AZ-500 Exam Topics Review Questions – updated 6-18-21

Updated: 6/18/2021

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

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.

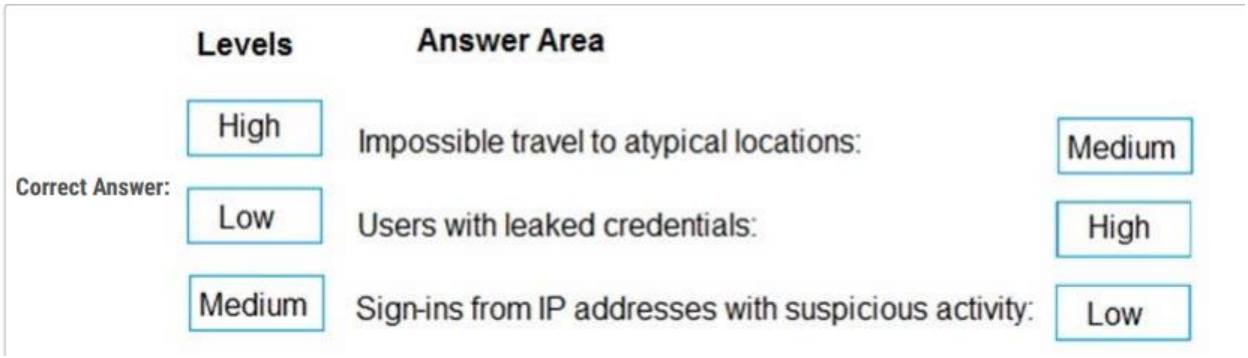
You need to identify the risk level of the following risk events:

☞ 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?



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 -

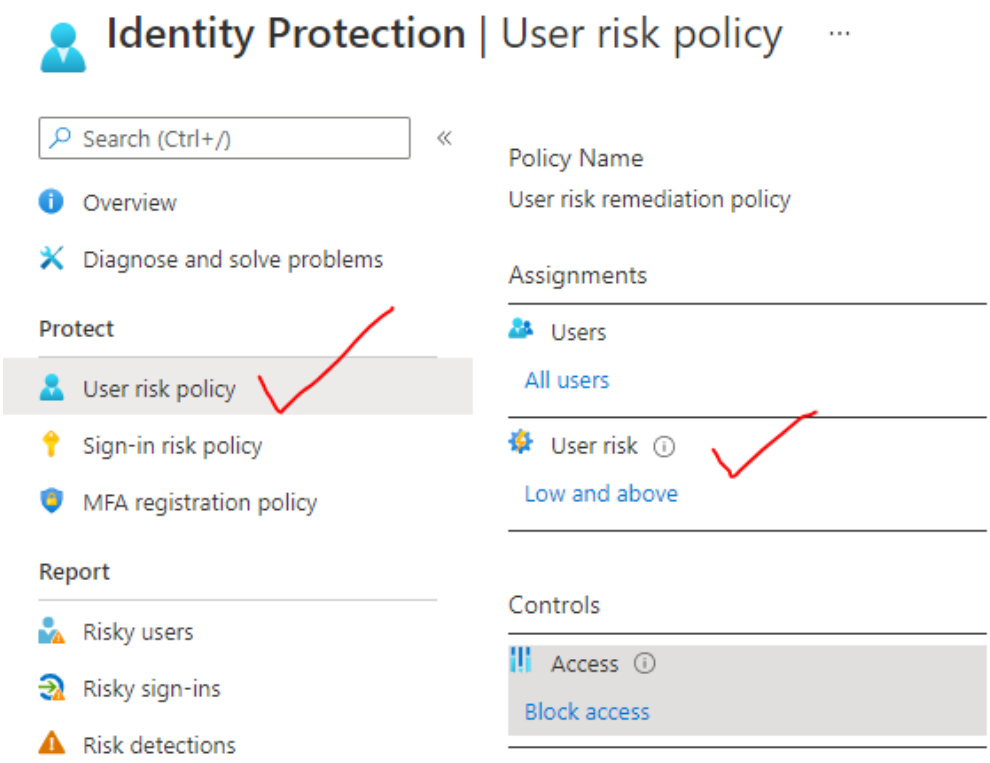
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

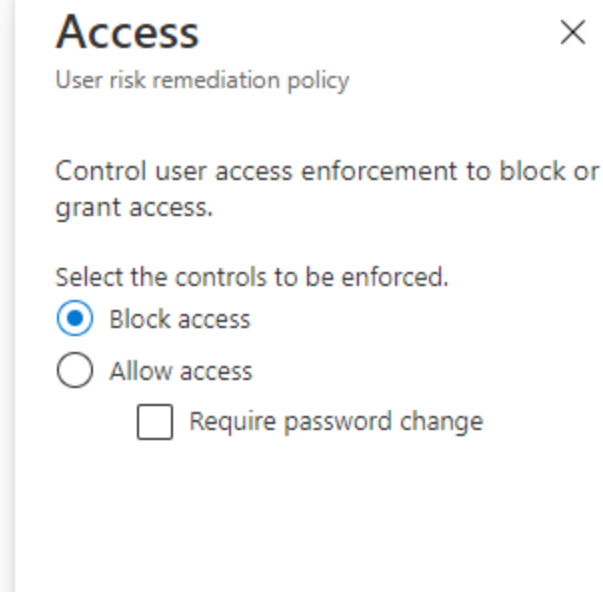
Box 2: Yes -

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.

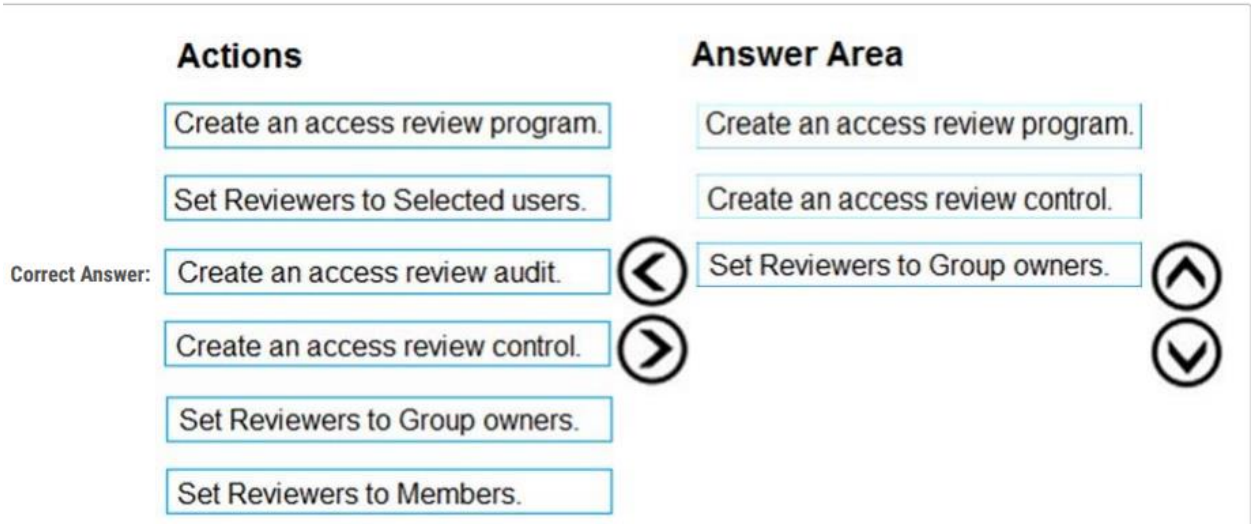




9. Access Review

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.

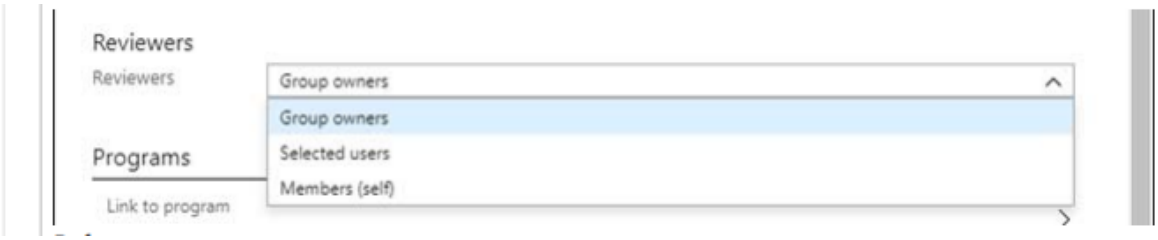


Step 1: Create an access review program

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

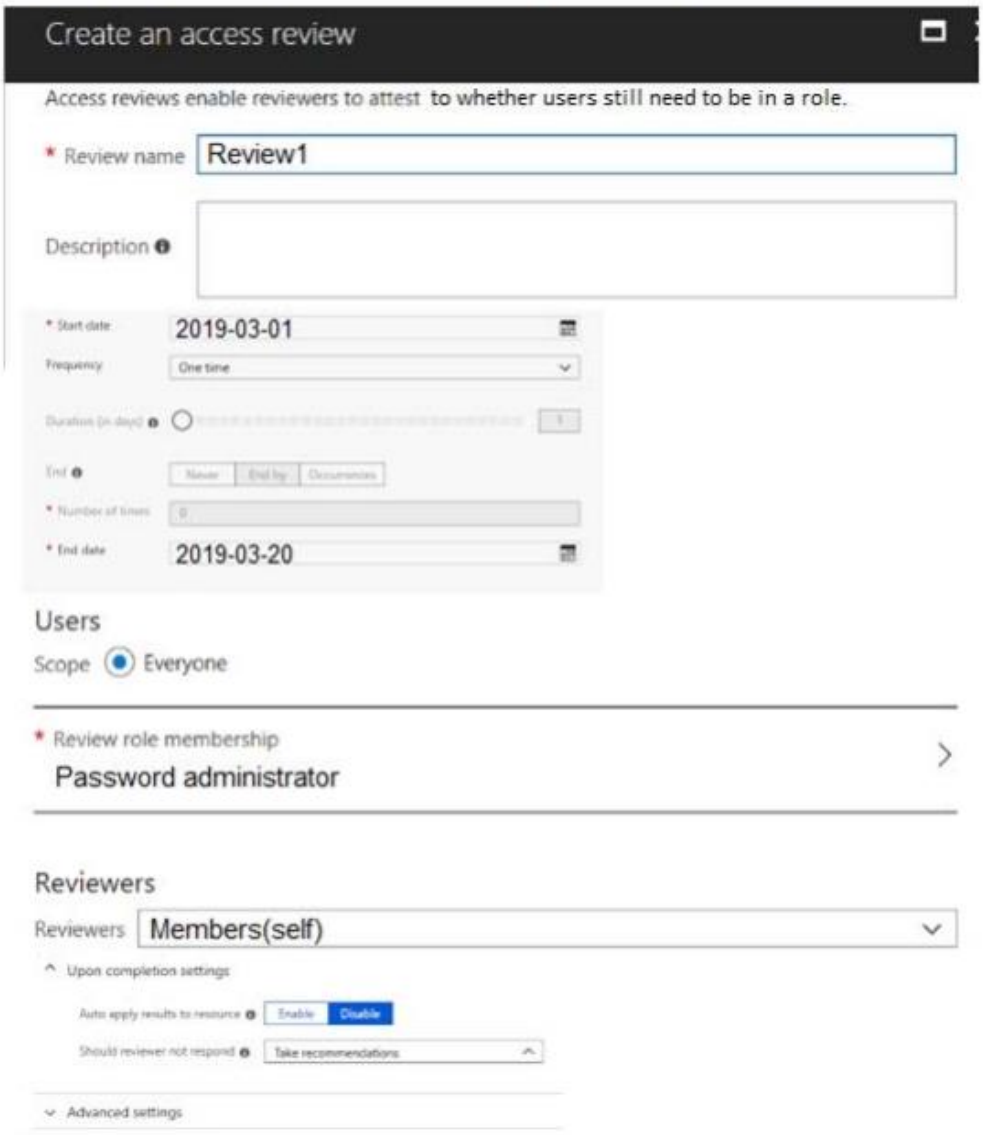
https://docs.microsoft.com/en-us/azure/activedirectory/governance/manage-programs-controls

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.



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

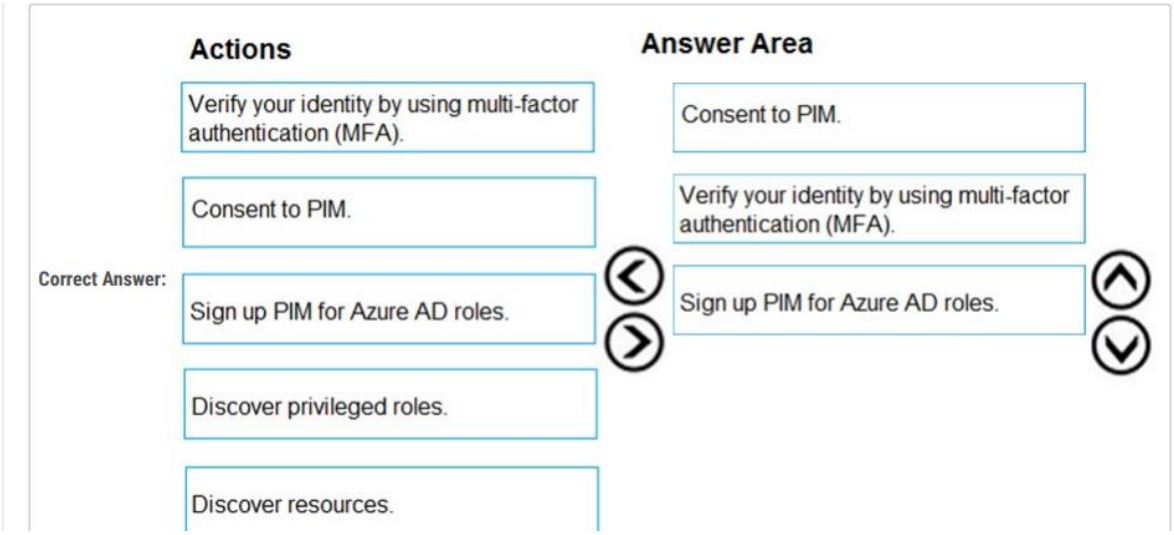
References:

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

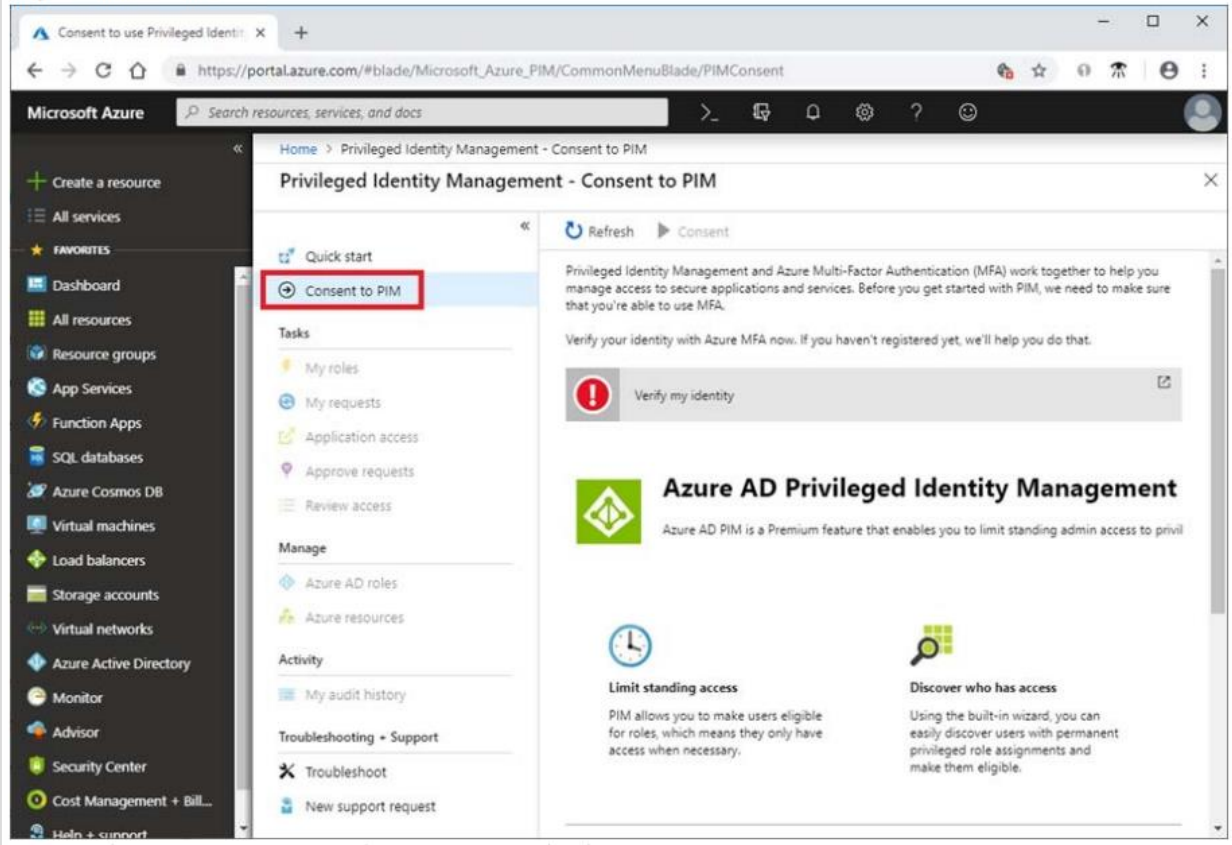
11. Privileged Identity Management (PIM)

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.



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

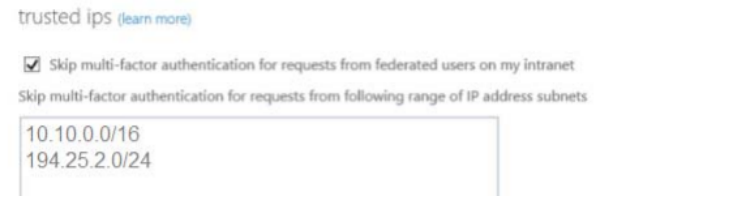
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

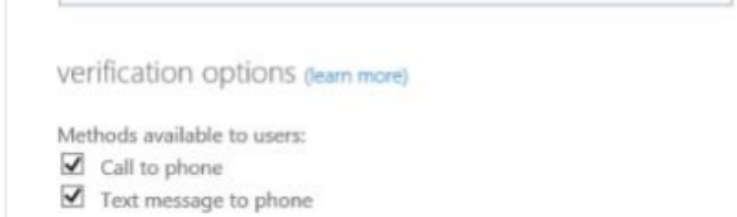
Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

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.)





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.

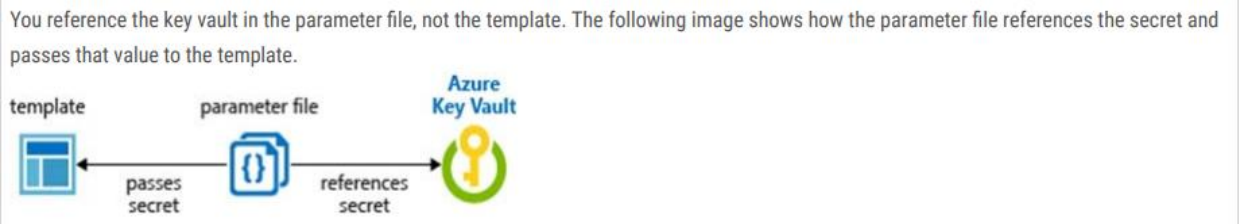
References: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-congure

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.

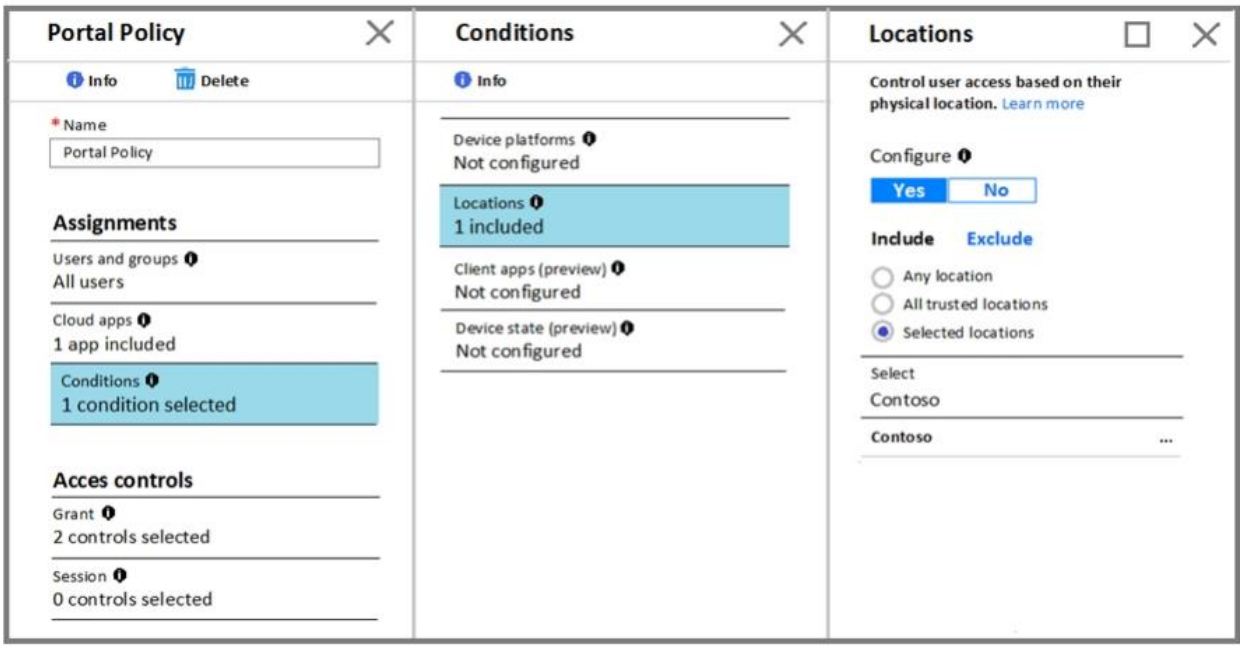
What should you use to construct the resource ID?



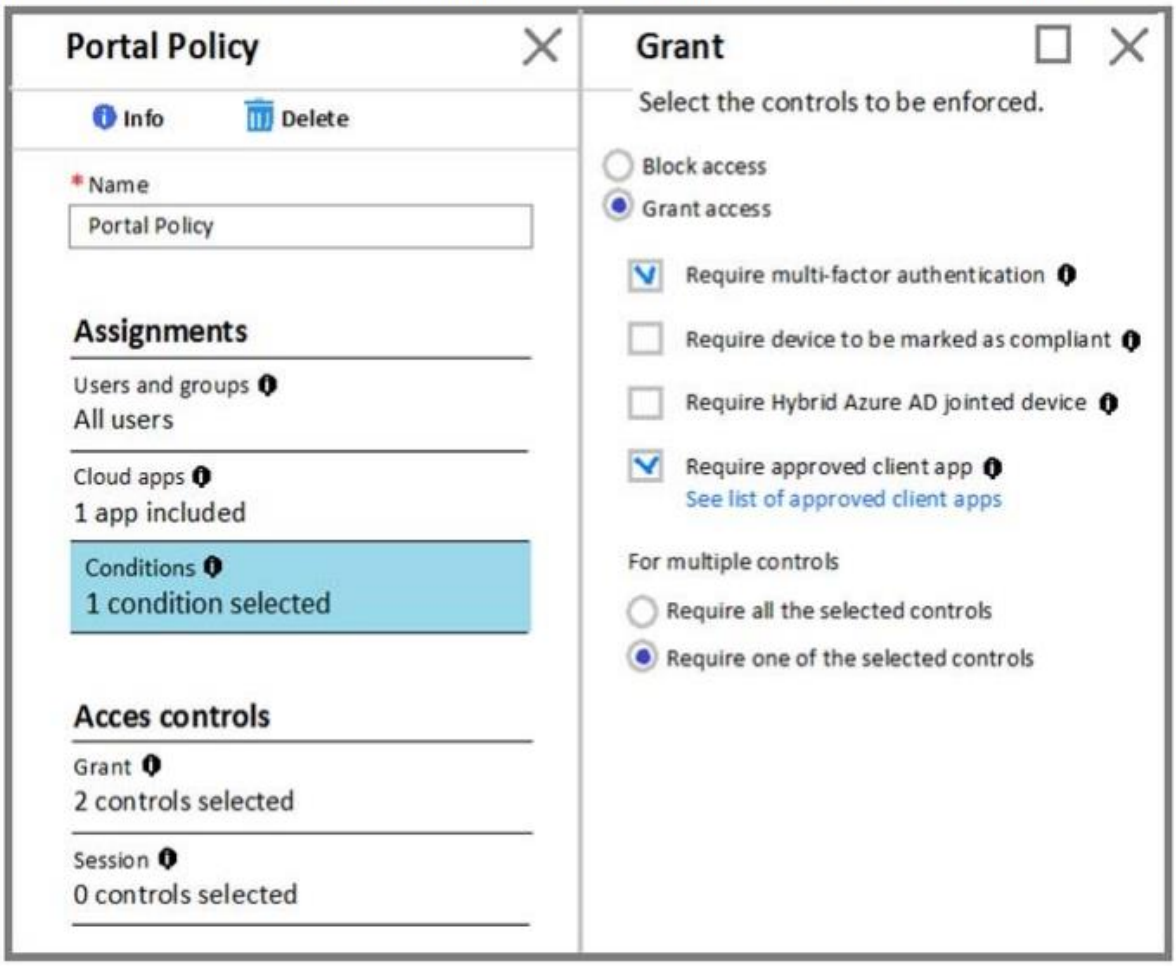
Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter

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.)



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



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

Configure security settings by using Azure Blueprint

https://learning.oreilly.com/library/view/exam-ref-az-500/9780136789000/ch03.xhtml

Azure Blueprints enable you to define a repeatable set of Azure resources that implement and adhere to an organization's standards, patterns, and requirements. It is very important for you to understand **when to use a blueprint instead of a policy**. Blueprints are used to orchestrate the deployment of various resource templates and other artifacts, such as role assignments, policy assignments, Azure Resource Manager templates, and resource groups.

The main difference between a blueprint and a policy is that a blueprint is a package for composing focus-specific sets of standards, patterns, and requirements related to the implementation of Azure cloud services, security, and design.

Another characteristic of the blueprint is that you can reuse them to maintain consistency and compliance. A policy can be included in this package as an artifact for the blueprint.

Both can be utilized in scenarios where you have multiple subscriptions and want to maintain governance. From the lifecycle perspective, a blueprint has these major stages:

Follow these steps to create a new blueprint and publish it:

- Navigate to the Azure portal at https://portal.azure.com
- In the search bar, type blueprint, and under Services, click Blueprints.

Topic 2 – Question set 2

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

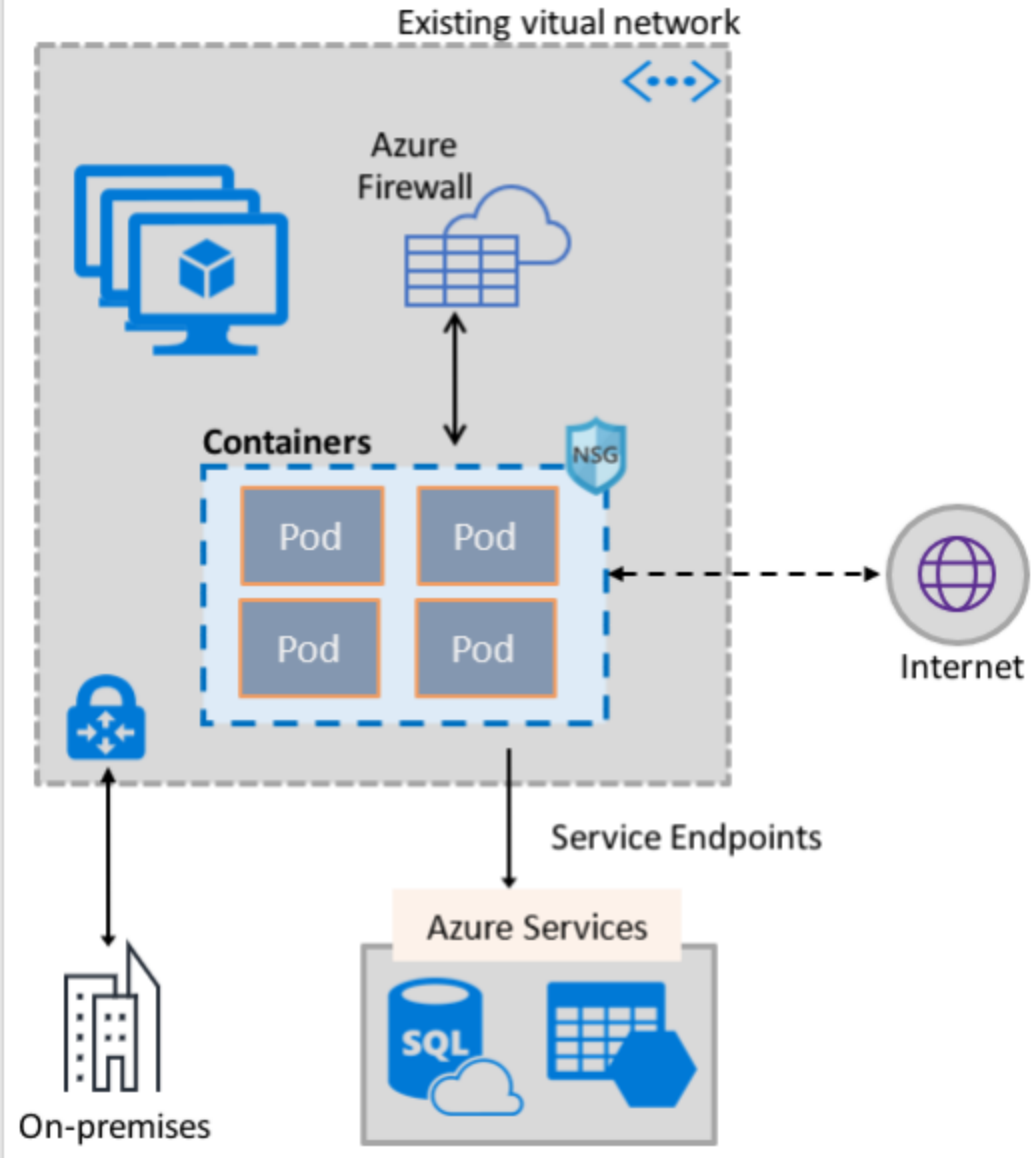
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

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.

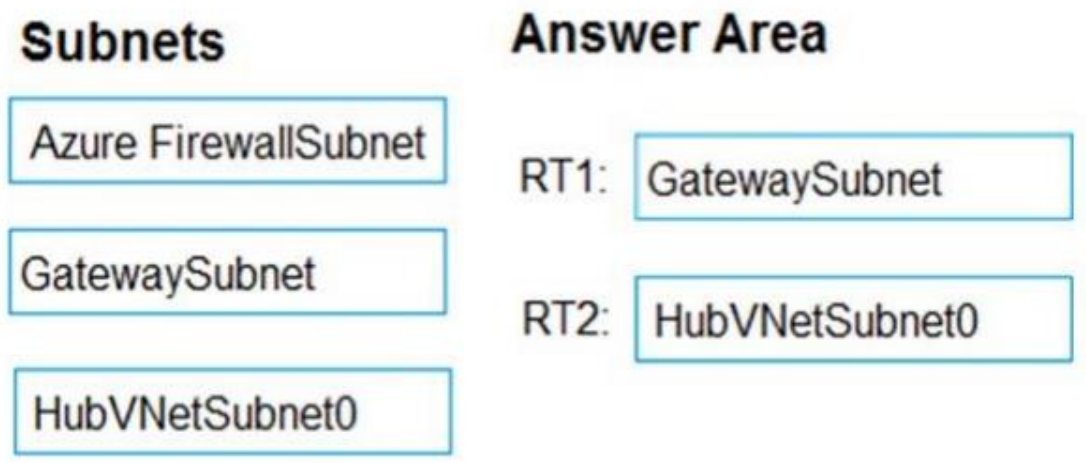
You create the following two routing tables:

- 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

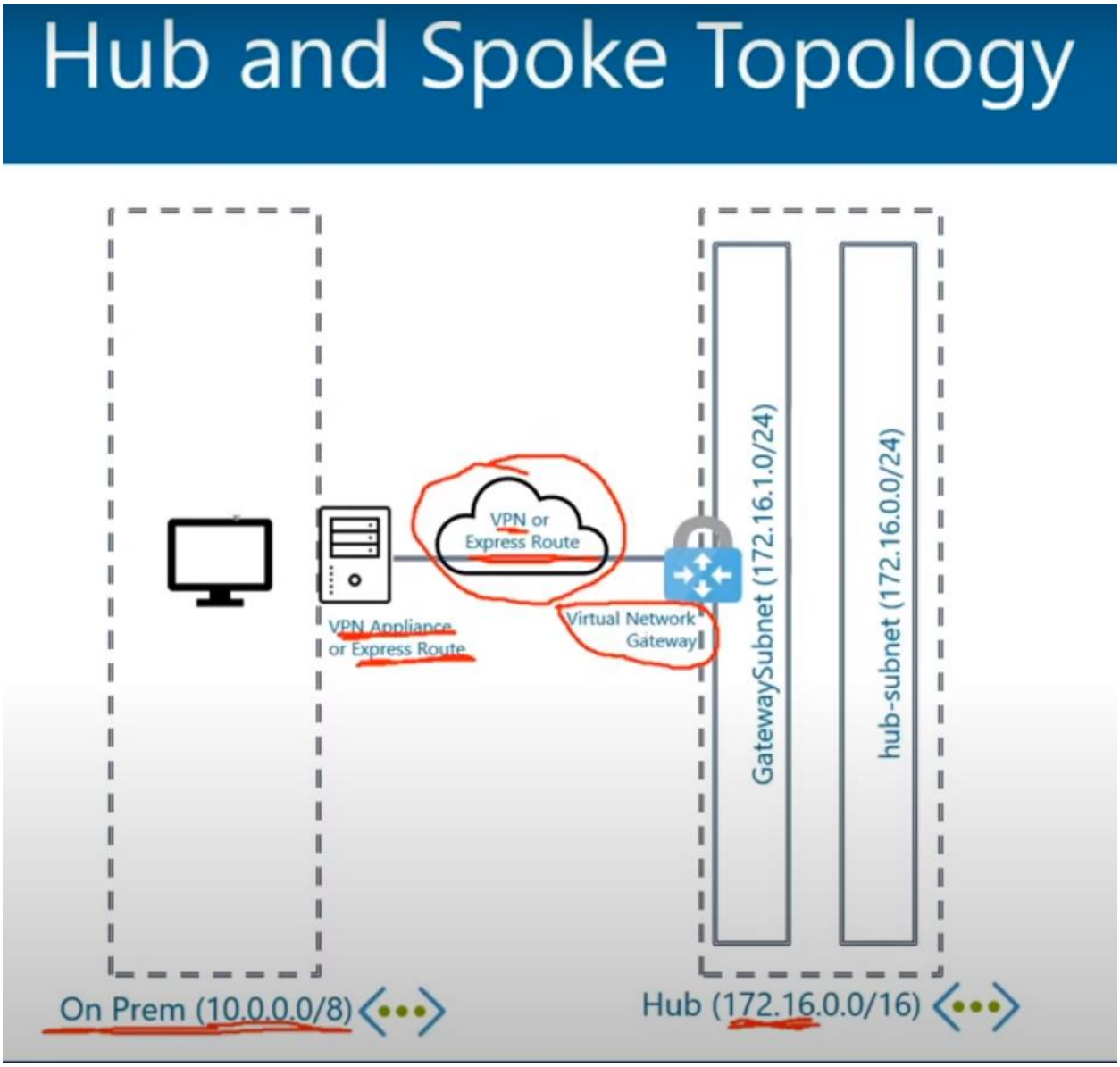
You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

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.

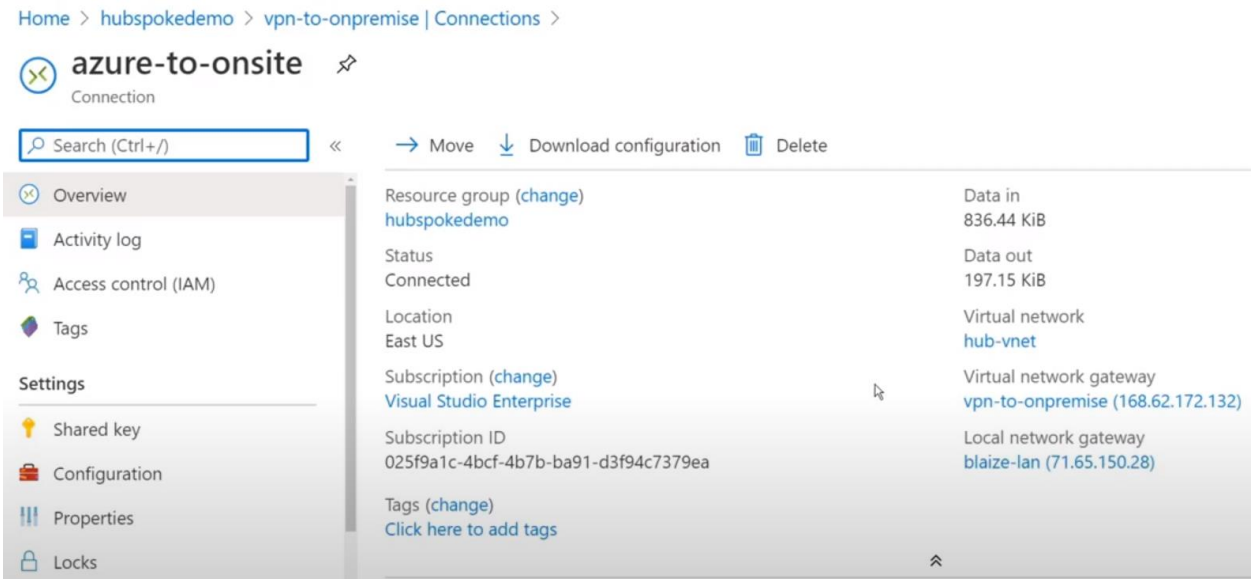
NOTE: Each correct selection is worth one point.



Hub and Spoke Topology

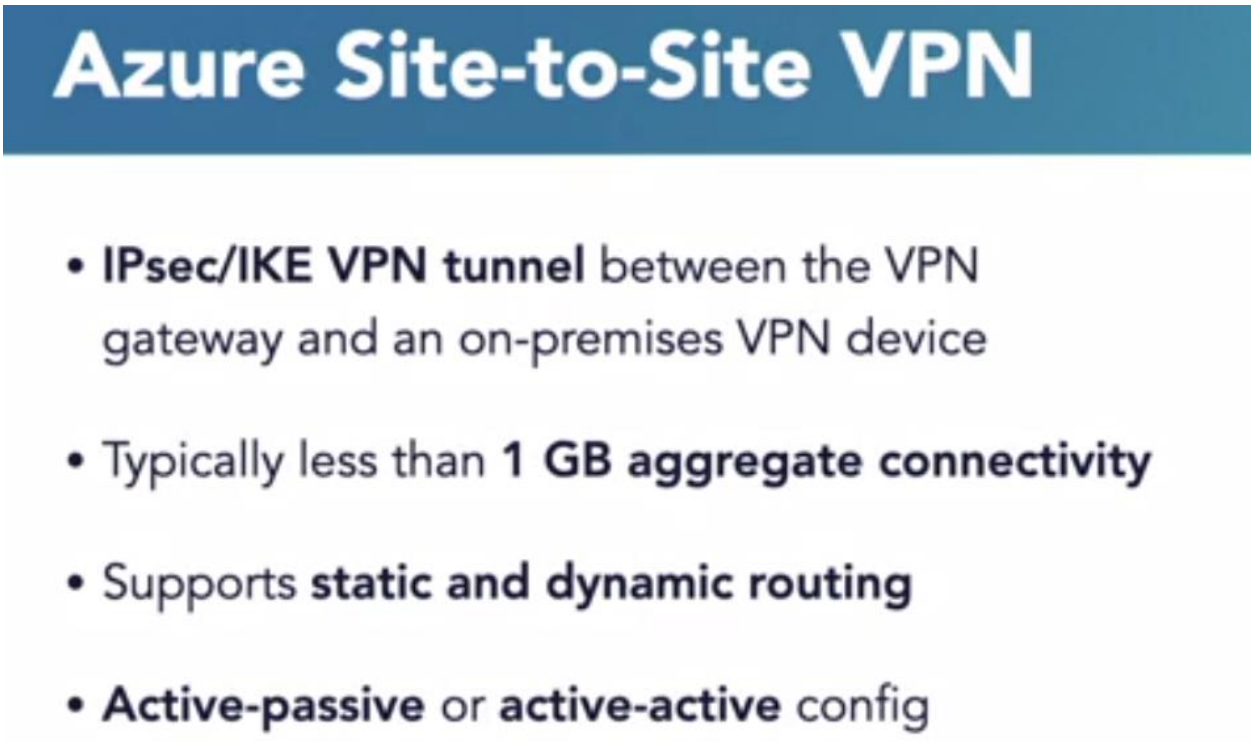


Azure -to-Onsite VPN

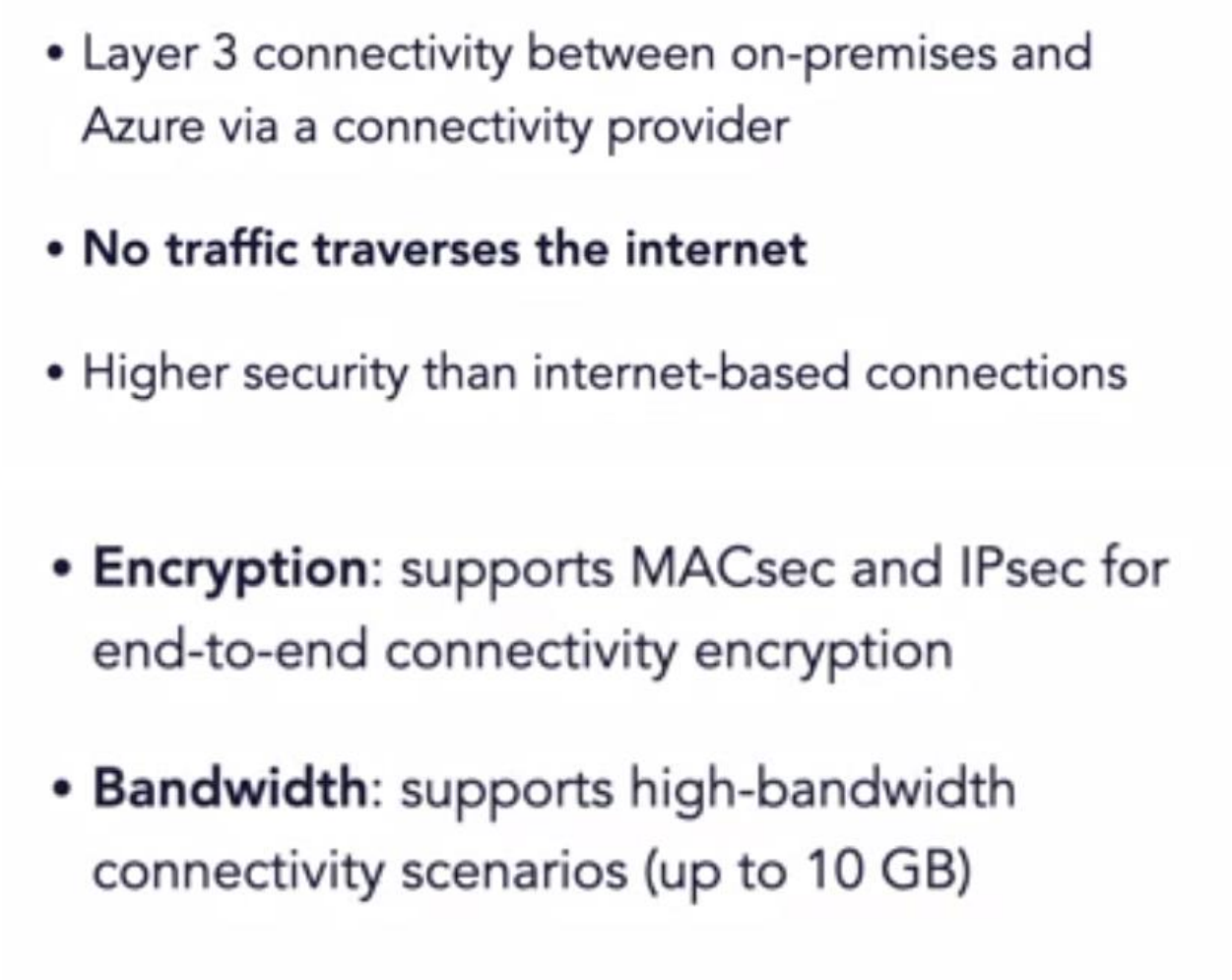


Tutorial: Setting Up HUB and SPOKE NETWORKS on AZURE

https://www.youtube.com/watch?v=j8meGy_mc1s



Azure ExpressRoute



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.

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

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

Authentication Options for ACR

Method	How to Authenticate
Individual AD identity	`az acr login` in Azure CLI
AD service principal	`docker login` `az acr login` in Azure CLI
Integrate with AKS	Attach registry when AKS cluster created or updated
Managed identity for Azure resources	`docker login` `az acr login` in Azure CLI
Admin user	`docker login`
Repository scoped access token	`docker login` `az acr login` 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.	○	○
You can start VM2.	○	○
You can create a virtual machine in RG2.	○	○

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

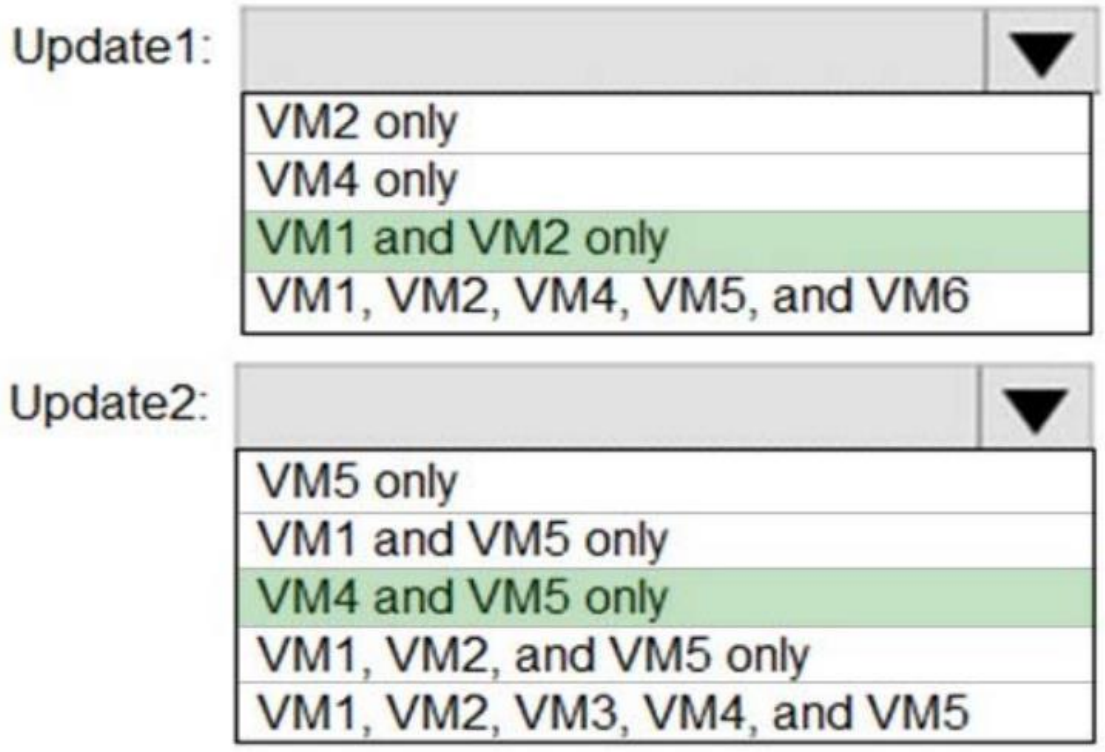
7. Azure update management

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: 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.

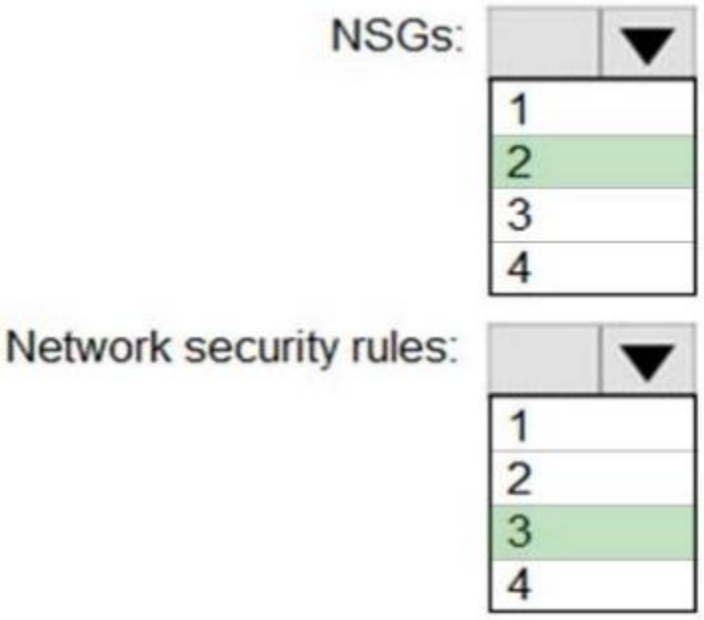
Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

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.



- 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?

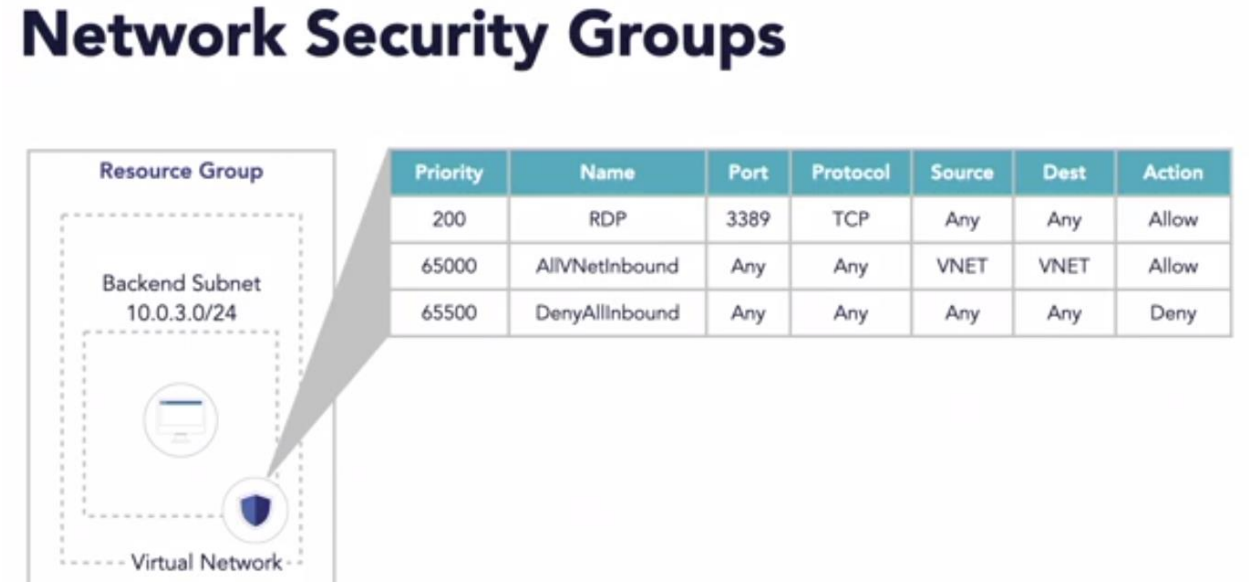
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

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.
-



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

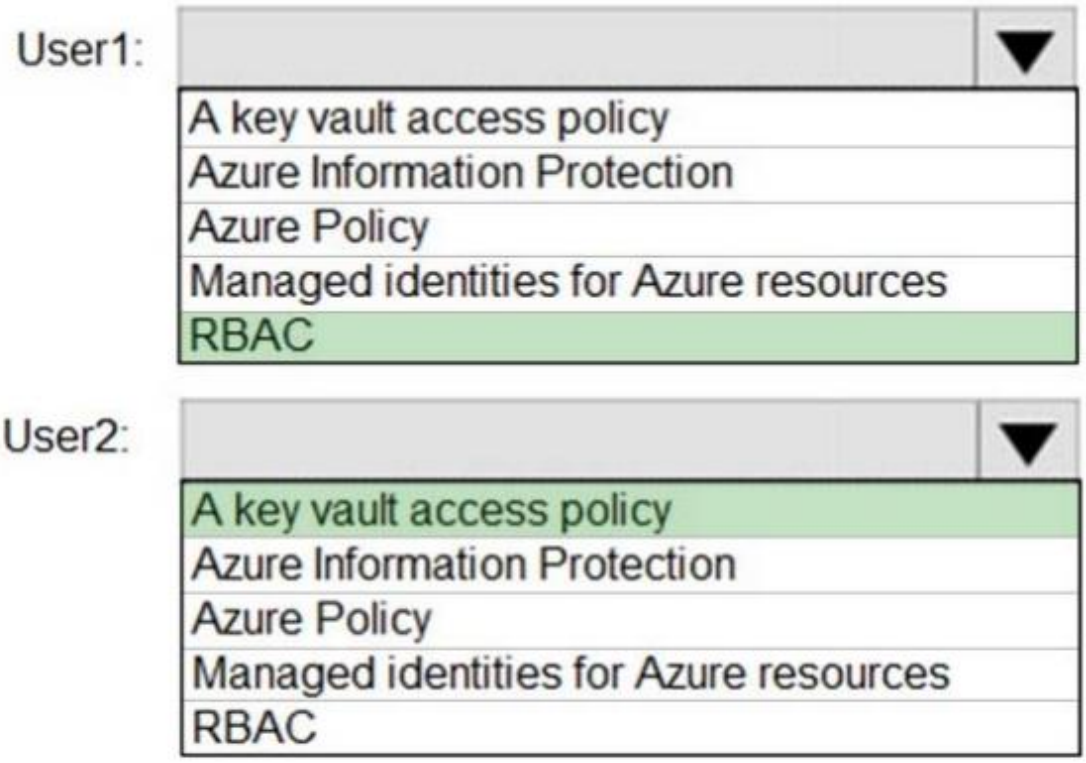
9. Azure Key Vault

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: 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.

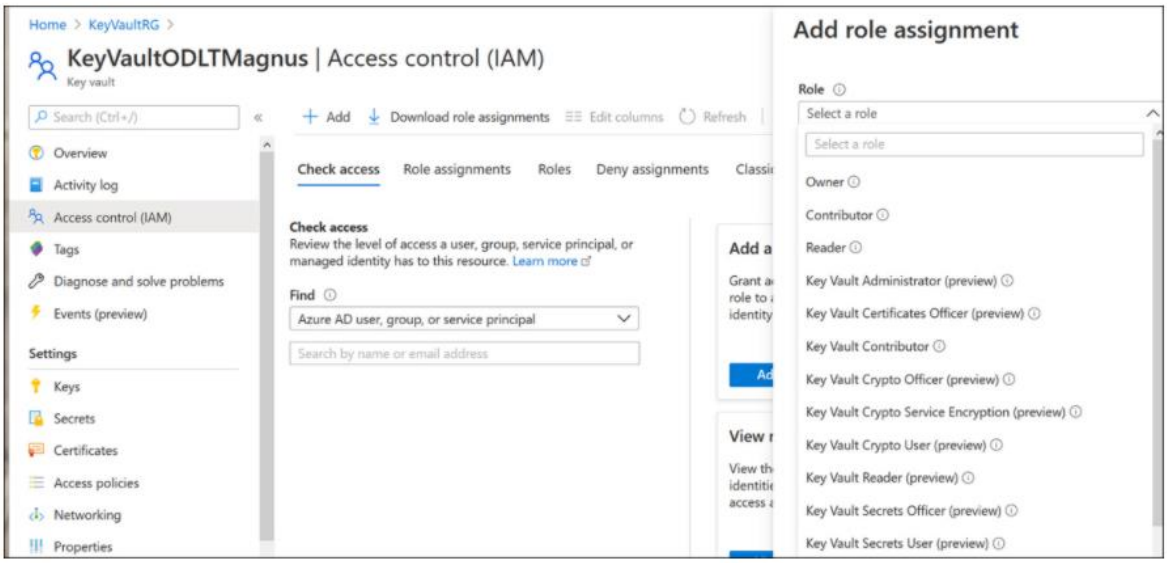


Figure 4-34 Add Role Assignment

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

10. Azure Disk Encryption

You have two Azure virtual machines in the East US2 region as shown in the following table.

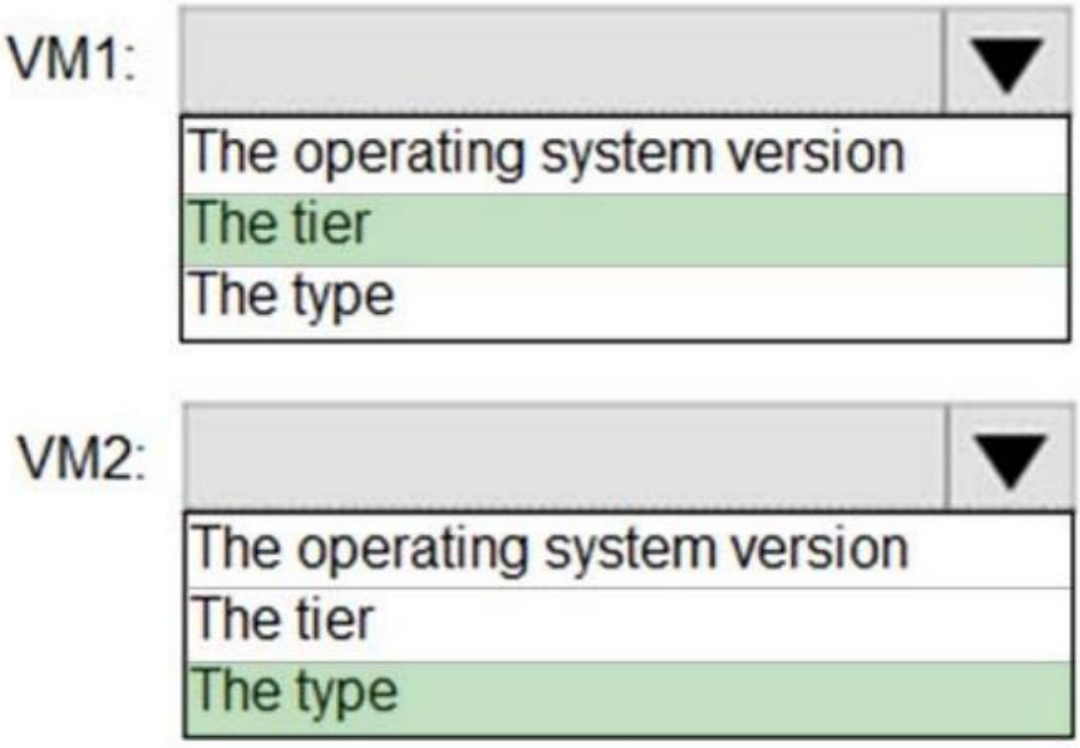
Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



VM1: The Tier -

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: The type -

Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.

Not the operating system version: Ubuntu 16.04 is supported.

References:

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

https://docs.microsoft.com/enus/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport

Implement Azure disk encryption

Data encryption at rest is an extremely important part of your overall VM security strategy. Security Center will even trigger a security recommendation when a VM is missing disk encryption. You can encrypt your Windows and Linux virtual machines' disks using Azure Disk Encryption (ADE). For Windows OS, you need Windows 8 or later (for client) and Windows Server 2008 R2 or later (for servers).

ADE provides operating system and data disk encryption. For Windows, it uses BitLocker Device Encryption; for Linux, it uses the DM-Crypt system.

ADE is not available in the following scenarios:

- Basic A-series VMs
- VMs with a less than 2 GB of memory
- Generation 2 VMs and Lsv2-series VMs
- Unmounted volumes

ADE requires that your Windows VM has connectivity with Azure AD to get a token to connect with Key Vault. At that point, the VM needs access to the Key Vault endpoint to write the encryption keys, and the VM also needs access to an Azure storage endpoint. This storage endpoint will host the Azure extension repository as well as the Azure storage account that hosts the VHD files.

Group policy is another important consideration when implementing ADE. If the VMs for which you are implementing ADE are domain joined, make sure to not push any group policy that enforces Trusted Platform Module (TPM) protectors. In this case, you will need to make sure that the Allow BitLocker Without A Compatible TPM policy is configured. Also, BitLocker policy for domain-joined VMs with custom group policy must include the following setting: Configure User Storage Of BitLocker Recovery Information / Allow 256-Bit Recovery Key.

Because ADE uses Azure Key Vault to control and manage disk encryption keys and secrets, you need to make sure Azure Key Vault has the proper configuration for this implementation.

When you need to encrypt both data and OS volumes where the root (/) file system usage is 4 GB or less, you will need to have at least 8 GB of memory. However, if you need to encrypt only the data volume, the requirement drops to 2 GB of memory. The requirement doubles if Linux systems are using a root (/) file system greater than 4 GB, which means that the minimum memory requirement is root file system usage * 2.

Assuming that you have the right prerequisites in place to implement ADE, you can use the Set-AzVmDiskEncryptionExtension PowerShell cmdlet to implement the encryption in a VM, as shown in the following example:

$AKeyVault = Get-AzKeyVault -VaultName MyAKV -ResourceGroupName MyRGSet-AzVMDiskEncryptionExtension -ResourceGroupName MyRG -VMName MyVM-DiskEncryptionKeyVaultUrl $AKeyVault.VaultUri -DiskEncryptionKeyVaultId $AKeyVault.ResourceId

11. Azure Log Analytics

You have an Azure virtual machines shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.

Which virtual machines can be enrolled in Analytics1?

- VM1 Only

A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location.

VM4 is a different resource group.

Configure diagnostic logging and log retention

https://learning.oreilly.com/library/view/exam-ref-az-500/9780136789000/ch03.xhtml

In Azure, each resource requires its own diagnostic setting. In these settings, you define the categories of logs and metric data that should be sent to the destinations defined in the setting. Also, you need to define the destination of the log, which includes sending it to the Log Analytics workspace, Event Hubs, and Azure Storage.

LinkedIn: Monitor security logs by using Azure Monitor

https://www.linkedin.com/learning/microsoft-azure-security-technologies-az-500-cert-prep-3-manage-security-operations-2/monitor-security-logs-by-using-azure-monitor?contextUrn=urn%3Ali%3AlyndaLearningPath%3A5ece9607498e01c03163ea39&u=86261762

12. Azure Kubernetes Service (AKS) Cluster

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the tab.)

BASICS

Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled
AUTHENTICATION	
Enable RBAC	No
NETWORKING	
HTTP application routing	Yes
Network configuration	Basic
MONITORING	
Enable container monitoring	No
TAGS	

You plan to deploy the cluster to production. You disable HTTP application routing. You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address. What should you do?

- Create an AKS Ingress controller.

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

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

13. Apply policies to multiple subscriptions

You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions. You need to deploy the policy definitions as a group to all three subscriptions. Solution: You create a policy definition and assignments that are scoped to resource groups. Does this meet the goal?

NO

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.

https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

Skill 3.2: Monitor security by using Azure Security Center

In large organizations where it's necessary to have a centralized standard across multiple subscriptions, it is common to use Azure Management Groups to aggregate all subscriptions that share a common set of policies.

Security Center enables you to have a centralized view across multiple subscriptions to ensure you have a better visibility of your cloud security posture. This section of the chapter covers the skills necessary to configure security policies in Security Center according to the Exam AZ-500 outline.

14. Deploy the policy definitions as a group to all three subscriptions

Solution: You create a resource graph and an assignment that is scoped to a management group.

Does this meet the goal? Yes

15. Enable and configure the Microsoft Antimalware service

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016. You need to deploy Microsoft Antimalware to the virtual machines.

- Solution: You add an extension to each virtual machine.

Does this meet the goal? Yes

You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

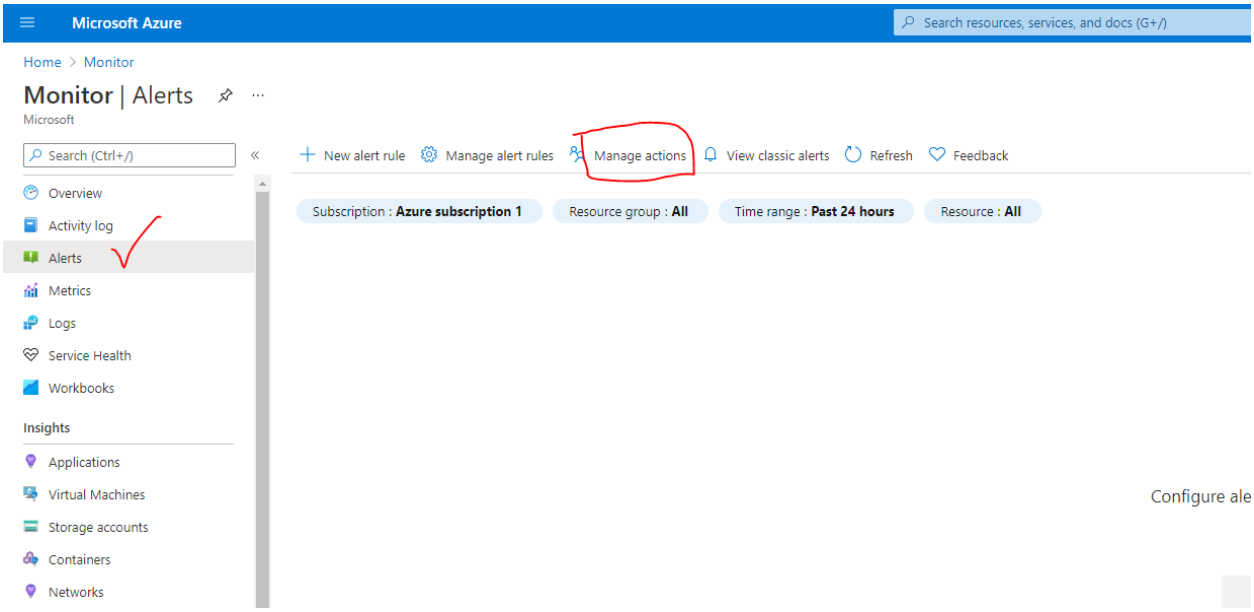
16. Same as 15

References: https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

17. Azure security Center – custom alert rule

You need to configure which users will receive an email message when the alert is triggered. What should you do?

- From Azure Monitor, create an action group.



Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

18. User Define route

You are configuring and securing a network environment. You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic. You need to ensure that all network traffic is routed through VM1.

What should you configure?

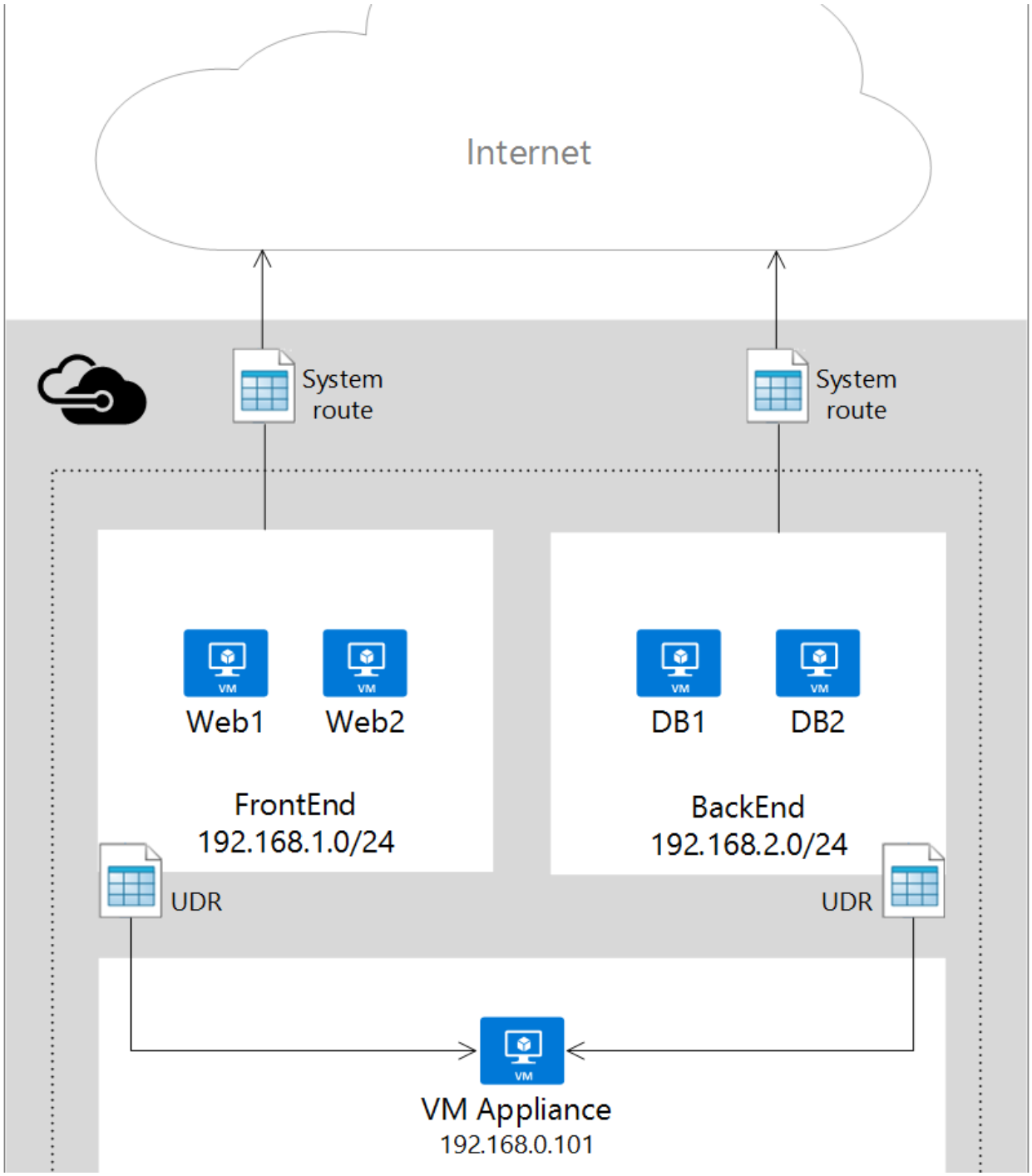
- a user-defined route

Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets owing to a specific subnet to go to your virtual appliance instead and enabling IP forwarding for the VM running as the virtual appliance.

For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

> - Force tunneling to the Internet via your on-premises network.
> - Use of virtual appliances in your Azure environment.
> - In the scenarios above, you will have to create a route table and add user defined routes to it.

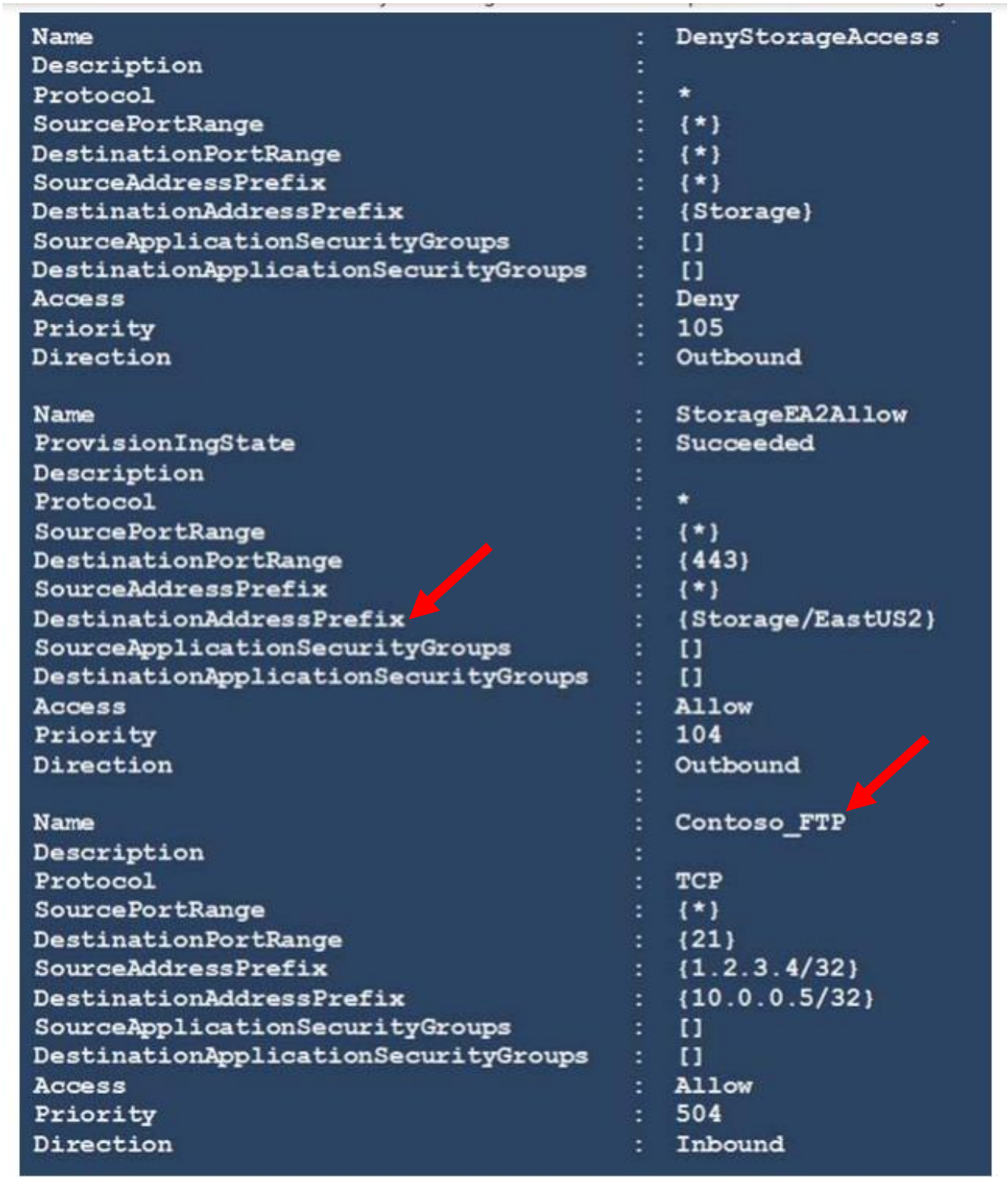
Reference: https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md

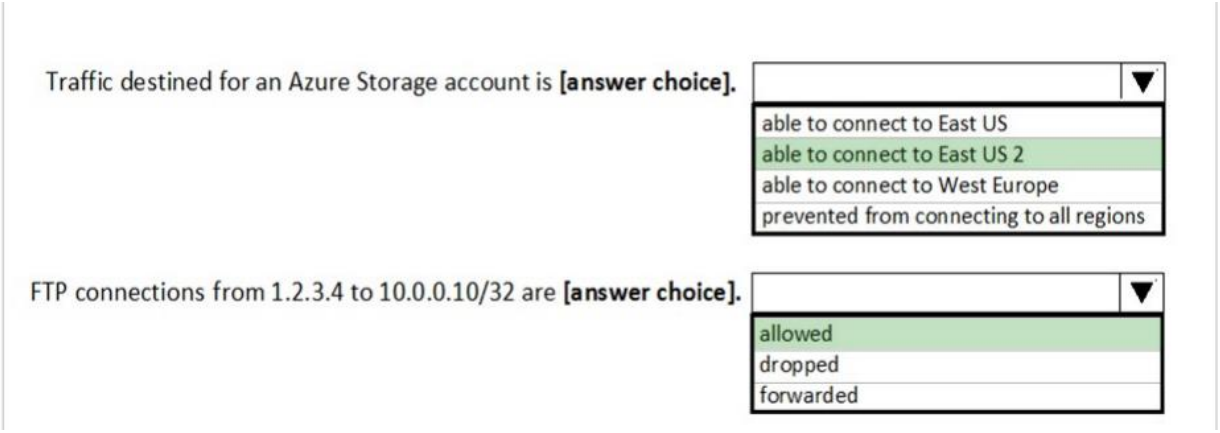


19. NSG

You have a network security group (NSG) bound to an Azure subnet.

You run Get-AzureRmNetworkSecurityRuleCong and receive the output shown in the following exhibit:


Name : DenyStorageAccess
Description :
Protocol : *
SourcePortRange : {*}
DestinationPortRange : {*}
SourceAddressPrefix : {*}
DestinationAddressPrefix : {Storage}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Deny
Priority : 105
Direction : Outbound
Name : StorageEA2Allow
ProvisionIngState : Succeeded
Description :
Protocol : *
SourcePortRange : {*}
DestinationPortRange : {443}
SourceAddressPrefix : {*}
DestinationAddressPrefix : {Storage/EastUS2}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 104
Direction : Outbound
Name : Contoso_FTP
Description :
Protocol : TCP
SourcePortRange : {*}
DestinationPortRange : {21}
SourceAddressPrefix : {1.2.3.4/32}
DestinationAddressPrefix : {10.0.0.5/32}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 504
Direction : Inbound



Reference: https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

The Get-AzureRmNetworkSecurityRuleCong cmdlet gets a network security rule conguration for an Azure network security group. Security rules in network security groups enable you to lter the type of network trac that can ow in and out of virtual network subnets and network interfaces.

20. ASG (Application Security Group)

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

The subscription contains the virtual machines shown in the following table.

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1.

On which other network interfaces can you configure ASG1?

A. NIC2 only

B. NIC2, NIC3, NIC4, and NIC5

C. NIC2 and NIC3 only

D. NIC2, NIC3, and NIC4 only

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

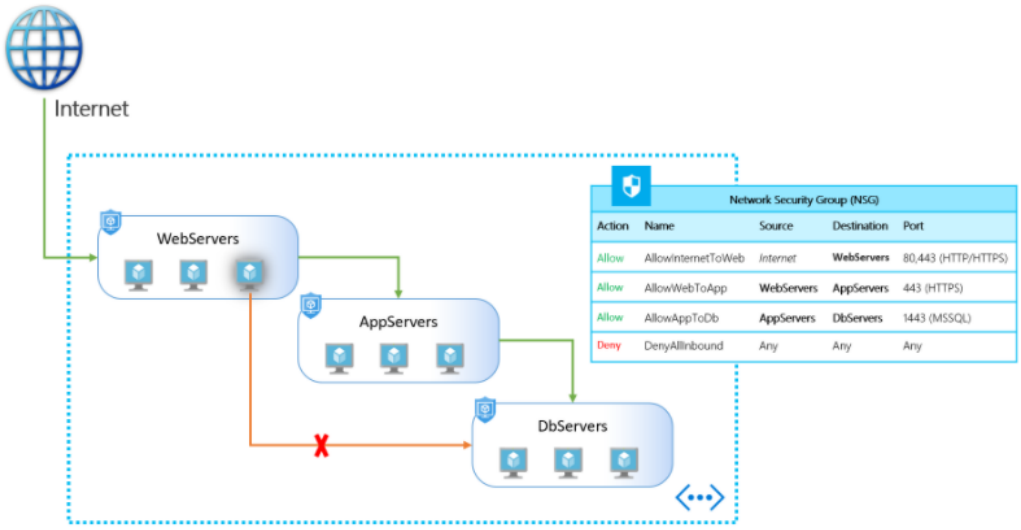
Reference: https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

Application Security Groups now generally available in all Azure regions

Publicado el 5 abril, 2018

Mario Lopez, Program Manager

We are pleased to announce the general availability of Application Security Groups (ASG) in all Azure regions. This feature provides security micro-segmentation for your virtual networks in Azure.



Network security micro segmentation

ASGs enable you to define fine-grained network security policies based on workloads, centralized on applications, instead of explicit IP addresses. Provides the capability to group VMs with monikers and secure applications by filtering traffic from trusted segments of your network.

Implementing granular security traffic controls improves isolation of workloads and protects them individually. If a breach occurs, this technique limits the potential impact of lateral exploration of your networks from hackers.

21. Adaptive application controls

You have 15 Azure virtual machines in a resource group named RG1.
All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines.
What should you do?

A. Apply an Azure policy to RG1.
B. From Azure Security Center, configure adaptive application controls.
C. Configure Azure Active Directory (Azure AD) Identity Protection.
D. Apply a resource lock to RG1.

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware.

Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence. Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

22. Container groups

You plan to deploy Azure container instances.
You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.
The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.
You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.
What should you include in the deployment?

A. application security groups
B. network security groups (NSGs)
C. management groups
D. container groups

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process. Reference: https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

23. Network access in VNETs and Subnets - Review

You create resources in an Azure subscription as shown in the following table.

Name	Type	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
Contoso1901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2

- Subnet1 has a network ID of 10.0.0.0/24
- Subnet2 has a network ID of 10.1.1.0/24

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass              : Logging, Metrics
DefaultAction       : Deny
IpRules             : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                      dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                      virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                                              IpRules

Action  IPAddressOrRange
------  ----------------
Allow   193.77.0.0/16


PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules

Action VirtualNetworkResourceId
------ ---------------                                                    State
 Allow /subscriptions/a90c8c8f-d8bc-4112-abfb dac4906573dd/resourceGroups/     ------
       RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1  Succeeded

PS C:\> _
```

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

NOTE: Each correct selection is worth one point.

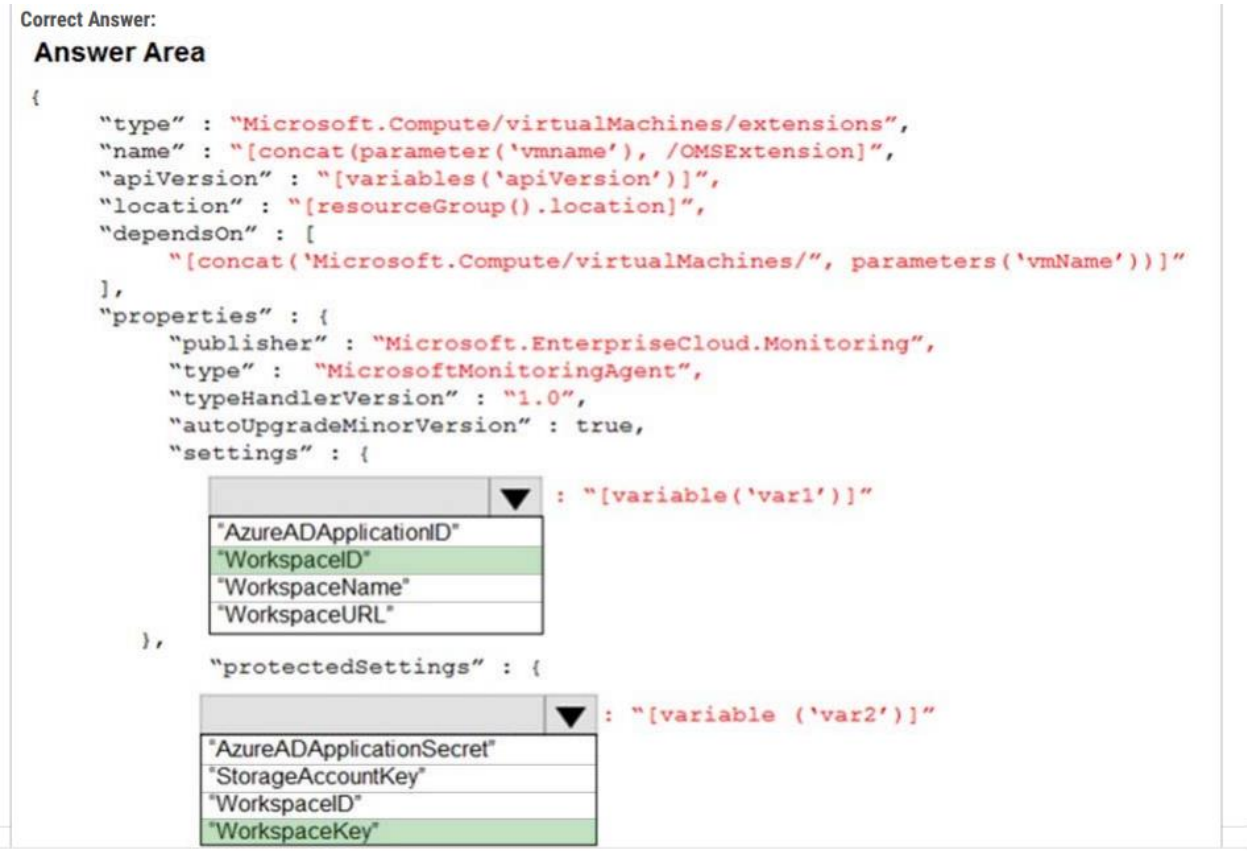
Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	○	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	○
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	○	○

24. Management Groups – same as 14

Topic 3 – Question Set 3

1. Azure Monitor Logs - Review

You plan to use Azure Monitor Logs to collect logs from 200 servers that run Windows Server 2016. You need to automate the deployment of the Log Analytics Agent to all the servers by using an Azure Resource Manager template. How should you complete the template?



2. Custom Sensitive information Type

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.

You need to create a custom sensitivity label. What should you do?

- Create a custom sensitive information type.

First, you need to create a new sensitive information type because you can't directly modify the default rules.

When looking for sensitive information in content, you need to describe that information in what's called a *rule* . Data loss prevention (DLP) includes rules for the most-common sensitive information types that you can use right away. To use these rules, you have to include them in a policy. You might find that you want to adjust these built-in rules to meet your organization's specific needs, and you can do that by creating a custom sensitive information type. This topic shows you how to customize the XML file that contains the existing rule collection to detect a wider range of potential credit-card information.

You can take this example and apply it to other built-in sensitive information types. For a list of default sensitive information

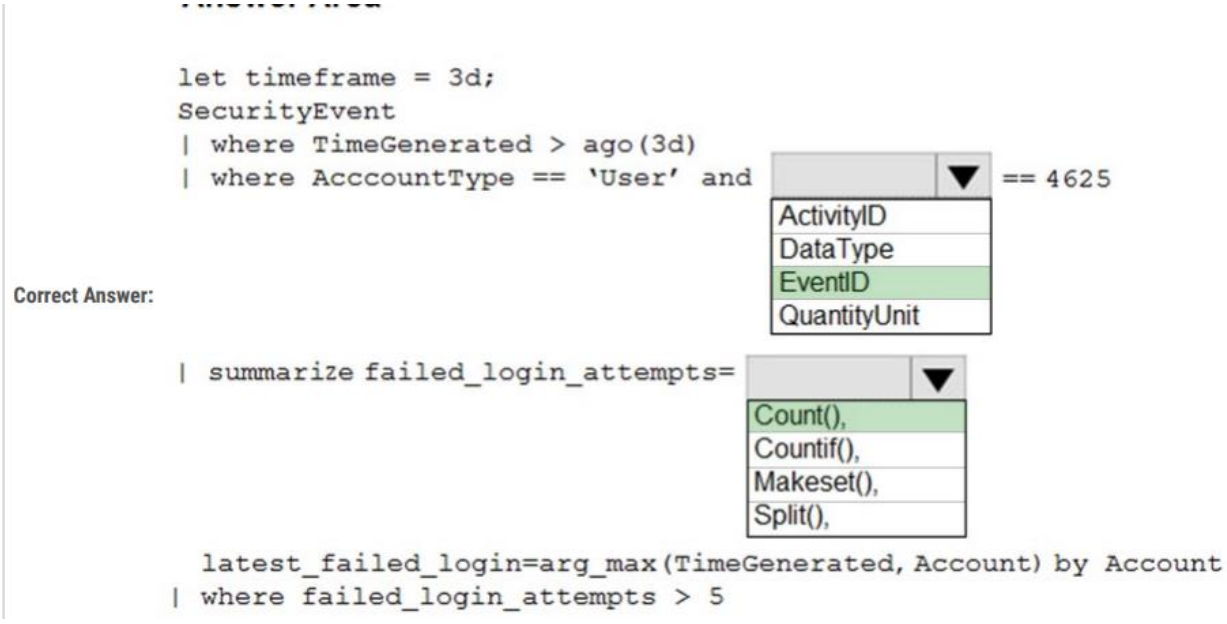
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide

References: https://docs.microsoft.com/en-us/microsoft-365/compliance/customize-a-built-in-sensitive-information-type?view=o365-worldwide

3. Create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than have failed sign-in attempts. How should you configure the query? To answer, select the appropriate options in the answer area.

Correct Answer:



References: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

4. Azure Logic Apps Designer

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

A. Azure DevOps

B. Azure Application Insights

C. Azure Monitor

D. Azure Logic Apps Designer

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up. References: https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

5. Create custom alert rules in Azure Security Center

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Onboard Azure Active Directory (Azure AD) Identity Protection.

B. Create an Azure Storage account.

C. Implement Azure Advisor recommendations.

D. Create an Azure Log Analytics workspace.

E. Upgrade the pricing tier of Security Center to Standard.

You need write permission in the workspace that you select to store your custom alert. References: https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

6. Metric

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.
You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.
You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:
- Alert rules must support dimensions.
- The time it takes to generate an alert must be minimized.
- Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

A. Log
B. Log (Saved Query)
C. Metric
D. Activity Log

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multidimensional platform metrics, custom metrics, Application Insights standard and custom metrics. Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log. References: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

7. Activity logs vs. Logs

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.
You are planning the monitoring of Azure services in the subscription.
You need to retrieve the following details:
- Identify the user who deleted a virtual machine three weeks ago.
- Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as "audit logs" or "operational logs," because they report control-plane events for your subscriptions. Activity logs help you determine the "what, who, and when" for write operations (that is, PUT, POST, or DELETE)

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

References: https://docs.microsoft.com/en-us/azure/security/azure-log-audit

8. Alerts action rules

You create an alert rule that has the following settings:

- Resource: RG1
- Condition: All Administrative operations

Actions: Action groups configured for this alert rule: ActionGroup1

-
- Alert rule name: Alert1

You create an action rule that has the following settings:

- Scope: VM1
- Filter criteria: Resource Type = "Virtual Machines"
- Define on this scope: Suppression
- Suppression config: From now (always)
- Name: ActionRule1

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

Note: Each correct selection is worth one point.

Answer area

Statements	Yes	No
If you start VM1, an alert is triggered.	○	○
If you start VM2, an alert is triggered.	○	○
If you add a tag to RG1, an alert is triggered.	○	○

Explanation

- Box 1: The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.

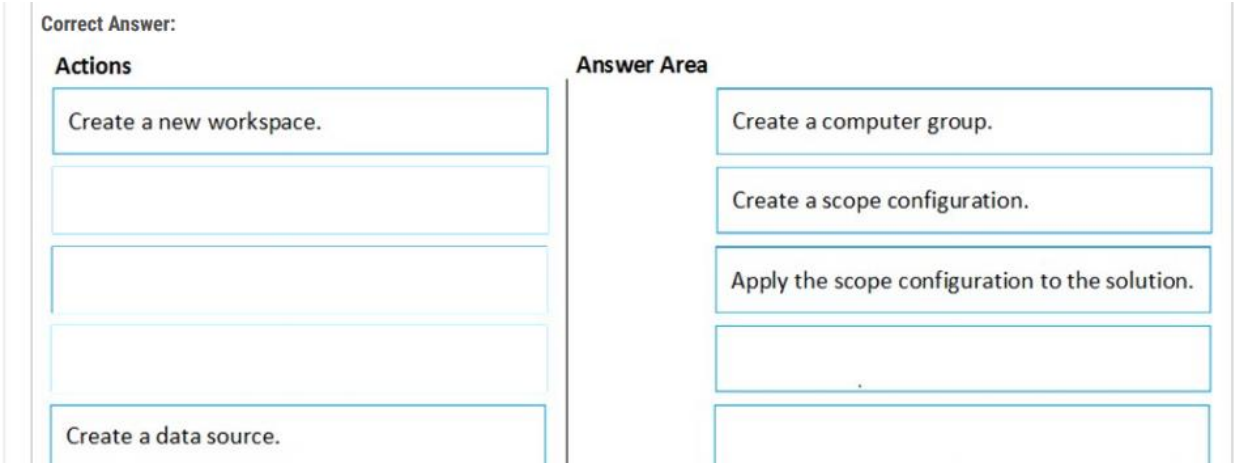
Box 2: The scope for the action rule is not set to VM2.

Box 3: Adding a tag is not an administrative operation.

References: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
https://docs.microsoft.com/en-us/azure/azuremonitor/platform/alerts-action-rules

9. Azure monitor insights

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.
You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.
You plan to add the System Update Assessment solution to LAW1.
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

10. Just in time (JIT) VM access

You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.
What should you configure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. an application security group
C. Azure Active Directory (Azure AD) conditional access
D. just in time (JIT) VM access

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down.

These ports are controlled by the just-in-time solution. When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified.

After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

11. Azure Network Watcher and NSG flow logs

You have 10 virtual machines on a single subnet that has a single network security group (NSG).
You need to log the network traffic to an Azure Storage account.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Install the Network Performance Monitor solution.
B. Enable Azure Network Watcher.
C. Enable diagnostic logging for the NSG.
D. Enable NSG flow logs.
E. Create an Azure Log Analytics workspace.

A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:

- Create a VM with a network security group
- Enable Network Watcher and register the Microsoft.Insights provider
- Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
- Download logged data
- View logged data

Reference: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-ow-logging-portal

12. Auto provisioning

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics agent installed?

A. VM3 only

B. VM1 and VM3 only

C. VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

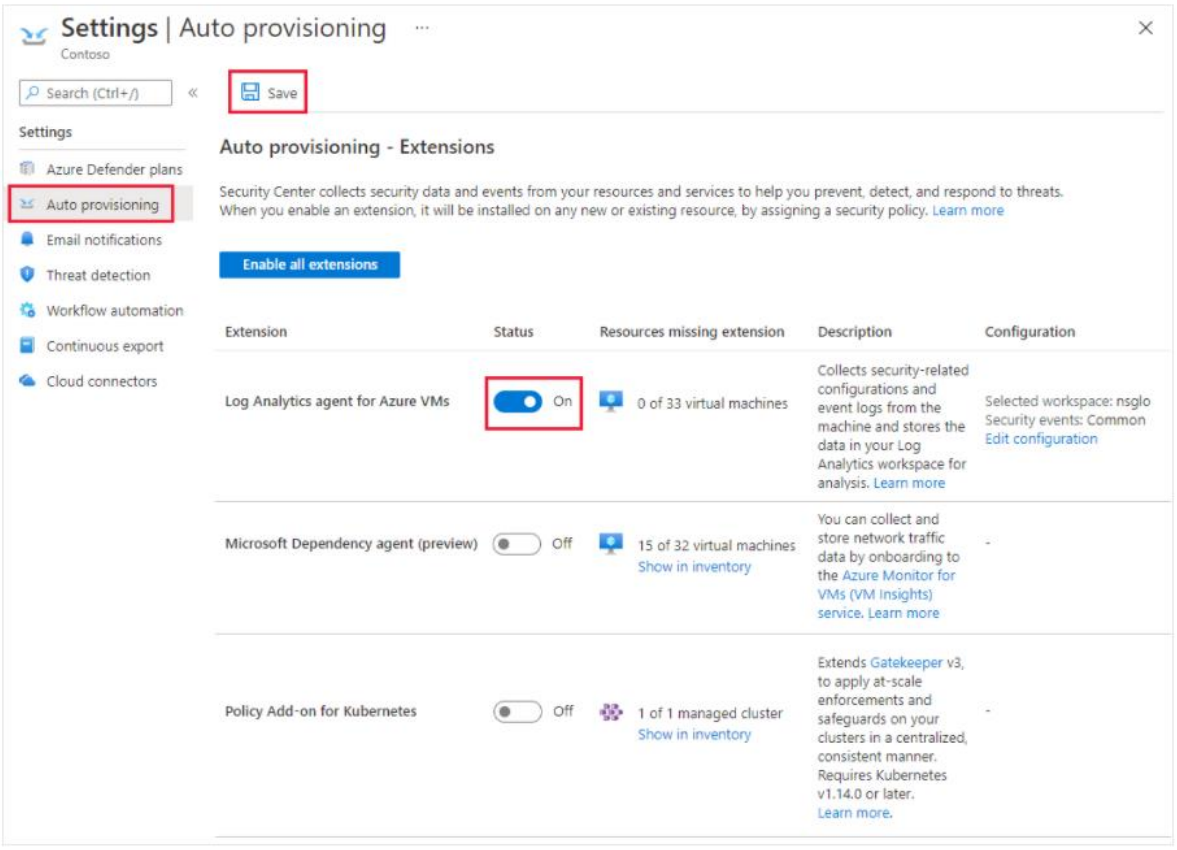
When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

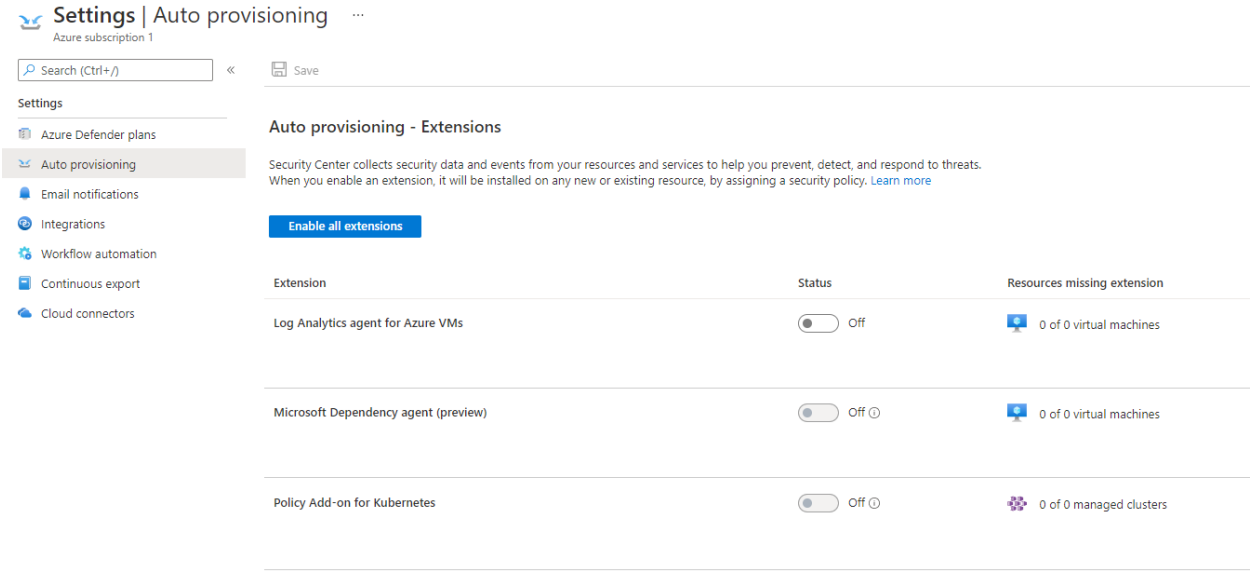
Supported Operating systems include Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

1. From Security Center's menu, select **Pricing & settings**.

2. Select the relevant subscription.

3. In the **Auto provisioning** page, set the Log Analytics agent's status to **On**.





Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Topic 4 – Questions set 4

1. Delegated permission without admin consent

You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users. What should you configure?

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.

References: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

Delegated vs. application

https://www.linkedin.com/learning/azure-for-developers-authenticating-to-azure-services-using-the-microsoft-identity-platform/delegated-vs-application-permissions?u=86261762

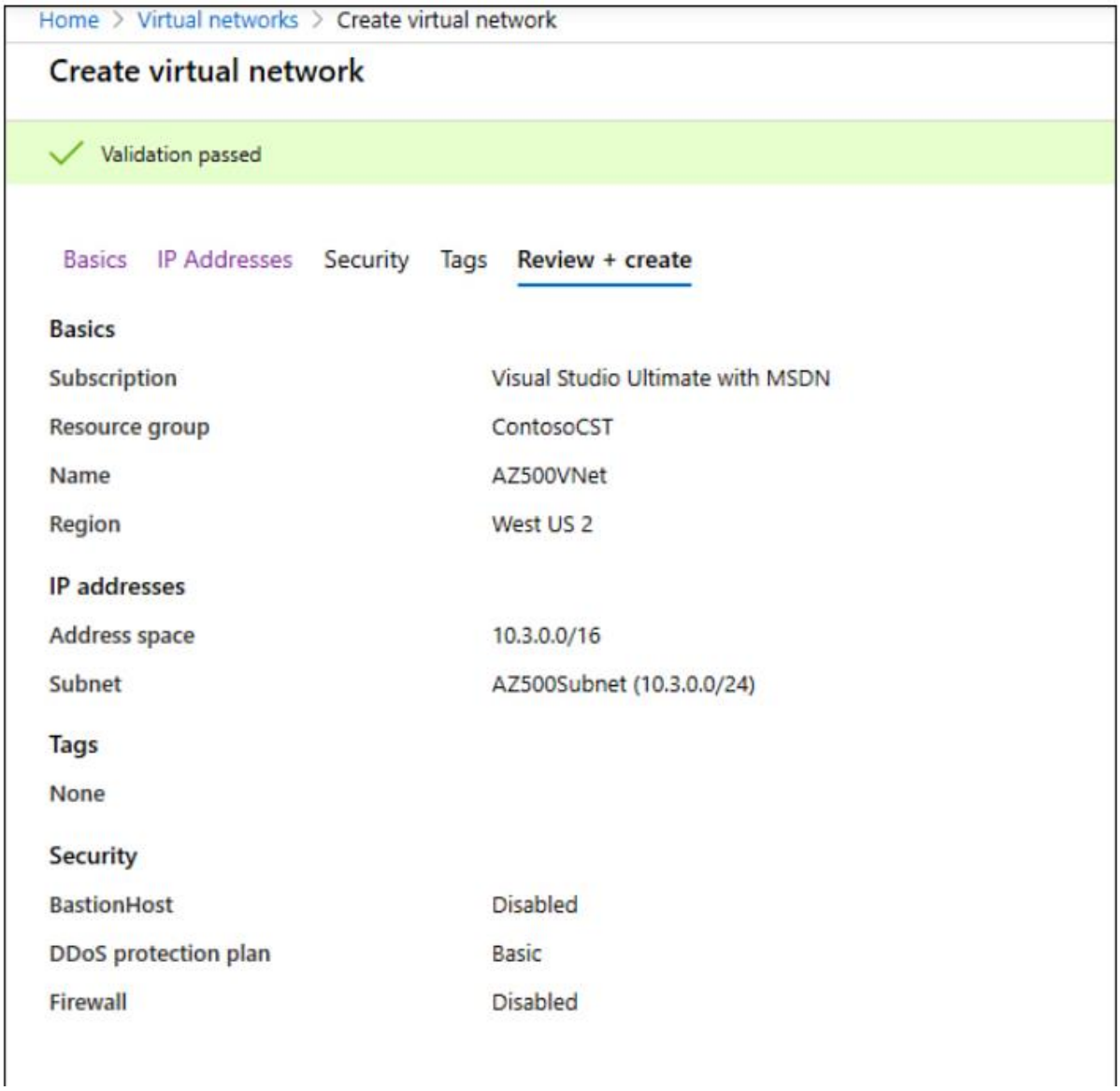
References

AZ-500: Course 2: Implement Platform Protection

ExamRef: Create a Virtual Network

Figure 2-5: Create a Virtual Network

Network security group - how it works | Microsoft Docs



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 3: Manage Security Operations Summary

- Azure resources logs register operations that were executed at the data plane level, while activity logs at the subscription level register operations that were executed in the management plane.
- You can customize alerts in Azure Monitor for different data types, including metrics, log search queries, and activity logs events.
- Monitoring solutions leverages services in Azure to provide additional insight into the operation of an application or service.
- Azure Security Center Standard tier provides built-in vulnerability assessment using native integration with Qualys.
- To enable vulnerability assessment for SQL, you first need to enable the SQL Advanced Data Security (ADS) feature.
- To implement centralized policy management in Azure Security Center, you should assign the ASC Default initiative to the Management Group level.
- The regulatory compliance dashboard in Azure Security Center can be customized to add other standards that are not available out of the box.
- To ingest data from different data sources into Azure Sentinel, you can use service-to-service connectors or external connectors.
- Azure Blueprints enable you to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

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.

LinkedIn Courses

Become an Azure Security Engineer

https://www.linkedin.com/learning/paths/become-an-azure-security-engineer?u=86261762

AZ-500: 3 Manage Security Operations

https://www.linkedin.com/learning/microsoft-azure-security-technologies-az-500-cert-prep-3-manage-security-operations-2/evaluate-vulnerability-scans-from-azure-security-center?contextUrn=urn%3Ali%3AlyndaLearningPath%3A5ece9607498e01c03163ea39&u=86261762

Demos and Labs

1. How To Create An Azure Monitor Action Group
2.