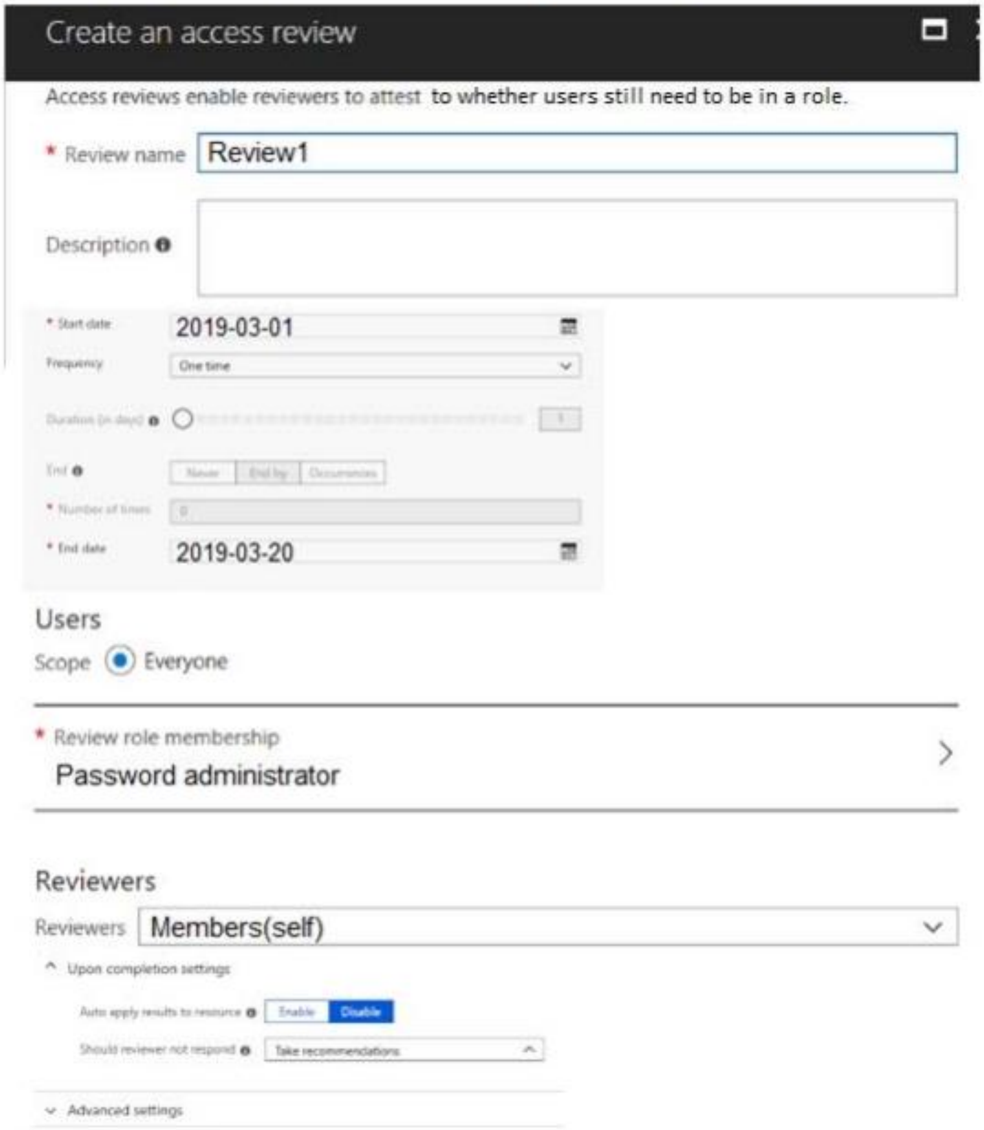
10. Access Review

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	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

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



Create an access review

Access reviews enable reviewers to attest to whether users still need to be in a role.

* Review name: Review1

Description

* Start date: 2019-03-01

Frequency: One time

Duration (in days): 1

End: Never | End by | Occurrences

* Number of times: 0

* End date: 2019-03-20

Users

Scope: ● Everyone

* Review role membership: Password administrator

Reviewers

Reviewers: Members(self)

Upon completion settings

Auto apply results to resource: Enable | [✓ Disable]

Should reviewer not respond: Take recommendations

Advanced settings

Correct Answer: *Explanation*

Box 1: User3 only -

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

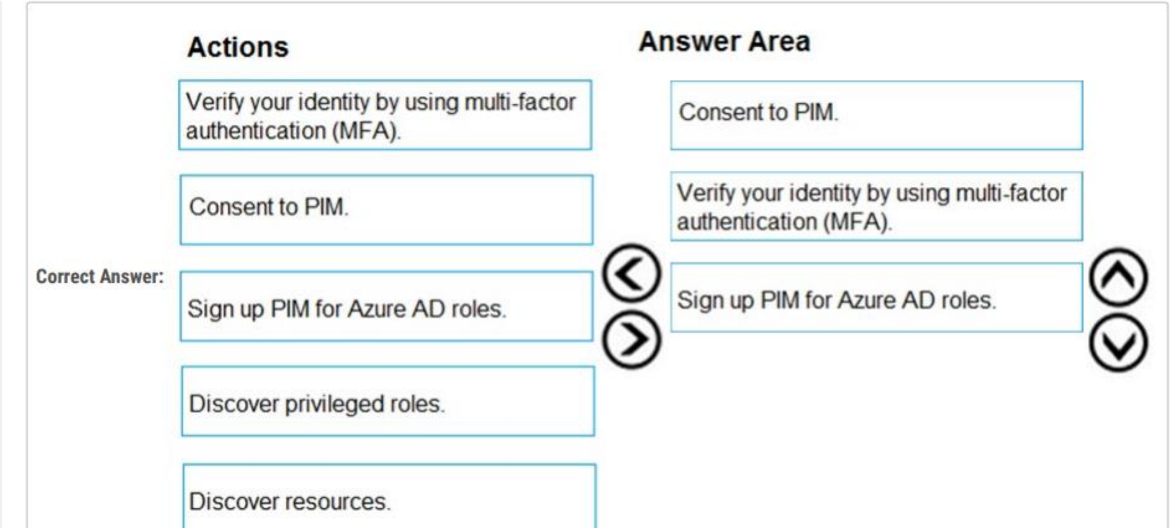
References:

https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review

11. Privileged Identity Management (PIM)

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.



Correct Answer:

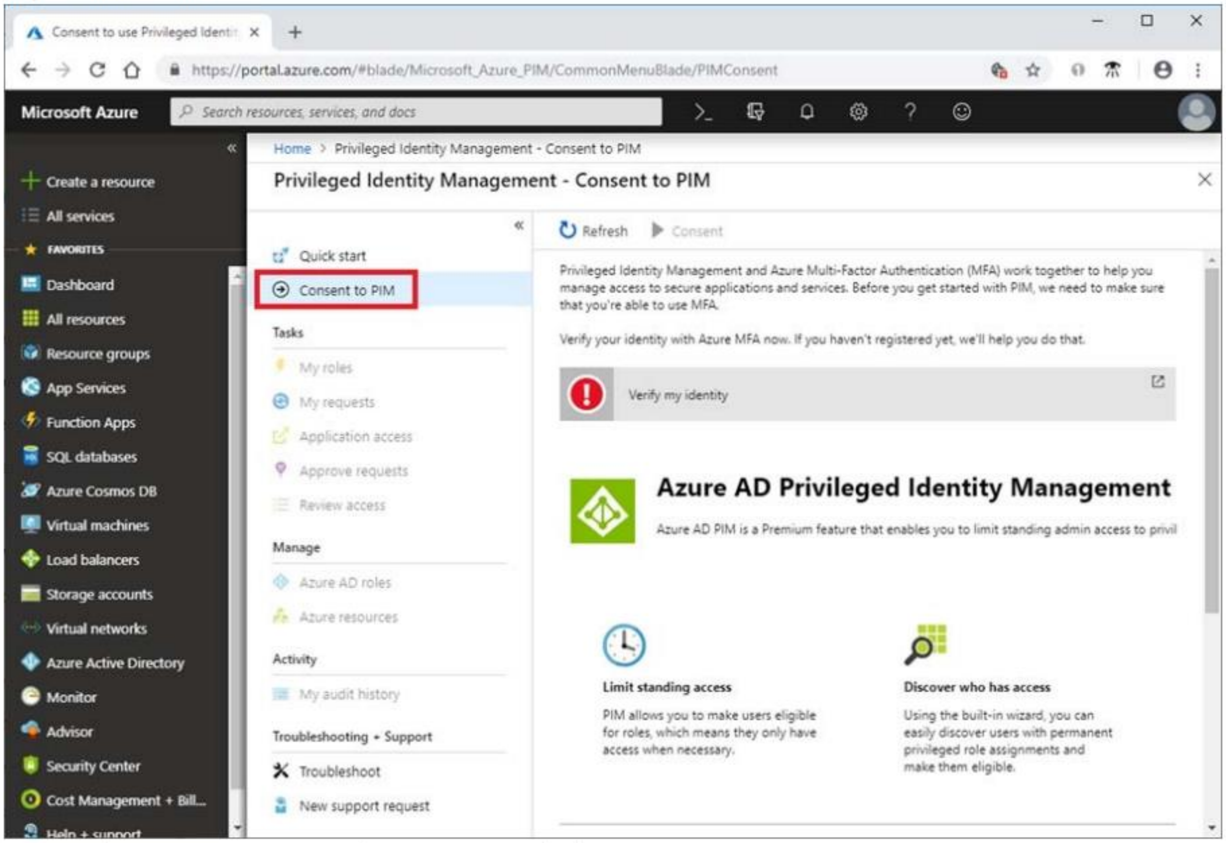
Actions

- Verify your identity by using multi-factor authentication (MFA).
- Consent to PIM.
- Sign up PIM for Azure AD roles.
- Discover privileged roles.
- Discover resources.

Answer Area

- Consent to PIM.
- Verify your identity by using multi-factor authentication (MFA).
- Sign up PIM for Azure AD roles.

Step 1: Consent to PIM -



Privileged Identity Management - Consent to PIM

Privileged Identity Management and Azure Multi-Factor Authentication (MFA) work together to help you manage access to secure applications and services. Before you get started with PIM, we need to make sure that you're able to use MFA.

Verify your identity with Azure MFA now. If you haven't registered yet, we'll help you do that.

Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privil

Limit standing access

PIM allows you to make users eligible for roles, which means they only have access when necessary.

Discover who has access

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.

Step: 2 Verify your identity by using multi-factor authentication (MFA)

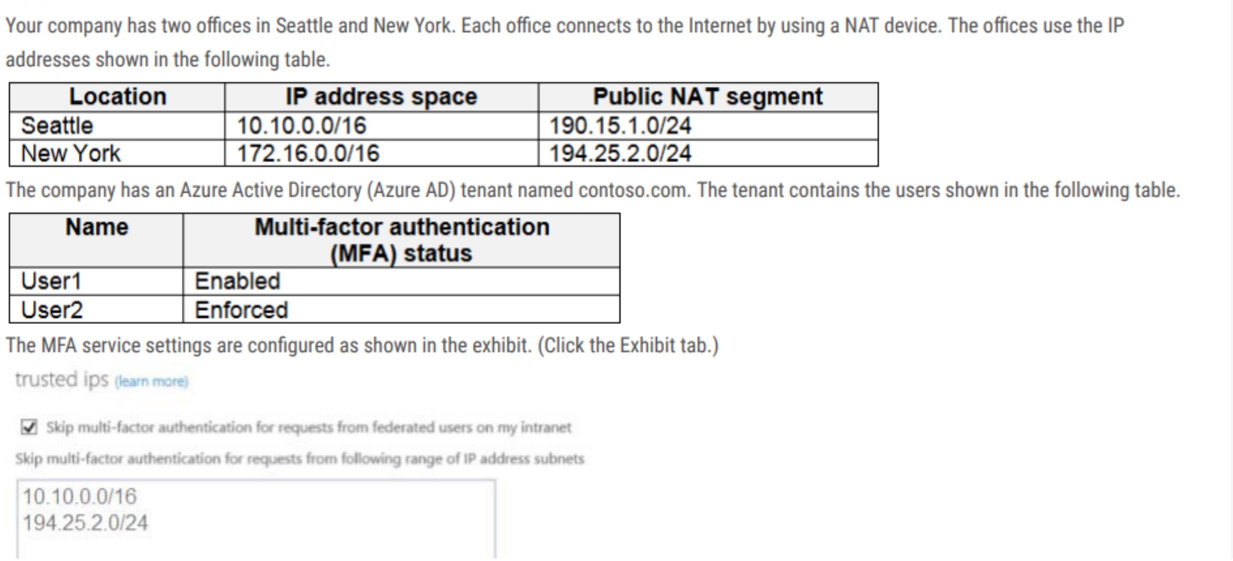
Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account.

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.

References: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

12. Conditional Access and MFA



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

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

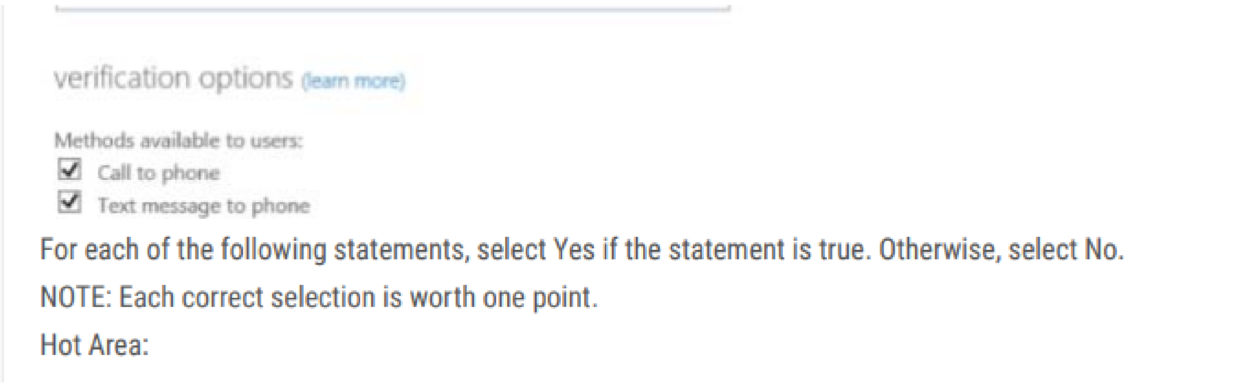
The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

trusted ips (learn more)

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16
194.25.2.0/24



verification options (learn more)

Methods available to users:

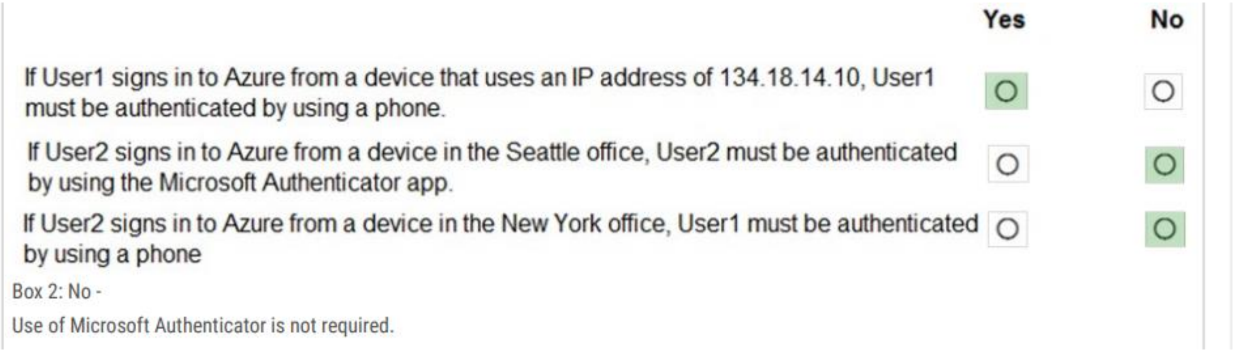
☑ Call to phone

☑ Text message to phone

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

NOTE: Each correct selection is worth one point.

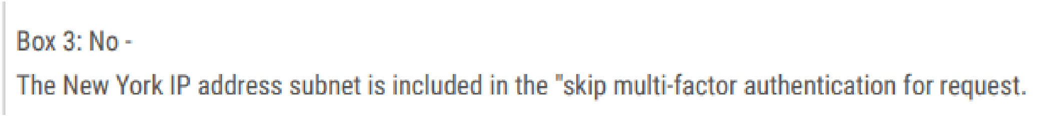
Hot Area:



	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, User1 must be authenticated by using a phone	○	[✓ ○]

Box 2: No -

Use of Microsoft Authenticator is not required.



Box 3: No -

The New York IP address subnet is included in the "skip multi-factor authentication for request.

References: https://www.cayosoft.com/difference-enabling-enforcing-mfa/

13. Azure AD Privileged Identity Management (PIM)

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

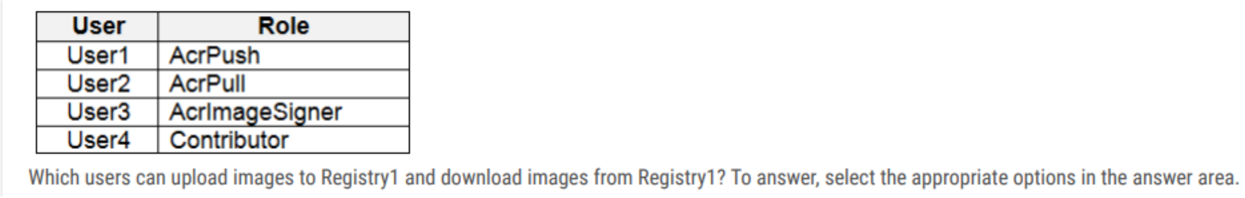
You need to configure each subscription to have the same role assignments. What should you use?

The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.

References: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

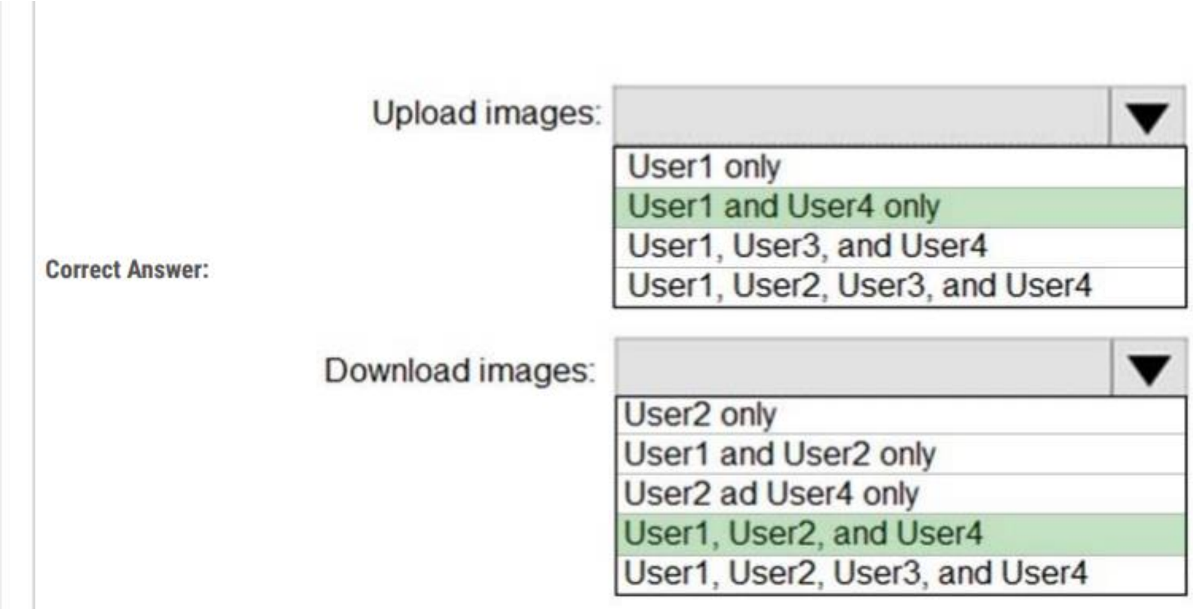
14. Uploading and downloading images to a Registry

You have an Azure Container Registry named Registry1. You add role assignment 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.



Correct Answer:

Upload images:

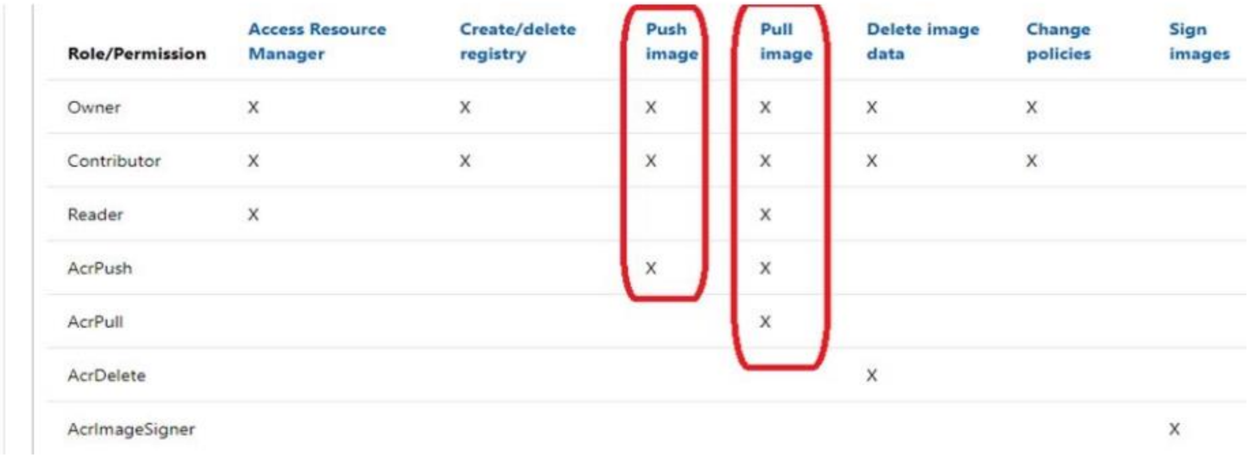
User1 only
[✓ User1 and User4 only]
User1, User3, and User4
User1, User2, User3, and User4

Download images:

User2 only
User1 and User2 only
User2 ad User4 only
[✓ User1, User2, and User4]
User1, User2, User3, and User4

Box 1: User1 and User4 only - Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4 - All, except AcrImagineSigner, can download/pull images



Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

References: https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

15. Configure Azure DNS to host a custom domain for your web apps

You create an Azure web app named Contoso1812 that uses an S1 App service plan. You create a DNS record for www.contoso.com that points to the IP address of 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.

- B. Add a hostname to Contoso1812.
- E. Scale up the App Service plan of Contoso1812.

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:

1. A root "A" record pointing to contoso.com
2. A root "TXT" record for verification
3. A "CNAME" record for the www name that points to the A record

E: To map a custom DNS name to a web app, the web app's App Service plan must be a paid tier (Shared, Basic, Standard, Premium or Consumption for Azure

References: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

16. Stored Access Policy

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? No

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.

References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

17. Connect HDInsight to your on-premises network

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? NO

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

18. Identify which roles and groups are required to configure AD Connect

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?

- The Global administrator role in Azure AD and
- The Enterprise Admins group in Active Directory

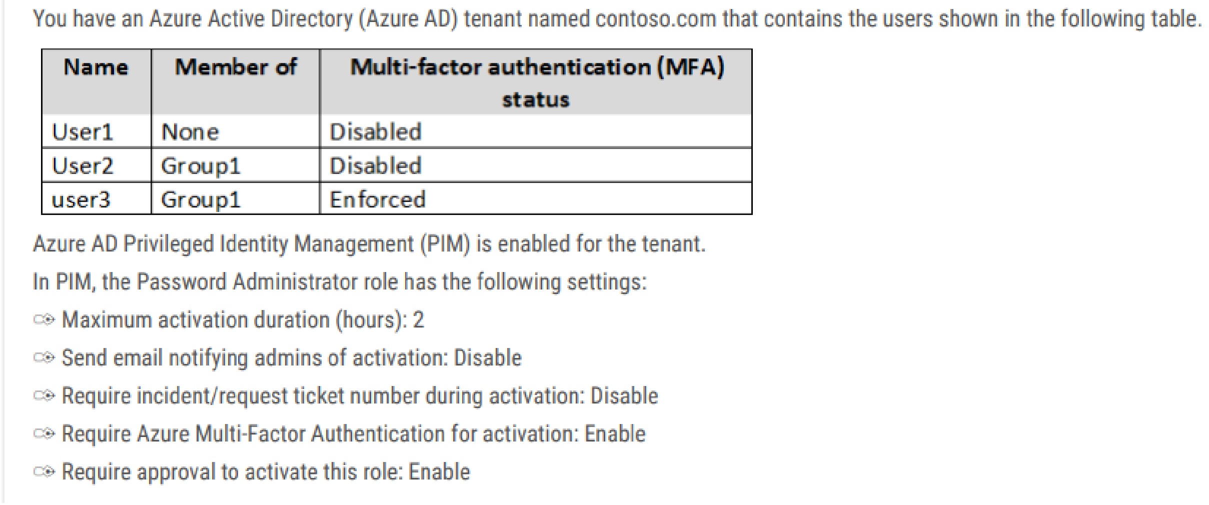
References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

19. Same as 11

20. Same as 3

21. Same as 1

22. Azure AD Privileged Identity Management (PIM)



You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

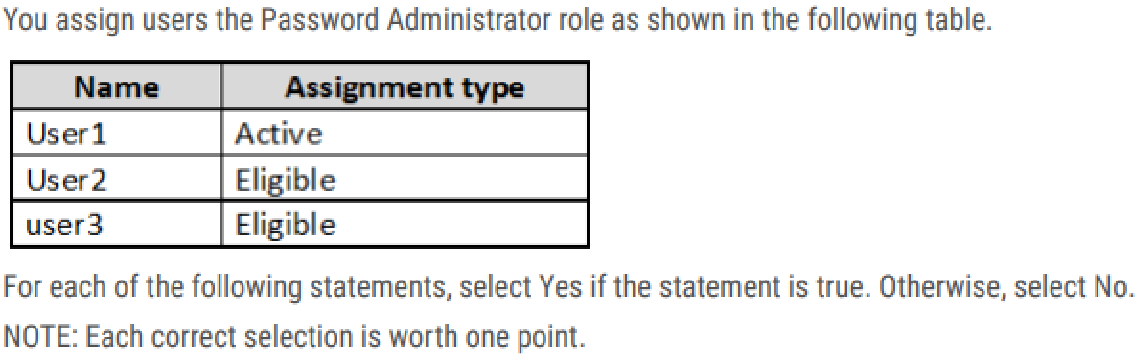
Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

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

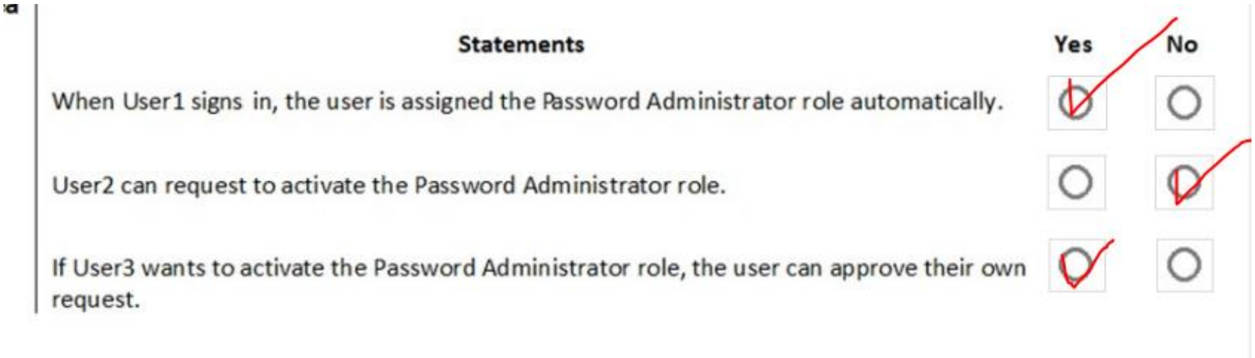


You assign users the Password Administrator role as shown in the following table.

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.



Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	[✓ ○]	○
User2 can request to activate the Password Administrator role.	○	[✓ ○]
If User3 wants to activate the Password Administrator role, the user can approve their own request.	[✓ ○]	○

Box 1: Yes - Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.

Box 2: No - MFA is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled. 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 justication, or requesting approval from designated approvers.

Box 3: Yes - User3 is Group1, which is a Selected Approver Group

Reference: https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

23. SQL Authentication: Active Directory - Password

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance 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?

Use Active Directory password authentication when connecting with an Azure AD principal name using the Azure AD managed domain. Use this method to authenticate to SQL DB/DW with Azure AD for native or federated Azure AD users. A native user is one explicitly created in Azure AD and being authenticated using user name and password, while a federated user is a Windows user whose domain is federated with Azure AD.

The latter method (using user & password) can be used when a user wants to use their windows credential, but their local machine is not joined with the domain (for example, using a remote access). In this case, a Windows user can indicate their domain account and password and can authenticate to SQL DB/DW using federated credentials.

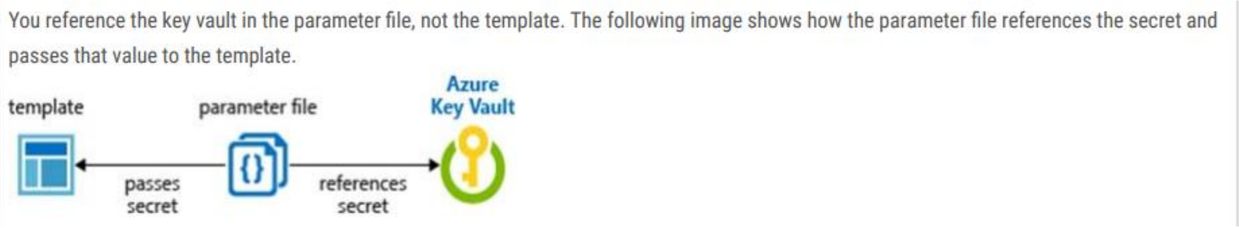
Use Active Directory integrated authentication if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

References: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-congure

24. Azure Resource Manager templates: parameters file

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?

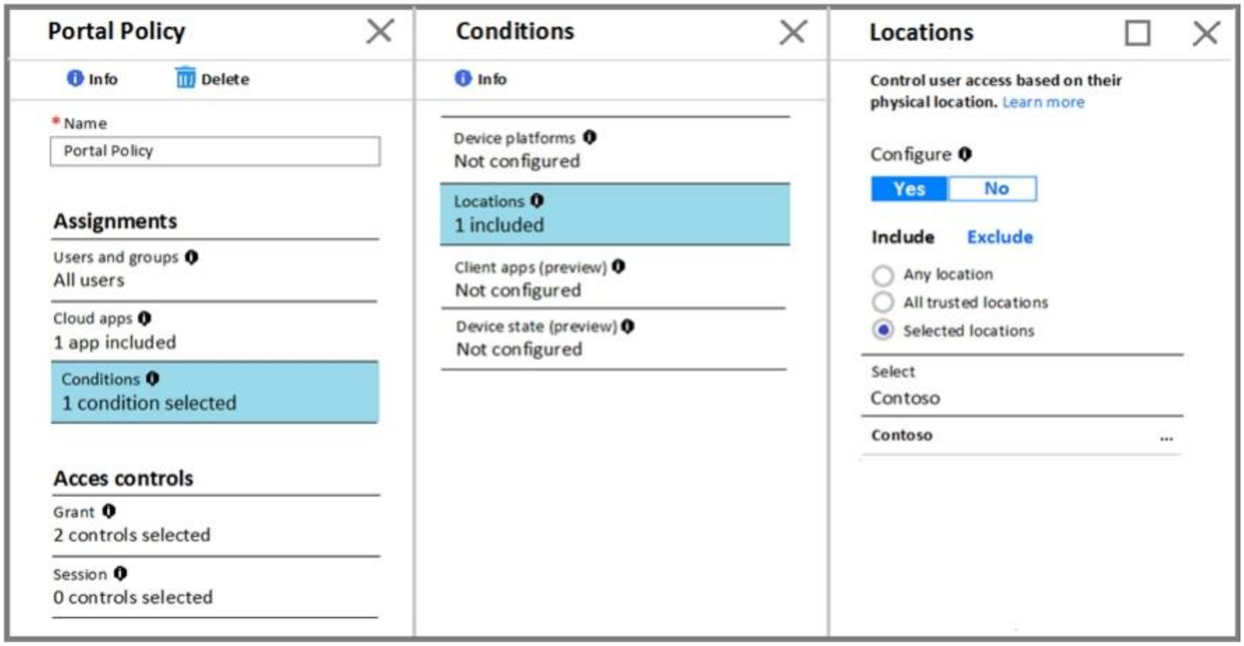


You reference the key vault in the parameter file, not the template. The following image shows how the parameter file references the secret and passes that value to the template.

Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter

25. Conditional Access Policy

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app. The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



Portal Policy

Info   Delete

*Name
Portal Policy

Assignments

Users and groups
All users

Cloud apps
1 app included

Conditions
1 condition selected

Acces controls

Grant
2 controls selected

Session
0 controls selected

Conditions

Info

Device platforms
Not configured

Locations
1 included

Client apps (preview)
Not configured

Device state (preview)
Not configured

Locations

Control user access based on their physical location. Learn more

Configure
[✓ Yes] No

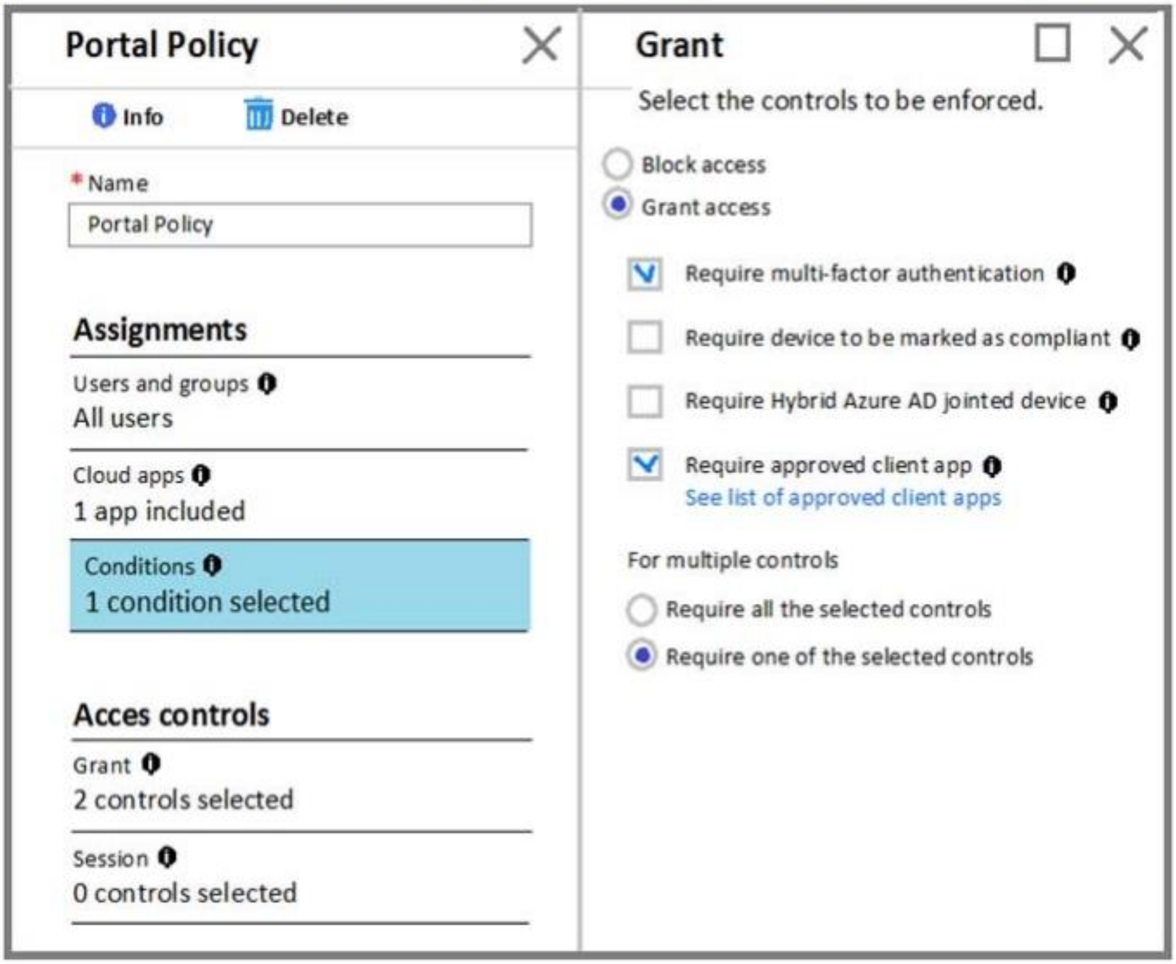
Include   Exclude

○ Any location
○ All trusted locations
● Selected locations

Select
Contoso

Contoso ...

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



Portal Policy

Info Delete

* Name

Portal Policy

Assignments

Users and groups
All users

Cloud apps
1 app included

Conditions
1 condition selected

Acces controls

Grant
2 controls selected

Session
0 controls selected

Grant

Select the controls to be enforced.

○ Block access

● Grant access

☑ Require multi-factor authentication

□ Require device to be marked as compliant

□ Require Hybrid Azure AD jointed device

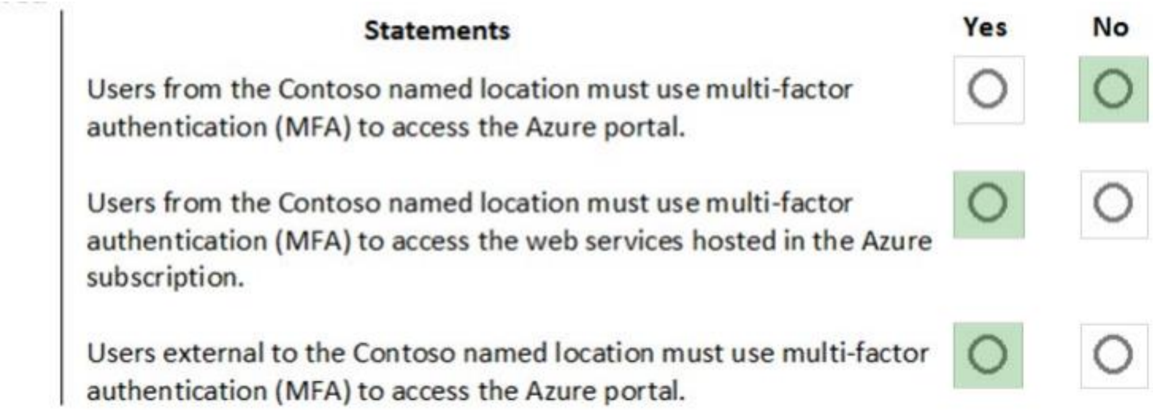
☑ Require approved client app
See list of approved client apps

For multiple controls

○ Require all the selected controls

● Require one of the selected controls

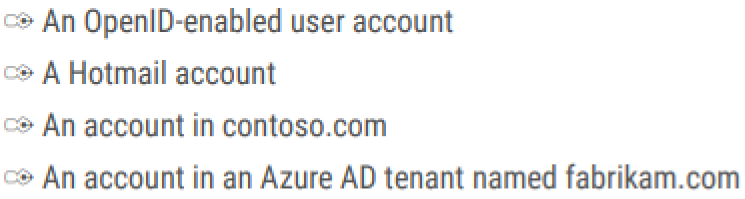
For each of the following statements, select Yes if the statement is true. Otherwise, select No.



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.	[✓ ○]	○

26. Transfering the ownership of Sub1 to Admin1

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?

- Contoso.com and fabrikam.com only

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/billingsubscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant

27. Azure Blueprints

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?

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

Topic 2 – Question set 2

1. Install the container network interface (CNI) plug-in.

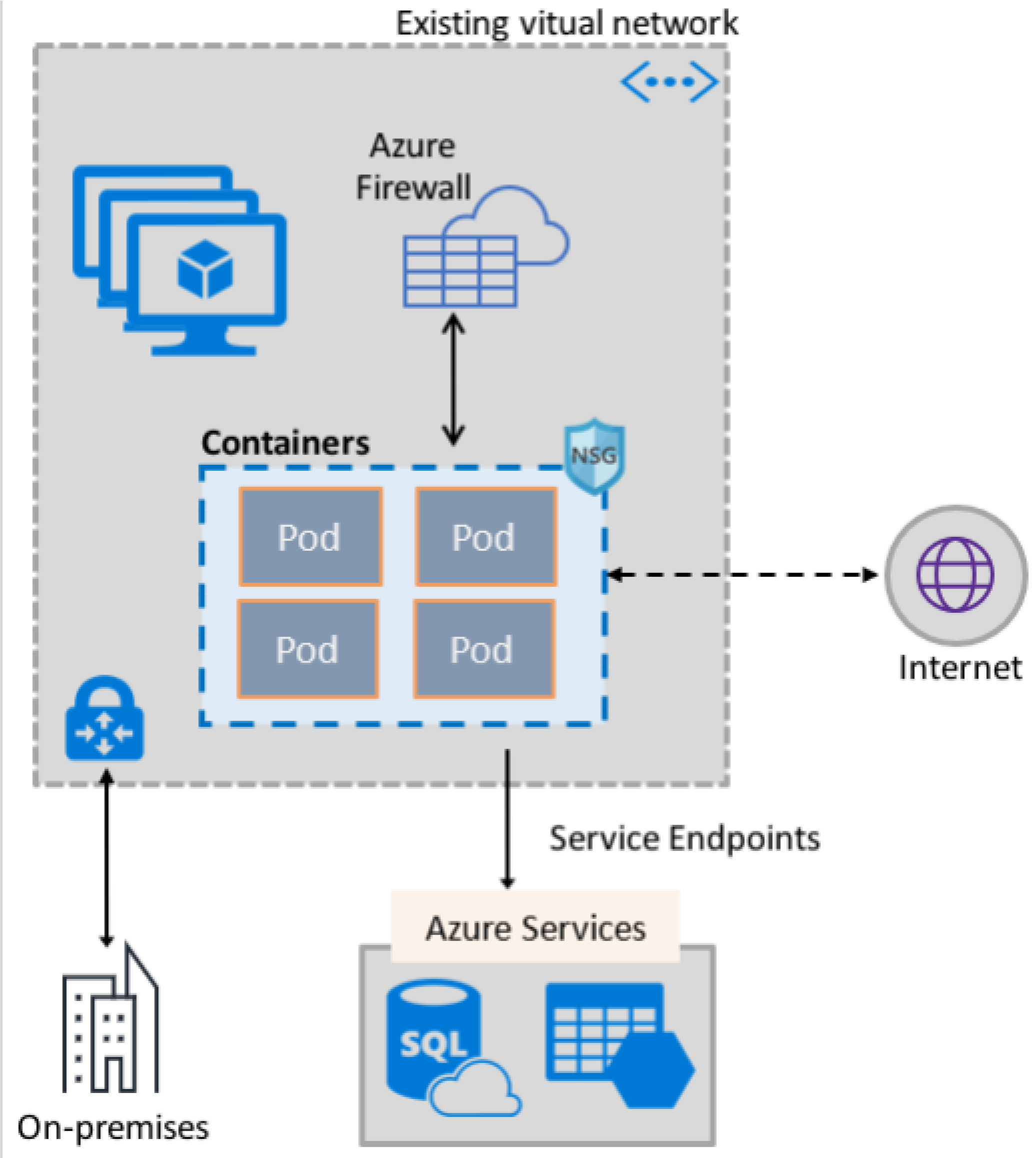
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

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?

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

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



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

2. Azure Desired State Configuration (DSC) virtual machine extension

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.

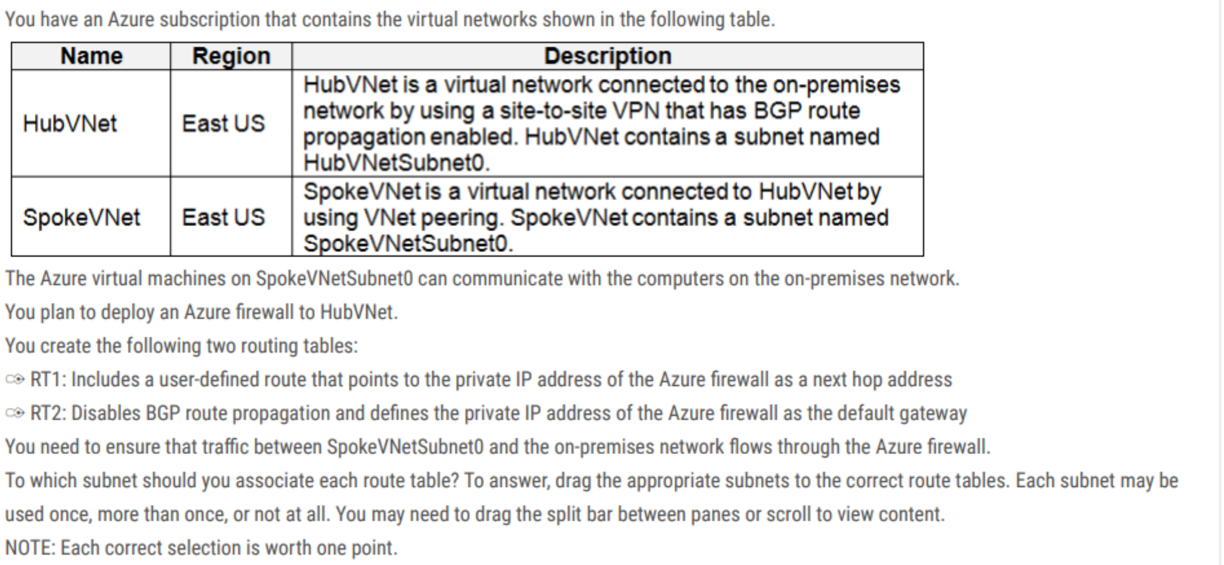
What should you use?

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

3. HubVNet and SpokeVNet



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 a subnet named HubVNetSubnet0.
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.

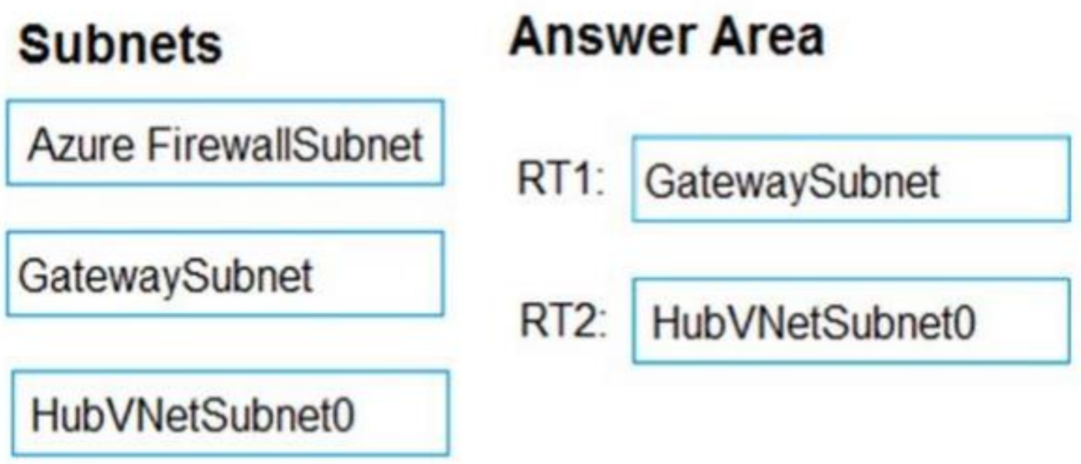
You create the following two routing tables:

- 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.



Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

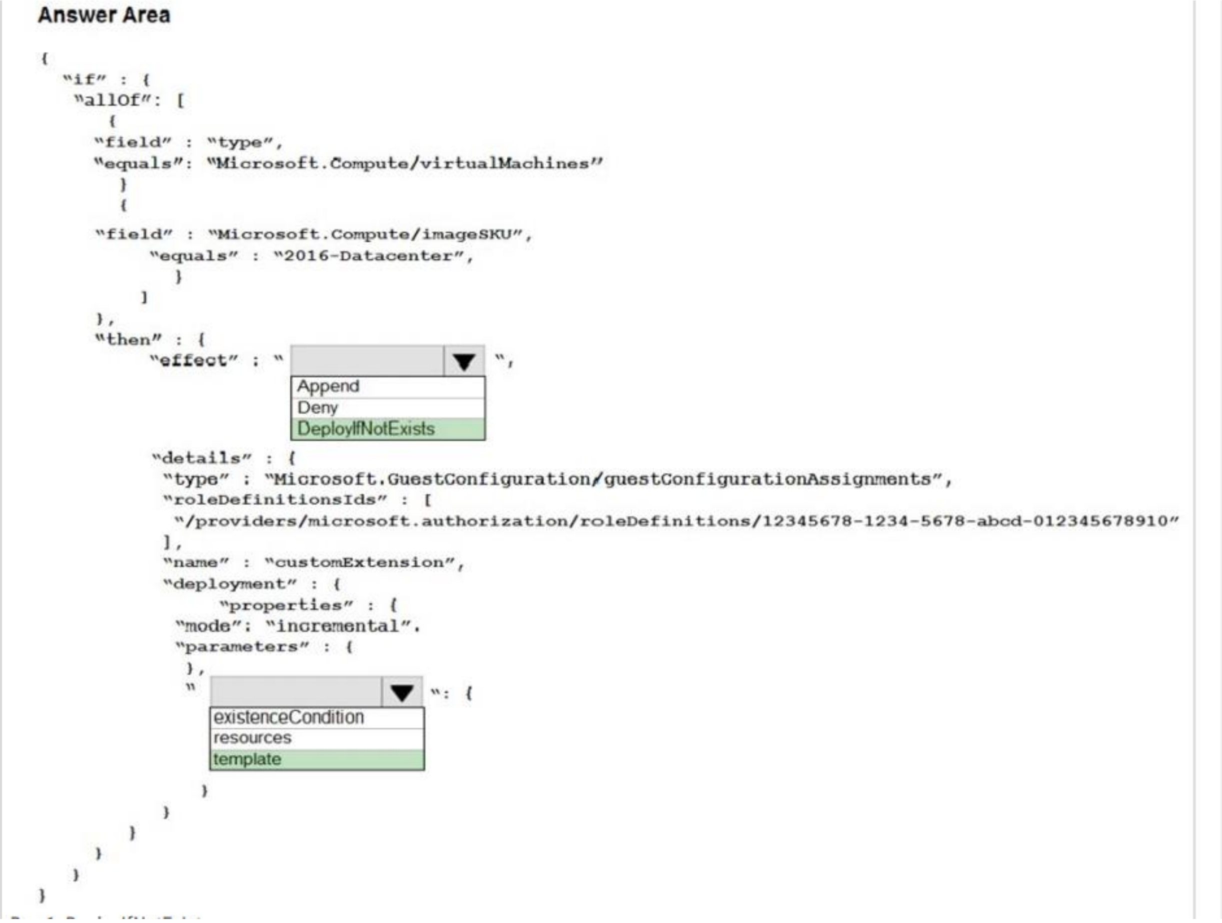
Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

4. DeployIfNotExists

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.



Answer Area

```
{
  "if" : {
   "allOf": [
     {
   "field" : "type",
   "equals": "Microsoft.Compute/virtualMachines"
      }
      {
   "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
           }
        ]
   },
   "then" : {
        "effect" : "                ",
        "details" : {
         "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
         "roleDefinitionsIds" : [
          "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
         ],
         "name" : "customExtension",
         "deployment" : {
              "properties" : {
          "mode": "incremental".
          "parameters" : {
           },
           "                ": {
             }
          }
      }
    }
  }
}
```

Box 1: DeployIfNotExists - DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template - The details property of the DeployIfNotExists effects has all the subproperties that dene 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