

# 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 .....	2
2. Same as 1 .....	3
3. Connect HDInsight to your on-premises network .....	3
4. Same as 3 .....	3
5. Password hash synchronization with seamless single sign-on (SSO).....	3
6. Synchronization Rules Editor .....	4
7. Conditional access policies.....	4
8. Azure AD Identity Protection user risk policy .....	5
9. Access Review .....	7
10. Access Review .....	8
11. Privileged Identity Management (PIM).....	10
12. Conditional Access and MFA.....	12
13. Azure AD Privileged Identity Management (PIM).....	13
14. Uploading and downloading images to a Registry.....	13
15. Configure Azure DNS to host a custom domain for your web apps .....	14
16. Stored Access Policy.....	14
17. Connect HDInsight to your on-premises network .....	15
18. Identify which roles and groups are required to configure AD Connect .....	15
19. Same as 11 .....	16
20. Same as 3 .....	16
21. Same as 1 .....	16
22. Azure AD Privileged Identity Management (PIM).....	16
23. SQL Authentication: Active Directory - Password.....	17
24. Azure Resource Manager templates: parameters file .....	17
25. Conditional Access Policy.....	18
26. Transferring the ownership of Sub1 to Admin1 .....	19
27. Azure Blueprints.....	20

Topic 2 – Question set 2.....	21
1. Install the container network interface (CNI) plug-in. ....	21
2. Azure Desired State Configuration (DSC) virtual machine extension .....	22
3. HubVNet and SpokeVNet.....	23
4. DeployIfNotExists.....	26
5. Configuring an Azure Kubernetes Service (AKS) cluster .....	27
6. Resource Locking – to review .....	29
7. Azure update management .....	30
8. Network Security Groups (NSG) and Network Security Rules .....	31
9. Azure Key Vault.....	34
References .....	37
ExamRef: Create a Virtual Network .....	37
ExamRef Summaries .....	38
Chapter 4 Summary .....	38

## 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 traffic 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-configuration>

## 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 ...

 Overview

 Diagnose and solve problems


### Protect


 User risk policy ✓


 Sign-in risk policy

 MFA registration policy

### Report

 Risky users

 Risky sign-ins

 Risk detections


### 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.

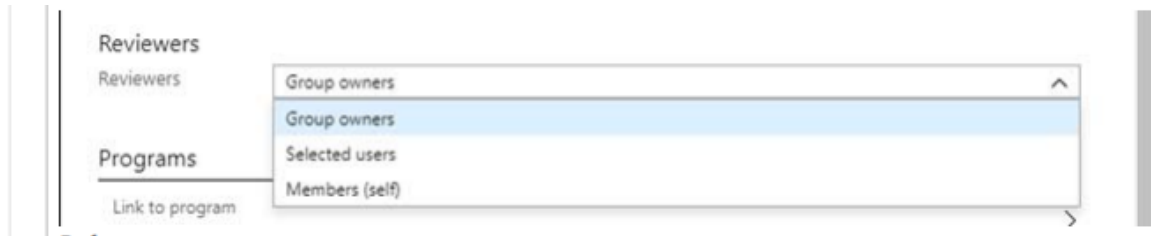
Actions		Answer Area
Create an access review program.		Create an access review program.
Set Reviewers to Selected users.		Create an access review control.
Correct Answer: Create an access review audit.	⬅	Set Reviewers to Group owners. ⬆
Create an access review control.	➡	⬇
Set Reviewers to Group owners.		
Set Reviewers to Members.		

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/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

Description

\* Start date:

Frequency:

Duration (in days)

End

\* Number of times

\* End date:

#### Users

Scope ☒ Everyone

---

\* Review role membership

---

#### Reviewers

Reviewers

^ Upon completion settings

Auto apply results to resource

Should reviewer not respond

^ 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>

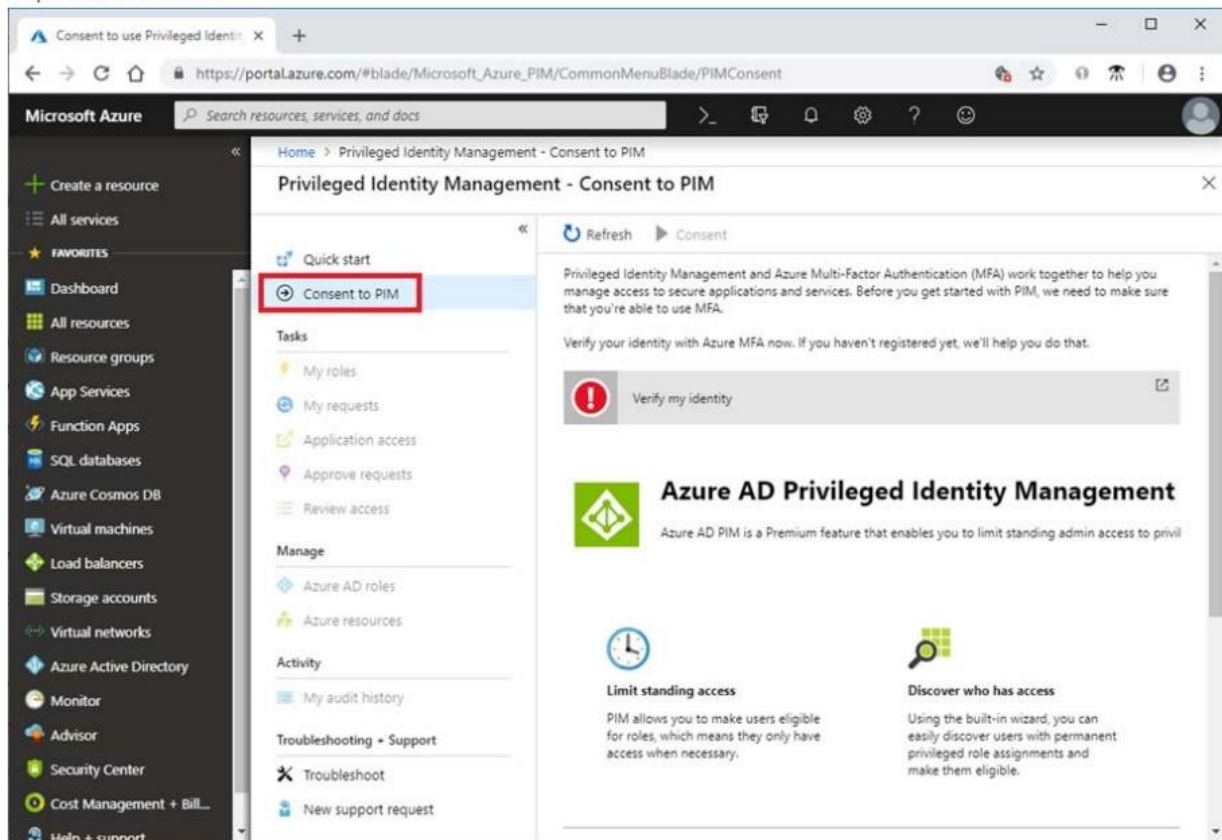
## 11. Privileged Identity Management (PIM)

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.

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

Step 1: Consent to PIM -



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.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input checked="" type="radio"/>
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 AcrImageSigner, 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.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input checked="" type="radio"/>	<input type="radio"/>

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 justification, 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.

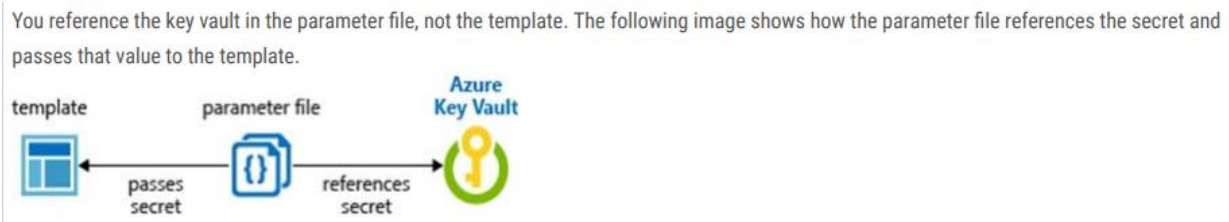
References: <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure>

## 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?



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	Conditions	Locations
<div><b>Info</b> <b>Delete</b></div> <div><b>Name</b> Portal Policy</div> <div><b>Assignments</b> Users and groups <b>1</b> All users Cloud apps <b>1</b> 1 app included <b>Conditions</b> <b>1</b> 1 condition selected <b>Access controls</b> Grant <b>1</b> 2 controls selected Session <b>1</b> 0 controls selected</div>	<div><b>Info</b></div> <div>Device platforms <b>1</b> Not configured</div> <div><b>Locations</b> <b>1</b> 1 included</div> <div>Client apps (preview) <b>1</b> Not configured</div> <div>Device state (preview) <b>1</b> Not configured</div>	<div>Control user access based on their physical location. <a href="#">Learn more</a></div> <div><b>Configure</b> <b>1</b> <b>Yes</b> <b>No</b></div> <div><b>Include</b> <b>Exclude</b> <input type="radio"/> Any location <input type="radio"/> All trusted locations <input checked="" type="radio"/> Selected locations</div> <div>Select Contoso Contoso ...</div>

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

### Portal Policy

Info
Delete

Name

#### Assignments

Users and groups

All users

Cloud apps

1 app included

Conditions

1 condition selected

#### Access 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 joined 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.	<input type="radio"/>	<input checked="" type="radio"/>
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>

## 26. Transferring 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/billing-subscription-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.

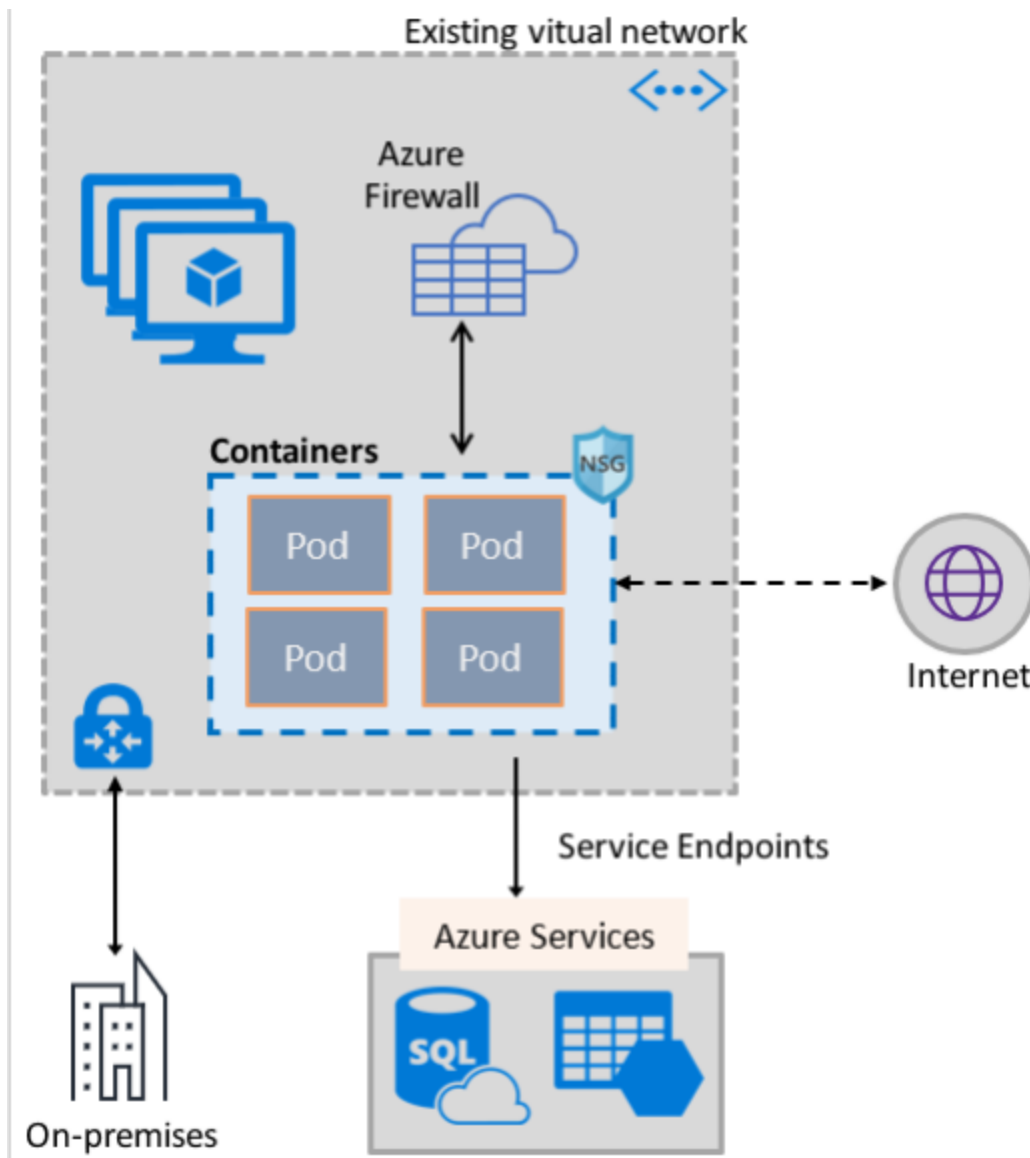
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

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

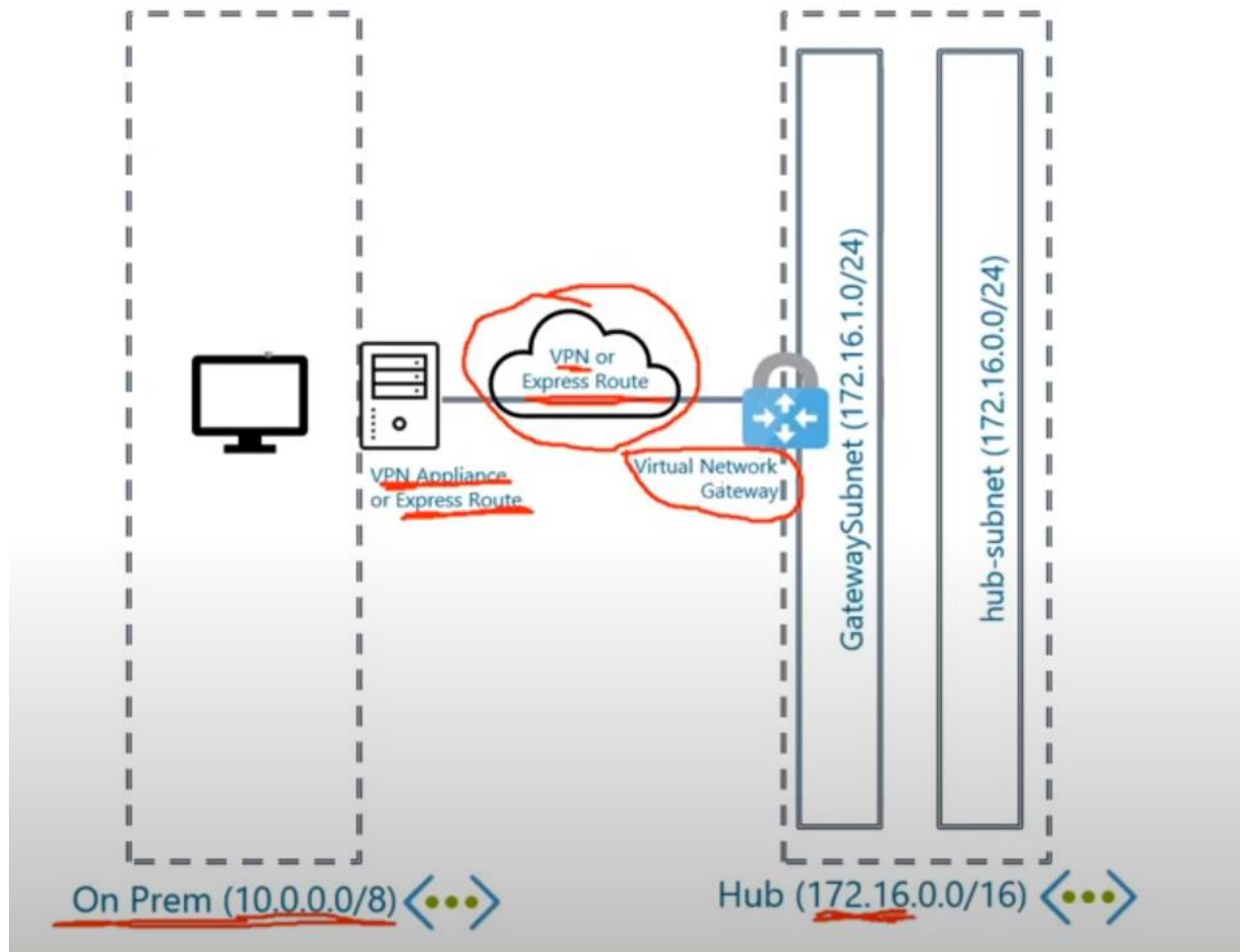
#### Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

### Hub and Spoke Topology

# Hub and Spoke Topology



Azure -to-Onsite VPN

Home > hubspokedemo > vpn-to-onpremise | Connections >



Search (Ctrl+/,)	Move	Download configuration	Delete
Overview	Resource group (change) hubspokedemo	Data in 836.44 KiB	
Activity log	Status Connected	Data out 197.15 KiB	
Access control (IAM)	Location East US	Virtual network hub-vnet	
Tags	Subscription (change) Visual Studio Enterprise	Virtual network gateway vpn-to-onpremise (168.62.172.132)	
Settings	Subscription ID 025f9a1c-4bcf-4b7b-ba91-d3f94c7379ea	Local network gateway blaize-lan (71.65.150.28)	
Shared key	Tags (change) Click here to add tags		
Configuration			
Properties			
Locks			

## Tutorial: Setting Up HUB and SPOKE NETWORKS on AZURE

[https://www.youtube.com/watch?v=j8meGy\\_mc1s](https://www.youtube.com/watch?v=j8meGy_mc1s)

# Azure Site-to-Site VPN

- **IPsec/IKE VPN tunnel** between the VPN gateway and an on-premises VPN device
- Typically less than **1 GB aggregate connectivity**
- Supports **static and dynamic routing**
- **Active-passive** or **active-active** config

Azure ExpressRoute

- Layer 3 connectivity between on-premises and Azure via a connectivity provider
- **No traffic traverses the internet**
- Higher security than internet-based connections
- **Encryption:** supports MACsec and IPsec for end-to-end connectivity encryption
- **Bandwidth:** supports high-bandwidth connectivity scenarios (up to 10 GB)

<https://www.linkedin.com/learning/microsoft-azure-security-technologies-az-500-cert-prep-2-implement-platform-protection-2/secure-the-connectivity-of-virtual-networks?u=86261762>

#### 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": "DeployIfNotExists",
    "details": {
      "type": "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds": [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name": "customExtension",
      "deployment": {
        "properties": {
          "mode": "incremental",
          "parameters": {
            "template": {
              "existenceCondition": {
                "allOf": [
                  {
                    "field": "type",
                    "equals": "Microsoft.Compute/virtualMachines"
                  },
                  {
                    "field": "Microsoft.Compute/imageSKU",
                    "equals": "2016-Datacenter",
                  }
                ]
              },
              "resources": [
                {
                  "type": "Microsoft.Compute/virtualMachines",
                  "name": "vm",
                  "apiVersion": "2016-03-30",
                  "location": "westus",
                  "properties": {
                    "hardwareProfile": {
                      "vmSize": "Standard_DS11_v2"
                    },
                    "osProfile": {
                      "linuxConfiguration": {
                        "provision": true
                      },
                      "passwordProfile": {
                        "password": "P@ssw0rd!",
                        "passwordBypass": {
                          "enabled": true,
                          "message": "The password is required by the operating system."
                        }
                      }
                    },
                    "storageProfile": {
                      "imageReference": {
                        "publisher": "Canonical",
                        "offer": "UbuntuServer",
                        "sku": "16.04-LTS",
                        "version": "latest"
                      },
                      "osDisk": {
                        "createOption": "FromImage",
                        "managedBy": "Azure"
                      }
                    }
                  }
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

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>

## 5. Configuring an Azure Kubernetes Service (AKS) cluster

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?

- an Azure Active Directory (Azure AD) role assignment

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>

[Demo: Configure authentication for containers](#)

# Registry

## Authentication Scenarios

Two primary scenarios are individual identity (interactive) and headless/service identity (no user involved).

### Authentication Options for ACR

Method	How to Authenticate
Individual AD identity	<b>az acr login</b> in Azure CLI
AD service principal	<b>docker login</b> <b>az acr login</b> in Azure CLI
Integrate with AKS	Attach registry when AKS cluster created or updated
Managed identity for Azure resources	<b>docker login</b> <b>az acr login</b> in Azure CLI
Admin user	<b>docker login</b>
Repository scoped access token	<b>docker login</b> <b>az acr login</b> in Azure CLI

### Microsoft Recommendation



## 6. Resource Locking – to review

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.

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input checked="" type="radio"/>
You can start VM2.	<input checked="" type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input checked="" type="radio"/>	<input type="radio"/>

- VM1 has Lock1 applied to it, which is Read-only lock. And Read-only lock does not allow a VM to start

## 7. Azure update management

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.

Update1:	<div><div></div><div>▼</div></div> <div>VM2 only</div> <div>VM4 only</div> <div>VM1 and VM2 only</div> <div>VM1, VM2, VM4, VM5, and VM6</div>
Update2:	<div><div></div><div>▼</div></div> <div>VM5 only</div> <div>VM1 and VM5 only</div> <div>VM4 and VM5 only</div> <div>VM1, VM2, and VM5 only</div> <div>VM1, VM2, VM3, VM4, and VM5</div>

Update1: VM1 and VM2 only -

VM3: Windows Server 2016 West US RG2

Update2: VM4 and VM5 only -

VM6: CentOS 7.5 East US RG1 -

- Update 1 updates VM3, which is a Windows Server 2016 VM in West US in RG2
- Update 2 updates VM6, which is a CentOS 7.5 Linux Machine in East US in RG1

### Windows VMs

- VM1, VM2, and VM3

### Linux VMs

- VM4, VM5, and VM6

## 8. Network Security Groups (NSG) and Network Security Rules

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.

NSGs:

	▼
1	
2	
3	
4	





Network security rules:

	▼
1	
2	
3	
4	

- Because there is only 1 subnet traffic is allowed internally in the VMs by default
- You need ??? NSG to allow traffic from the Internet to VM1 and VM2
- You need 3 rules: why?

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

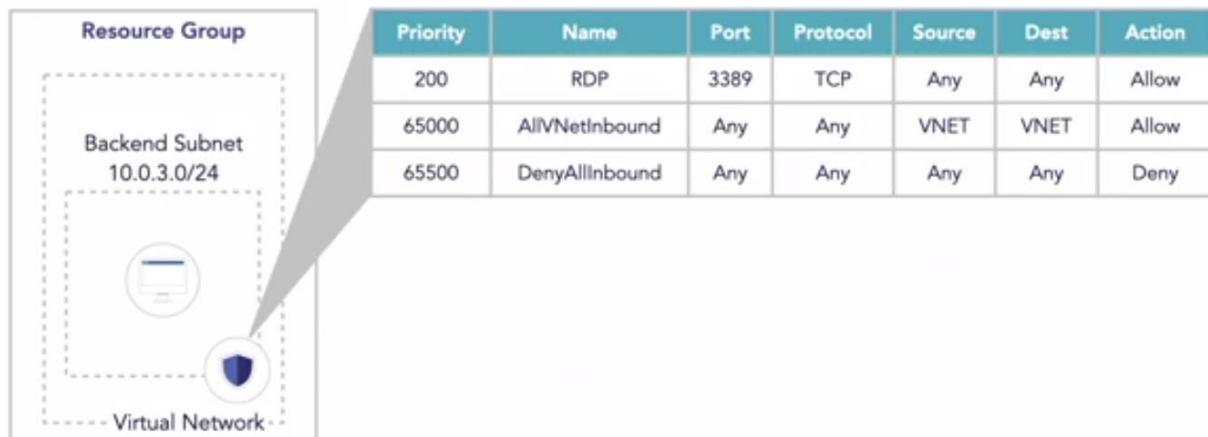
## Network security groups

09/08/2020 • 9 minutes to read •    

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains [security rules](#) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

- Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic.
-

# Network Security Groups



## ExamRef Key Points

- NSG security rules are evaluated by their priority, and each is identified with a number between 100 and 4096, where the lowest numbers are processed first.
- The security rules use 5-tuple information (source address, source port, destination address, destination port, and protocol) to allow or deny the traffic.
- When the traffic is evaluated, a flow record is created for existing connections and the communication is allowed or denied based on the connection state of the flow record.
- You can compare this type of configuration to the old VLAN segmentation that was often implemented with on-premises networks.
- When planning your VNets, consider that each VNet may only have one virtual network gateway of each type, and the gateway type may only be VPN or ExpressRoute.
- Use VPN when you need to send encrypted traffic across the public Internet to your on-premises resources.
- Azure Bastion is a platform-managed PaaS service that can be provisioned in a VNet.
- ExpressRoute allows Contoso to extend its on-premises networks into the Microsoft cloud (Azure or Office 365) over a private connection because ExpressRoute does not go over the public Internet.

<https://learning.oreilly.com/library/view/Exam+Ref+AZ-500+Microsoft+Azure+Security+Technologies/9780136789000/ch02.xhtml#ch02lev1sec1>

## 9. Azure Key Vault

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.

User1:

	▼
A key vault access policy	
Azure Information Protection	
Azure Policy	
Managed identities for Azure resources	
RBAC	

User2:

	▼
A key vault access policy	
Azure Information Protection	
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.

## Skill 4.3: Configure and Manage Key Vault

<https://learning.oreilly.com/library/view/Exam+Ref+AZ-500+Microsoft+Azure+Security+Technologies/9780136789000/ch04.xhtml#ch04lev1sec3>

### Key Points

## Manage access to Key Vault

- Key vault can be thought of as a cloud hardware security module (HSM)
- You can use Azure Key Vault to securely store encryption keys and secrets, including certificates, database connection strings, and virtual machine passwords.
- You manage Key Vault access at the management plane and at the data plane.
- The management plane contains the tools you use to manage Key Vault, such as the Azure portal, Azure CLI, and Cloud Shell.
- When you control access at the management plane, you can configure who can access the contents of the Key Vault at the data plane.
- From the Key Vault perspective, the data plane involves the items stored within Key Vault, and access permissions allow the ability to add, delete and modify certificates, secrets, and keys.
- Microsoft recommends that you use separate Key Vaults for development, preproduction, and production environments.

## Key Vault firewalls and virtual networks

## Manage permissions to secrets, certificates, and keys

You use Key Vault access control policies to manage permissions to secrets, certificates, and keys at the data plane level.

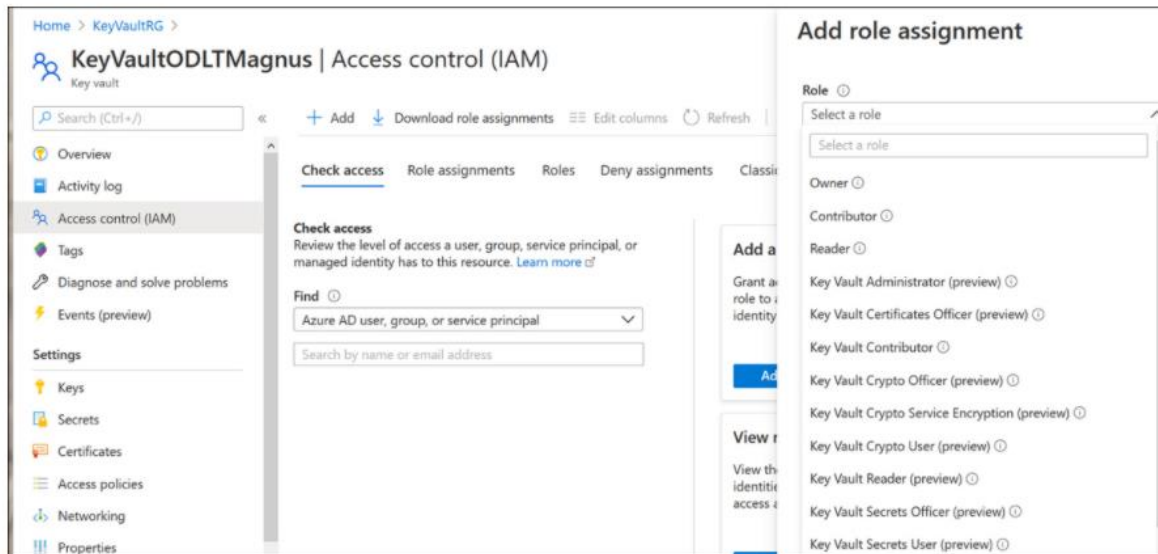
Each Key Vault access control policy includes entries specifying what access the designated security principal has to keys, secrets, and certificates.

An access policy entry grants a distinct set of permissions to a security principal. A security principal can be a user, service principal, managed identity, or group. Microsoft recommends assigning permissions to groups and then adding and removing users, service principals, and managed identities to and from those groups as a way of granting or revoking permissions.

Key Vault access policies don't allow you to configure granular access to specific keys, secrets, or certificates. You can only assign a set of permissions at the keys, secrets, or certificates levels. If you need to allow a specific security principal access to only some and not all keys, secrets, or certificates. Instead, you should store those keys, secrets, or certificates in separate Key Vaults. For example, if there are three secrets that you need to protect using Key Vault, and one user should only have access to two of those secrets, you'll need to store the third of those secrets in a separate Key Vault from the first two.

## Configure RBAC usage in Azure Key Vault

RBAC allows you to secure Azure Key Vault at the management plane. In mid-2020, Microsoft introduced a new set of RBAC roles that provide a simplified way of assigning permissions to the contents of Key Vaults. Going forward, you should only configure access policies when you need to configure complex permissions that are not covered by the new RBAC roles.



**Figure 4-34** Add Role Assignment

### Creating and importing certificates.

You can add certificates to Key Vault by importing them or generating them using the Key Vault. When generating certificates, you can have the certificate self-signed or have it be generated as part of a trust chain from a trusted CA provider.

### Manage Secrets

Secrets, in the context of Azure KeyVault, allow you to securely store items such as passwords and database connection strings. Key Vault automatically encrypts all stored secrets. This encryption is transparent. The Key Vault will encrypt a secret when you add it, and it decrypts the secret when an authorized user accesses the secret from the vault. Each Key Vault encryption key is unique to an Azure Key Vault.

Key Vault secrets are stored with an identifier and the secret itself. When you want to retrieve the secret, you specify the identifier in the request to the Key Vault. You can add a secret to a Key Vault using the `az keyvault secret set` command.

### Backup and restore of Key Vault items

## References

[AZ-500: Course 2: Implement Platform Protection](#)

ExamRef: Create a Virtual Network

Figure 2-5: Create a Virtual Network

Home > Virtual networks > Create virtual network

### Create virtual network

✓ Validation passed

Basics IP Addresses Security Tags Review + create

**Basics**

Subscription	Visual Studio Ultimate with MSDN
Resource group	ContosoCST
Name	AZ500VNet
Region	West US 2

**IP addresses**

Address space	10.3.0.0/16
Subnet	AZ500Subnet (10.3.0.0/24)

**Tags**

None

**Security**

BastionHost	Disabled
DDoS protection plan	Basic
Firewall	Disabled

<https://learning.oreilly.com/library/view/Exam+Ref+AZ-500+Microsoft+Azure+Security+Technologies/9780136789000/ch02.xhtml#ch02lev1sec1>

## Key Points

In Azure, the routing table is automatically created for each subnet within an Azure VNet.

## ExamRef Summaries

### Chapter 4: Secure Data and Applications Summary

There are two storage account access keys that can be used to provide access to a storage account. You should only use one at a time so that you can perform key rotation on a regular basis:

Shared Access Signatures (SAS) allow you to provide secure granular delegated access to storage accounts.

Stored access policies allow you to specifically control service-level shared access signatures.

Rather than rely upon storage account keys or shared access signatures, you can use Azure AD to authorize access to Blob and Queue Storage. Azure AD authenticates a security principal's identity and then returns an OAuth 2.0 token.

When you enable AD DS authentication for Azure Files, your Active Directory Domain Services (AD DS) domain joined computers can mount Azure File Shares using AD DS user credentials.

You configure share-level permission by assigning RBAC roles at the Azure File Share-level. Once you have assigned share-level permissions to an Azure File Share using RBAC, you should then configure file and folder permissions on the contents of the share.

Azure Storage encryption is enabled by default for all storage accounts regardless of performance tier or access tier. This means you don't have to modify code or applications for Azure Storage Encryption to be enabled.

Encryption scopes allow you to configure separate encryption keys at the container and blob level.

Advanced threat protection for Azure Storage allows you to detect unusual and malicious attempts to interact with Azure Storage accounts.

When you create an Azure SQL database server instance, you create an administrator login and a password associated with that login. This administrative account granted full administrative permissions on all databases hosted off the Azure SQL instance as a server-level principal.

Auditing allows you to track database events, such as tables being added or dropped. Audit logs for Azure SQL databases can be stored in an Azure Storage account, a Log Analytics workspace, or Event Hubs.

Azure SQL Database Advanced Threat Protection allows you to detect unusual activity that might indicate that a third party might be trying to attack your organization's Azure SQL databases.

Transparent data encryption (TDE) allows you to protect Azure SQL databases by encrypting data at rest. When you enable TDS, the databases, associated backups, and transaction log files are automatically encrypted and decrypted, as necessary.

Always Encrypted is a technology available for Azure SQL that allows you to protect specific types of sensitive data that has a known recognizable pattern, such as passport numbers, tax file identification numbers, and credit card numbers.

Azure Key Vault allows you to store information that should not be made public, such as secrets, certificates, and keys.

You use Key Vault access control policies to manage permissions to secrets, certificates, and keys at the data plane level. Each Key Vault access control policy includes entries specifying what access the designated security principal has to keys, secrets, and certificates.