

T

estpassport考題



质 量 更 高 服 务 更 好

免费半年更新服务
<http://www.testpassport.cn>

Exam : AZ-104

**Title : Microsoft Azure
Administrator**

Version : V13.02

1. Topic 1, Litware, inc.

Overview

Litware, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named Litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

Existing Environment

The network contains an Active Directory forest named Litware.com. All domain controllers are configured as DNS servers and host the Litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private links.

Litware has data centers in the Montreal and Seattle offices. Each data center has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized.

The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMWare vCenter server	VM1
Server2	Hyper-V-host	VM2

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1GB of memory.

The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs).

Planned Changes

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.
- Migrate the virtual machines hosted on Server1 and Server2 to Azure.
- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
- Migrate App1 and App2 to two Azure web apps named webApp1 and WebApp2.

Technical requirements

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instances*.
- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.Litware.com.
- Connect the New York office to VNet1 over the Internet by using an encrypted connection.
- Create a workflow to send an email message when the settings of VM4 are modified.
- Create a custom Azure role named Role1 that is based on the Reader role.
- Minimize costs whenever possible.

You discover that VM3 does NOT meet the technical requirements. You need to verify whether the issue relates to the NSGs.

What should you use?

- A. Diagram in VNet1
- B. the security recommendations in Azure Advisor
- C. Diagnostic settings in Azure Monitor
- D. Diagnose and solve problems in Traffic Manager Profiles
- E. IP flow verify in Azure Network Watcher**

Answer: E

Explanation:

Scenario: Litware must meet technical requirements including:

Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

References:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

2. You need to meet the technical requirement for VM4.

What should you create and configure?

A. an Azure Notification Hub

B. an Azure Event Hub

C. an Azure Logic App

D. an Azure services Bus

Answer: B

Explanation:

Scenario: Create a workflow to send an email message when the settings of VM4 are modified.

You can start an automated logic app workflow when specific events happen in Azure resources or third-party resources. These resources can publish those events to an Azure event grid. In turn, the event grid pushes those events to subscribers that have queues, webhooks, or event hubs as endpoints. As a subscriber, your logic app can wait for those events from the event grid before running automated workflows to perform tasks - without you writing any code.

References:

<https://docs.microsoft.com/en-us/azure/event-grid/monitor-virtual-machine-changes-event-grid-logic-app>

3. You need to recommend a solution to automate the configuration for the finance department users. The solution must meet the technical requirements.

What should you include in the recommended?

A. Azure AP B2C

B. Azure AD Identity Protection

C. an Azure logic app and the Microsoft Identity Management (MIM) client

D. dynamic groups and conditional access policies

Answer: D

Explanation:

Scenario: Ensure Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

The recommendation is to use conditional access policies that can then be targeted to groups of users, specific applications, or other conditions.

References: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

4. HOTSPOT

You need to the appropriate sizes for the Azure virtual for Server2.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

From the Azure portal:

- Create an Azure Migrate project.
- Create a Recovery Services vault.
- Upload a management certificate.
- Create an Azure Import/Export job.

On Server2:

- Enable Hyper-V Replica.
- Install the Azure File Sync agent.
- Create a collector virtual machine.
- Configure Hyper-V storage migration.
- Install the Azure Site Recovery Provider.

Answer:

From the Azure portal:

- Create an Azure Migrate project.
- Create a Recovery Services vault.**
- Upload a management certificate.
- Create an Azure Import/Export job.

On Server2:

- Enable Hyper-V Replica.
- Install the Azure File Sync agent.
- Create a collector virtual machine.
- Configure Hyper-V storage migration.
- Install the Azure Site Recovery Provider.**

Explanation:

Box 1: Create a Recovery Services vault

Create a Recovery Services vault on the Azure Portal.

Box 2: Install the Azure Site Recovery Provider

Azure Site Recovery can be used to manage migration of on-premises machines to Azure.

Scenario: Migrate the virtual machines hosted on Server1 and Server2 to Azure.

Server2 has the Hyper-V host role.

References: <https://docs.microsoft.com/en-us/azure/site-recovery/migrate-tutorial-on-premises-azure>

5.HOTSPOT

You need to implement Role1.

Which command should you run before you create Role1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

<input type="checkbox"/> Find-RoleCapability <input type="checkbox"/> Get-AzureADDirectoryRole <input type="checkbox"/> Get-AzureRmRoleAssignment <input type="checkbox"/> Get-AzureRmRoleDefinition	<input type="checkbox"/> -Name "Reader" <input type="checkbox"/> ConvertFrom-Json <input type="checkbox"/> ConvertFrom-String <input type="checkbox"/> ConvertTo-Json <input type="checkbox"/> ConvertTo-Xml
---	--

Answer:

<input type="checkbox"/> Find-RoleCapability <input type="checkbox"/> Get-AzureADDirectoryRole <input type="checkbox"/> Get-AzureRmRoleAssignment <input type="checkbox"/> Get-AzureRmRoleDefinition	<input type="checkbox"/> -Name "Reader" <input type="checkbox"/> ConvertFrom-Json <input type="checkbox"/> ConvertFrom-String <input checked="" type="checkbox"/> ConvertTo-Json <input type="checkbox"/> ConvertTo-Xml
---	---

6. HOTSPOT

You need to meet the connection requirements for the New York office.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

From the Azure portal:

- Create an ExpressRoute circuit only.
- Create a virtual network gateway only.
- Create a virtual network gateway and a local network gateway.
- Create an ExpressRoute circuit and an on-premises data gateway.
- Create a virtual network gateway and an on-premises data gateway.

In the New York office:

- Deploy ExpressRoute.
- Deploy a DirectAccess server.
- Implement a Web Application Proxy.
- Configure a site-to-site VPN connection.

Answer:

From the Azure portal:

- Create an ExpressRoute circuit only.
- Create a virtual network gateway only.
- Create a virtual network gateway and a local network gateway.**
- Create an ExpressRoute circuit and an on-premises data gateway.
- Create a virtual network gateway and an on-premises data gateway.

In the New York office:

- Deploy ExpressRoute.
- Deploy a DirectAccess server.
- Implement a Web Application Proxy.
- Configure a site-to-site VPN connection.**

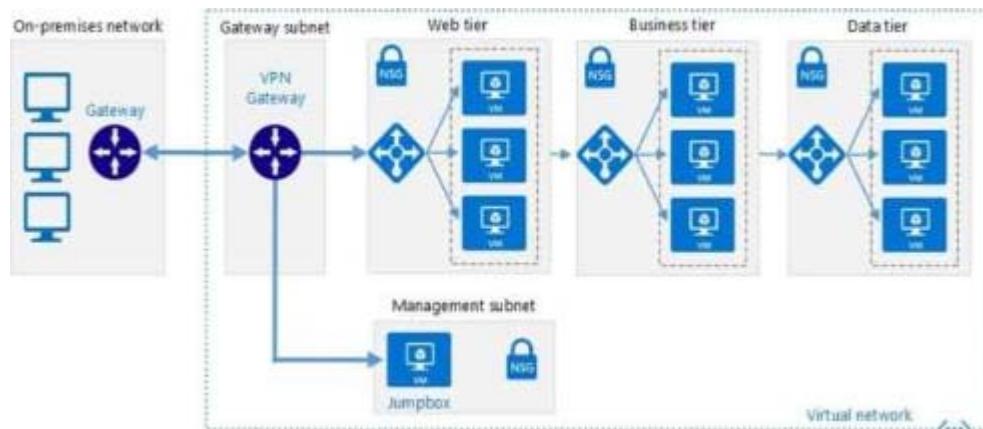
Explanation:

Box 1: Create a virtual network gateway and a local network gateway.

Azure VPN gateway. The VPN gateway service enables you to connect the VNet to the on-premises network through a VPN appliance. For more information, see Connect an on-premises network to a Microsoft Azure virtual network. The VPN gateway includes the following elements:

Box 2: Configure a site-to-site VPN connection

On premises create a site-to-site connection for the virtual network gateway and the local network gateway.



Scenario: Connect the New York office to VNet1 over the Internet by using an encrypted connection.

7. Topic 2, Humongous Insurance

Overview

Existing Environment

Humongous Insurance is an insurance company that has three offices in Miami, Tokoyo, and Bangkok. Each has 5000 users.

Active Directory Environment

Humongous Insurance has a single-domain Active Directory forest named `humongousinsurance.com`.

The functional level of the forest is Windows Server 2012.

You recently provisioned an Azure Active Directory (Azure AD) tenant.

Network Infrastructure

Each office has a local data center that contains all the servers for that office. Each office has a dedicated connection to the Internet.

Each office has several link load balancers that provide access to the servers.

Active Directory Issue

Several users in humongousinsurance.com have UPNs that contain special characters.

You suspect that some of the characters are unsupported in Azure AD.

Licensing Issue

You attempt to assign a license in Azure to several users and receive the following error message:

"Licenses not assigned. License agreement failed for one user."

You verify that the Azure subscription has the available licenses.

Requirements

Planned Changes

Humongous Insurance plans to open a new office in Paris. The Paris office will contain 1,000 users who will be hired during the next 12 months.

All the resources used by the Paris office users will be hosted in Azure.

Planned Azure AD Infrastructure

The on-premises Active Directory domain will be synchronized to Azure AD. All client computers in the Paris office will be joined to an Azure AD domain.

Planned Azure Networking Infrastructure

You plan to create the following networking resources in a resource group named All_Resources:

- Default Azure system routes that will be the only routes used to route traffic
- A virtual network named Paris-VNet that will contain two subnets named Subnet1 and Subnet2
- A virtual network named ClientResources-VNet that will contain one subnet named ClientSubnet
- A virtual network named AllOffices-VNet that will contain two subnets named Subnet3 and Subnet4

You plan to enable peering between Paris-VNet and AllOffices-VNet.

You will enable the Use remote gateways setting for the Paris-VNet peerings.

You plan to create a private DNS zone named humongousinsurance.local and set the registration network to the ClientResources-VNet virtual network.

Planned Azure Computer Infrastructure

Each subnet will contain several virtual machines that will run either Windows Server 2012 R2, Windows Server 2016, or Red Hat Linux.

Department Requirements

Humongous Insurance identifies the following requirements for the company's departments:

- Web administrators will deploy Azure web apps for the marketing department. Each web app will be added to a separate resource group. The initial configuration of the web apps will be identical. The web administrators have permission to deploy web apps to resource groups.
- During the testing phase, auditors in the finance department must be able to review all Azure costs from

the past week.

Authentication Requirements

Users in the Miami office must use Azure Active Directory Seamless Single Sign-on (Azure AD Seamless SSO) when accessing resources in Azure.

DRAG DROP

You need to prepare the environment to ensure that the web administrators can deploy the web apps as quickly as possible.

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
From the Templates service, select the template, and then share the template to the web administrators.	
Create a resource group, and then deploy a web app to the resource group.	
From the Automation script blade of the resource group, click the Parameters tab.	
From the Automation script blade of the resource group, click Deploy .	
From the Automation Accounts service, add an automation account.	
From the Automation script blade of the resource group, click Add to library .	

Answer:

Actions	Answer Area
From the Templates service, select the template, and then share the template to the web administrators.	Create a resource group, and then deploy a web app to the resource group.
Create a resource group, and then deploy a web app to the resource group.	From the Automation script blade of the resource group, click Add to library .
From the Automation script blade of the resource group, click the Parameters tab.	From the Templates service, select the template, and then share the template to the web administrators.
From the Automation script blade of the resource group, click Deploy .	
From the Automation Accounts service, add an automation account.	
From the Automation script blade of the resource group, click Add to library .	

Explanation:

Scenario:

1. Web administrators will deploy Azure web apps for the marketing department.
2. Each web app will be added to a separate resource group.
3. The initial configuration of the web apps will be identical.
4. The web administrators have permission to deploy web apps to resource groups.

Steps:

1 --> Create a resource group, and then deploy a web app to the resource group.

2 --> From the Automation script blade of the resource group, click Add to Library.

3 --> From the Templates service, select the template, and then share the template to the web administrators.

References:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/quickstart-create-templates-use-the-portal>

8.Which blade should you instruct the finance department auditors to use?

- A. Partner information
- B. Overview
- C. Payment methods
- D. Invoices**

Answer: D

Explanation:

You can opt in and configure additional recipients to receive your Azure invoice in an email. This feature may not be available for certain subscriptions such as support offers, Enterprise Agreements, or Azure in Open.

Scenario: During the testing phase, auditors in the finance department must be able to review all Azure costs from the past week.

References:

<https://docs.microsoft.com/en-us/azure/billing/billing-download-azure-invoice-daily-usage-date>

9.You need to prepare the environment to meet the authentication requirements.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE Each correct selection is worth one point.

- A. Azure Active Directory (AD) Identity Protection and an Azure policy
- B. a Recovery Services vault and a backup policy**
- C. an Azure Key Vault and an access policy
- D. an Azure Storage account and an access policy**

Answer: B,D

Explanation:

D: Seamless SSO works with any method of cloud authentication - Password Hash Synchronization or Pass-through Authentication, and can be enabled via Azure AD Connect.

B: You can gradually roll out Seamless SSO to your users. You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory:

<https://autologon.microsoftazuread-sso.com>

10. You need to define a custom domain name for Azure AD to support the planned infrastructure.

Which domain name should you use?

A. Join the client computers in the Miami office to Azure AD.

B. Add <http://autologon.microsoftazuread-sso.com> to the intranet zone of each client computer in the Miami office.

C. Allow inbound TCP port 8080 to the domain controllers in the Miami office.

D. Install Azure AD Connect on a server in the Miami office and enable Pass-through Authentication

E. Install the Active Directory Federation Services (AD FS) role on a domain controller in the Miami office.

Answer: B,D

Explanation:

Every Azure AD directory comes with an initial domain name in the form of `domainname.onmicrosoft.com`. The initial domain name cannot be changed or deleted, but you can add your corporate domain name to Azure AD as well. For example, your organization probably has other domain names used to do business and users who sign in using your corporate domain name. Adding custom domain names to Azure AD allows you to assign user names in the directory that are familiar to your users, such as '`alice@contoso.com`' instead of '`alice@domain name.onmicrosoft.com`'.

Scenario:

Network Infrastructure: Each office has a local data center that contains all the servers for that office.

Each office has a dedicated connection to the Internet.

Humongous Insurance has a single-domain Active Directory forest named `humongousinsurance.com`

Planned Azure AD Infrastructure: The on-premises Active Directory domain will be synchronized to Azure AD.

References: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>

11. You need to resolve the Active Directory issue.

What should you do?

A. From Active Directory Users and Computers, select the user accounts, and then modify the User Principal Name value.

B. Run `idfix.exe`, and then use the Edit action.

C. From Active Directory Domains and Trusts, modify the list of UPN suffixes.

D. From Azure AD Connect, modify the outbound synchronization rule.

Answer: B

Explanation:

`IdFix` is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. `IdFix` is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

Scenario: Active Directory Issue

Several users in `humongousinsurance.com` have UPNs that contain special characters.

You suspect that some of the characters are unsupported in Azure AD.

References: <https://www.microsoft.com/en-us/download/details.aspx?id=36832>

12. Which blade should you instruct the finance department auditors to use?

- A. invoices
- B. partner information
- C. cost analysis**
- D. External services

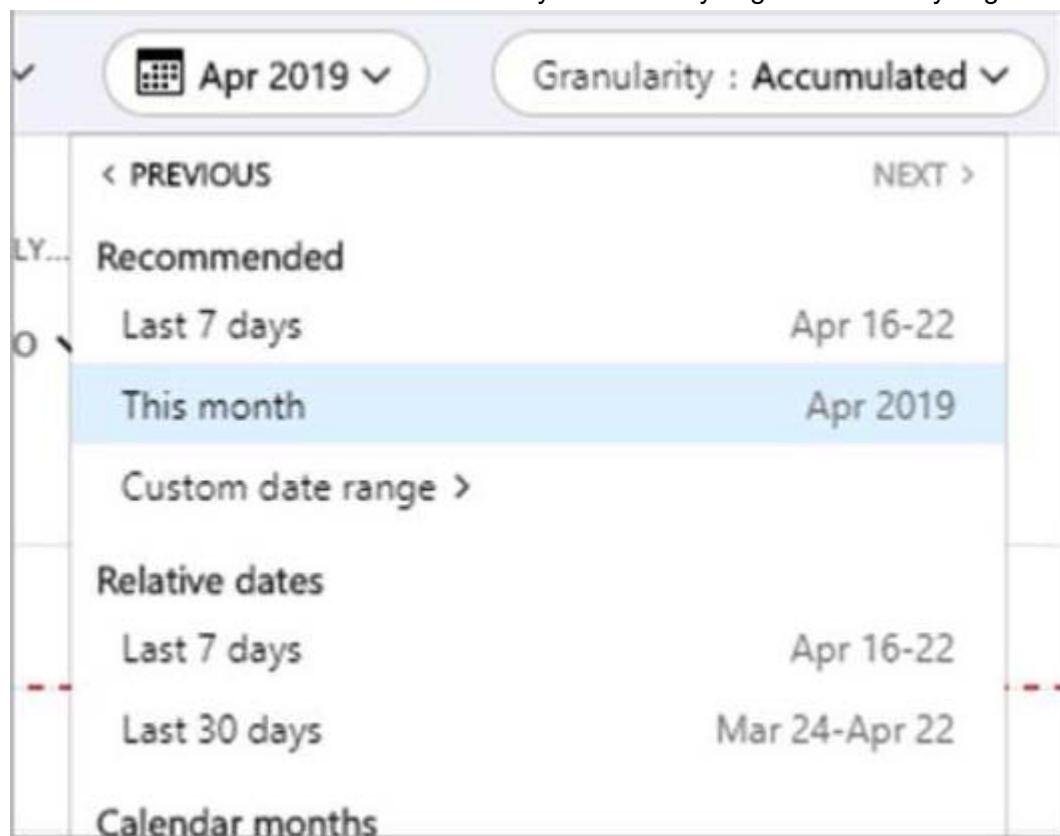
Answer: C

Explanation:

Cost analysis: Correct Option

In cost analysis blade of Azure, you can see all the detail for custom time span. You can use this to determine expenditure of last few day, weeks, and month. Below options are available in Cost analysis blade for filtering information by time span: last 7 days, last 30 days, and custom date range. Choosing the first option (last 7 days) auditors can view the costs by time span.

Cost analysis shows data for the current month by default. Use the date selector to switch to common date ranges quickly. Examples include the last seven days, the last month, the current year, or a custom date range. Pay-as-you-go subscriptions also include date ranges based on your billing period, which isn't bound to the calendar month, like the current billing period or last invoice. Use the <PREVIOUS and NEXT> links at the top of the menu to jump to the previous or next period, respectively. For example, <PREVIOUS will switch from the Last 7 days to 8-14 days ago or 15-21 days ago.



Invoice: Incorrect Option

Invoices can only be used for past billing periods not for current billing period, i.e. if your requirement is to know the last week's cost then that also not filled by invoices because Azure generates invoice at the end of the month.

Even though Invoices have custom timespan, but when you put in dates for a week, the pane would be empty. Below is from Microsoft document:

Why don't I see an invoice for the last billing period?

There could be several reasons that you don't see an invoice:

- It's less than 30 days from the day you subscribed to Azure.
- The invoice isn't generated yet. Wait until the end of the billing period.
- You don't have permission to view invoices. If you have a Microsoft Customer Agreement, you must be the billing profile Owner, Contributor, Reader, or Invoice manager. For other subscriptions, you might not see old invoices if you aren't the Account Administrator. To learn more about getting access to billing information, see [Manage access to Azure billing using roles](#).
- If you have a Free Trial or a monthly credit amount with your subscription that you didn't exceed, you won't get an invoice unless you have a Microsoft Customer Agreement.

Resource Provider: Incorrect Option

When deploying resources, you frequently need to retrieve information about the resource providers and types. For example, if you want to store keys and secrets, you work with the Microsoft.KeyVault resource provider. This resource provider offers a resource type called vaults for creating the key vault. This is not useful for reviewing all Azure costs from the past week which is required for audit.

Payment method: Incorrect Option

Payment methods is not useful for reviewing all Azure costs from the past week which is required for audit.

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/quick-acm-cost-analysis>

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/download-azure-invoice-daily-usage-date>

13. You need to define a custom domain name for Azure AD to support the planned infrastructure.

Which domain name should you use?

- A. ad.humongousinsurance.com
- B. humongousinsurance.onmicrosoft.com
- C. humongousinsurance.local
- D. humongousinsurance.com**

Answer: D

Explanation:

Every Azure AD directory comes with an initial domain name in the form of domainname.onmicrosoft.com. The initial domain name cannot be changed or deleted, but you can add your corporate domain name to Azure AD as well. For example, your organization probably has other domain names used to do business and users who sign in using your corporate domain name. Adding custom domain names to Azure AD allows you to assign user names in the directory that are familiar to your users, such as 'alice@contoso.com.' instead of 'alice@domain name.onmicrosoft.com'.

Scenario:

Network Infrastructure: Each office has a local data center that contains all the servers for that office. Each office has a dedicated connection to the Internet.

Humongous Insurance has a single-domain Active Directory forest named humongousinsurance.com
Planned Azure AD Infrastructure: The on-premises Active Directory domain will be synchronized to Azure AD.

References: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>

14. You need to prepare the environment to meet the authentication requirements.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Allow inbound TCP port 8080 to the domain controllers in the Miami office.
- B. Add <http://autologon.microsoftazuread-sso.com> to the intranet zone of each client computer in the Miami office.**
- C. Join the client computers in the Miami office to Azure AD.
- D. Install the Active Directory Federation Services (AD FS) role on a domain controller in the Miami office.
- E. Install Azure AD Connect on a server in the Miami office and enable Pass-through Authentication.**

Answer: B,E

Explanation:

B: You can gradually roll out Seamless SSO to your users. You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory:

<https://autologon.microsoftazuread-sso.com>

E: Seamless SSO works with any method of cloud authentication - Password Hash

Synchronization or Pass-through Authentication, and can be enabled via Azure AD Connect.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start>

15. You need to resolve the licensing issue before you attempt to assign the license again.

What should you do?

- A. From the Groups blade, invite the user accounts to a new group.
- B. From the Profile blade, modify the usage location.**
- C. From the Directory role blade, modify the directory role.

Answer: B

Explanation:

Scenario: Licensing Issue

1. You attempt to assign a license in Azure to several users and receive the following error message: "Licenses not assigned. License agreement failed for one user."

2. You verify that the Azure subscription has the available licenses.

Solution:

License cannot be assigned to a user without a usage location specified.

Some Microsoft services aren't available in all locations because of local laws and regulations. Before you can assign a license to a user, you must specify the Usage location property for the user. You can specify the location under the User > Profile > Settings section in the Azure portal.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-resolve-problems>

16.HOTSPOT

You are evaluating the name resolution for the virtual machines after the planned implementation of the Azure networking infrastructure.

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

Statements	Yes	No
The virtual machines on Subnet1 will be able to resolve the hosts in the humongousinsurance.local zone.	<input type="radio"/>	<input type="radio"/>
The virtual machines on ClientSubnet will be able to register the hostname records in the humongousinsurance.local zone.	<input type="radio"/>	<input type="radio"/>
The virtual machines on Subnet4 will be able to register the hostname records in the humongousinsurance.local zone.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
The virtual machines on Subnet1 will be able to resolve the hosts in the humongousinsurance.local zone.	<input checked="" type="radio"/>	<input type="radio"/>
The virtual machines on ClientSubnet will be able to register the hostname records in the humongousinsurance.local zone.	<input checked="" type="radio"/>	<input type="radio"/>
The virtual machines on Subnet4 will be able to register the hostname records in the humongousinsurance.local zone.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statement 1: Yes

All client computers in the Paris office will be joined to an Azure AD domain.

A virtual network named Paris-VNet that will contain two subnets named Subnet1 and Subnet2. Microsoft Windows Server Active Directory domains, can resolve DNS names between virtual networks. Automatic registration of virtual machines from a virtual network that's linked to a private zone with auto-registration enabled. Forward DNS resolution is supported across virtual networks that are linked to the private zone.

Statement 2: Yes

A virtual network named ClientResources-VNet that will contain one subnet named ClientSubnet. You plan to create a private DNS zone named humongousinsurance.local and set the registration network to the ClientResources-VNet virtual network. As this is a registration network so this will work.

Statement 3: No

Only VMs in the registration network, here the ClientResources-VNet, will be able to register hostname records. Since Subnet4 is not connected to Client Resources Network thus not able to register its hostname with humongousinsurance.local

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-overview>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances>

17.HOTSPOT

You are evaluating the connectivity between the virtual machines after the planned implementation of the

Azure networking infrastructure.

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

Statements	Yes	No
The virtual machines on Subnet1 will be able to connect to the virtual machines on Subnet3.	<input type="radio"/>	<input type="radio"/>
The virtual machines on ClientSubnet will be able to connect to the Internet.	<input type="radio"/>	<input type="radio"/>
The virtual machines on Subnet3 and Subnet4 will be able to connect to the Internet.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
The virtual machines on Subnet1 will be able to connect to the virtual machines on Subnet3.	<input checked="" type="radio"/>	<input type="radio"/>
The virtual machines on ClientSubnet will be able to connect to the Internet.	<input checked="" type="radio"/>	<input type="radio"/>
The virtual machines on Subnet3 and Subnet4 will be able to connect to the Internet.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Once the VNets are peered, all resources on one VNet can communicate with resources on the other peered VNets. You plan to enable peering between Paris-VNet and AllOffices-VNet. Therefore VMs on Subnet1, which is on Paris-VNet and VMs on Subnet3, which is on AllOffices-VNet will be able to connect to each other.

All Azure resources connected to a VNet have outbound connectivity to the Internet by default. Therefore VMs on ClientSubnet, which is on ClientResources-VNet will have access to the Internet; and VMs on Subnet3 and Subnet4, which are on AllOffices-VNet will have access to the Internet.

Reference:

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

<https://docs.microsoft.com/en-us/azure/networking/networking-overview#internet-connectivity>

18. Topic 3, Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Ensure that partner access to the blueprint files is secured and temporary.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service administrator of the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to meet the user requirement for Admin1.

What should you do?

- A. From the Subscriptions blade, select the subscription, and then modify the Properties.
- B. From the Subscriptions blade, select the subscription, and then modify the Access control (IAM) settings.
- C. From the Azure Active Directory blade, modify the Properties.
- D. From the Azure Active Directory blade, modify the Groups.

Answer: A

Explanation:

Change the Service administrator for an Azure subscription

Scenario: Designate a new user named Admin1 as the service administrator of the Azure subscription.

References:

<https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator>

19. You need to move the blueprint files to Azure.

What should you do?

- A. Generate a shared access signature (SAS). Map a drive, and then copy the files by using File Explorer.
- B. Use the Azure Import/Export service.
- C. Generate an access key. Map a drive, and then copy the files by using File Explorer.
- D. Use Azure Storage Explorer to copy the files.**

Answer: D

Explanation:

Azure Storage Explorer is a free tool from Microsoft that allows you to work with Azure Storage data on Windows, macOS, and Linux. You can use it to upload and download data from Azure blob storage.

Scenario:

Planned Changes include: move the existing product blueprint files to Azure Blob storage.

Technical Requirements include: Copy the blueprint files to Azure over the Internet.

References:

<https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-data-to-azure-blob-using-azure-storage-explorer>

20. You need to implement a backup solution for App1 after the application is moved.

What should you create first?

- A. a recovery plan
- B. an Azure Backup Server
- C. a backup policy
- D. a Recovery Services vault**

Answer: D

Explanation:

Explanation:

A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs. When the backup job for a protected resource runs, it creates a recovery point inside the Recovery Services vault.

Scenario:

There are three application tiers, each with five virtual machines.

Move all the virtual machines for App1 to Azure.

Ensure that all the virtual machines for App1 are protected by backups.

References: <https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal>

21.HOTSPOT

You need to recommend a solution for App1. The solution must meet the technical requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Number of virtual networks:

1
2
3

Number of subnets:

1
2
3

Answer:

Number of virtual networks:

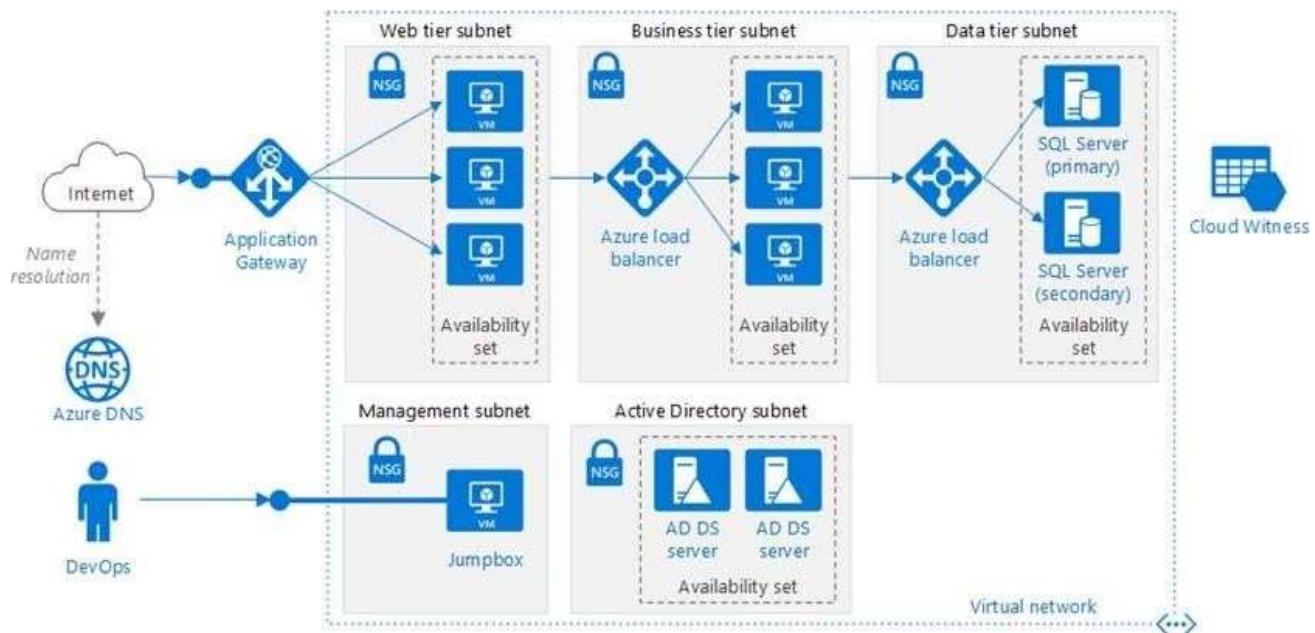
1
2
3

Number of subnets:

1
2
3

Explanation:

This reference architecture shows how to deploy VMs and a virtual network configured for an N-tier application, using SQL Server on Windows for the data tier.



Scenario: You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

- Technical requirements include:
- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.

References:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/n-tier-sql-server>

22.HOTSPOT

You need to configure the Device settings to meet the technical requirements and the user requirements. Which two settings should you modify? To answer, select the appropriate settings in the answer area.

Answer Area



Save



Discard

Users may join devices to Azure AD

All

Selected

None

Selected

No member selected

Additional local administrators on Azure AD joined devices

Selected

None

Selected

No member selected

Users may register their devices with Azure AD

All

None

Require Multi-Factor Auth to join devices

Yes

No

Maximum number of devices per user

50

Users may sync settings and app data across devices

All

Selected

None

Selected

No member selected

Answer:

Answer Area



Save



Discard

Users may join devices to Azure AD

All

Selected

None

Selected

No member selected

Additional local administrators on Azure AD joined devices

Selected

None

Selected

No member selected

Users may register their devices with Azure AD

All

None

Require Multi-Factor Auth to join devices

Yes

No

Maximum number of devices per user

50

Users may sync settings and app data across devices

All

Selected

None

Selected

No member selected

Explanation:

Box 1: Selected

Only selected users should be able to join devices

Box 2: Yes

Require Multi-Factor Auth to join devices.

From scenario:

23. You need to recommend an identify solution that meets the technical requirements.

What should you recommend?

- A. federated single-on (SSO) and Active Directory Federation Services (AD FS)
- B. password hash synchronization and single sign-on (SSO)
- C. cloud-only user accounts
- D. Pass-through Authentication and single sign-on (SSO)

Answer: A

Explanation:

Active Directory Federation Services is a feature and web service in the Windows Server Operating System that allows sharing of identity information outside a company's network.

Scenario: Technical Requirements include:

Prevent user passwords or hashes of passwords from being stored in Azure.

References: <https://www.sherweb.com/blog/active-directory-federation-services/>

24. You are planning the move of App1 to Azure.

You create a network security group (NSG).

You need to recommend a solution to provide users with access to App1.

What should you recommend?

- A. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to all the subnets.
- B. Create an incoming security rule for port 443 from the Internet. Associate the NSG to all the subnets.
- C. Create an incoming security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers.**
- D. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers.

Answer: C

Explanation:

As App1 is public-facing we need an incoming security rule, related to the access of the web servers.

Scenario: You have a public-facing application named App1. App1 is comprised of the following

three tiers: a SQL database, a web front end, and a processing middle tier.

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

25. HOTSPOT

You need to identify the storage requirements for Contoso.

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
Contoso requires a storage account that supports Blob storage.	<input type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure Table storage.	<input type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure File Storage.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Contoso requires a storage account that supports Blob storage.	<input checked="" type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure Table storage.	<input type="radio"/>	<input checked="" type="radio"/>
Contoso requires a storage account that supports Azure File Storage.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statement 1: Yes

Contoso is moving the existing product blueprint files to Azure Blob storage which will ensure that the blueprint files are stored in the archive storage tier.

Use unmanaged standard storage for the hard disks of the virtual machines. We use Page Blobs for these.

Statement 2: No

Azure Table storage stores large amounts of structured data. The service is a NoSQL datastore which accepts authenticated calls from inside and outside the Azure cloud. Azure tables are ideal for storing structured, non-relational data.

Common uses of Table storage include:

1. Storing TBs of structured data capable of serving web scale applications
2. Storing datasets that don't require complex joins, foreign keys, or stored procedures and can be denormalized for fast access
3. Quickly querying data using a clustered index
4. Accessing data using the OData protocol and LINQ queries with WCF Data Service .NET Libraries

Statement 3: No

File Storage can be used if your business use case needs to deal mostly with standard File extensions like *.docx, *.png and *.bak then you should probably go with this storage option.

Reference:

<https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-data-to-azure-blob-using-azure-storage-explorer>

<https://docs.microsoft.com/en-us/azure/storage/tables/table-storage-overview>

<https://www.serverless360.com/blog/azure-blob-storage-vs-file-storage>

26. Topic 4, Misc. Questions Set A

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource

group.

Solution: On Dev, you assign the Contributor role to the Developers group.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

The Contributor role can manage all resources (and add resources) in a Resource Group.

Reference: <https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

27.**Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Dev, you assign the Logic App Contributor role to the Developers group.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

The Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

References:

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

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app>

28.**Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Subscription1, you assign the DevTest Labs User role to the Developers group.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

DevTest Labs User role only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.

You would need the Logic App Contributor role.

References:

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

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app>

29. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG2 and West US.

Does this meet the goal?

A. Yes

B. NO

Answer: A

Explanation:

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

References: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

30. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1 that contains the resources shown in the following

table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG2 and Central US.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

References: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

31. This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG1 and Central US.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

References: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

32. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You modify the Azure Active Directory (Azure AD) authentication policies.

Does this meet this goal?

A. Yes

B. No

Answer: B

Explanation:

Instead export the client certificate from Computer1 and install the certificate on Computer2.

Note:

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed.

You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

Reference: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

33. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You export the client certificate from Computer1 and install the certificate on Computer2.

Does this meet this goal?

A. Yes

B. No

Answer: A

Explanation:

Each client computer that connects to a VNet using Point-to-Site must have a client certificate

installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

References: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

34. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: On Computer2, you set the Startup type for the IPSec Policy Agent service to Automatic.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead export the client certificate from Computer1 and install the certificate on Computer2.

Note: Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

References: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

35. HOTSPOT

You have a virtual network named VNet1 that has the configuration shown in the following exhibit.

```
PS C:\> Get-AzureRmVirtualNetwork -Name Vnet1 -ResourceGroupName Production

Name          : VNet1
ResourceGroupName : Production
Location      : westus
Id            : /subscriptions/14d26092-8e42-4ea7-b770-9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/virtualNetworks/VNet1
Etag          : W/"76f7edd6-d022-455b-aeae-376059318e5d"
ResourceGuid   : 562696cc-b2ba-4cc5-9619-0a735d6c34c7
ProvisioningState : Succeeded
Tags          :
AddressSpace  : {
    "AddressPrefixes": [
        "10.2.0.0/16"
    ]
}
DhcpOptions   : {}
Subnets       : [
    {
        "Name": "default",
        "Etag": "W/"76f7edd6-d022-455b-aeae-376059318e5d"",
        "Id": "/subscriptions/14d26092-8e42-4ea7-b770-9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/virtualNetworks/VNet1/subnets/default",
        "AddressPrefix": "10.2.0.0/24",
        "IpConfigurations": [],
        "ResourceNavigationLinks": [],
        "ServiceEndpoints": [],
        "ProvisioningState": "Succeeded"
    }
]
VirtualNetworkPeerings : []
EnableDDoSProtection : false
EnableVmProtection   : false
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first [answer choice].

- | |
|-------------------------|
| add a network interface |
| add a subnet |
| add an address space |
| delete a subnet |
| delete an address space |

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first [answer choice].

- | |
|-------------------------|
| add a network interface |
| add a subnet |
| add an address space |
| delete a subnet |
| delete an address space |

Answer:

Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first **[answer choice]**.

add a network interface
add a subnet
add an address space
delete a subnet
delete an address space

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first **[answer choice]**.

add a network interface
add a subnet
add an address space
delete a subnet
delete an address space

Explanation:Box 1: add an address space

Your IaaS virtual machines (VMs) and PaaS role instances in a virtual network automatically receive a private IP address from a range that you specify, based on the address space of the subnet they are connected to. We need to add the 192.168.1.0/24 address space.

Box 2: add a subnet

Address space is present but need to add subnet

References:

<https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models?view=o365-worldwide>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-static-private-ip-arm-pportal>

36. You have an Azure subscription that contains the resources in the following table.

Name	Type	Details
VNet1	Virtual network	<i>Not applicable</i>
Subnet1	Subnet	Hosted on VNet1
VM1	Virtual machine	On Subnet1
VM2	Virtual machine	On Subnet1

VM1 and VM2 are deployed from the same template and host line-of-business applications accessed by using Remote Desktop.

You configure the network security group (NSG) shown in the exhibit. (Click the Exhibit button.)

 Move  Delete

Resource group (change) ProductionRG	Security rules 1 inbound, 1 outbound
Location North Europe	Associated with 0 subnets, 0 network interfaces
Subscription (change) Production subscription	
Subscription ID 14d26092-8e42-4ea7-b770-9dcef70fb1ea	
Tags (change) Click here to add tags	

▲

Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
1500	Port_80	80	TCP	Internet	Any	 Deny	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow	...
65500	DenyAllBound	Any	Any	Any	Any	 Deny	...

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
1000	DenyWebSites	80	TCP	Any	Internet	 Deny	...
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow	...
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny	...

You need to prevent users of VM1 and VM2 from accessing websites on the Internet.

What should you do?

- A. Associate the NSG to Subnet1.
- B. Disassociate the NSG from a network interface.
- C. Change the DenyWebSites outbound security rule.
- D. Change the Port_80 inbound security rule.

Answer: A

Explanation:

You can associate or dissociate a network security group from a network interface or subnet. The NSG has the appropriate rule to block users from accessing the Internet. We just need to associate it with Subnet1.

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

37.DRAG DROP

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2.

Virtual machines connect to the virtual networks.

The virtual networks on-premises server named Server1 that configured as shown in the following table.

Virtual network	Address space	Subnet	Peering
VNet1	10.1.0.0/16	10.1.0.0/24	VNet2
		10.1.1.0/26	
VNet2	10.2.0.0/16	10.2.0.0/24	VNet1

You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.

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**

On the peering connection in VNet2, allow gateway transit.

On the peering connection in VNet1, allow gateway transit.

Create a new virtual network named VNet1.

Recreate peering between VNet1 and VNet2.

Add the 10.33.0.0/16 address space to VNet1.

Remove peering between VNet1 and VNet2.

Remove VNet1.

Answer:

Actions	Answer Area
On the peering connection in VNet2, allow gateway transit.	Recreate peering between VNet1 and VNet2.
On the peering connection in VNet1, allow gateway transit.	Add the 10.33.0.0/16 address space to VNet1.
Create a new virtual network named VNet1.	Remove peering between VNet1 and VNet2.
Recreate peering between VNet1 and VNet2.	
Add the 10.33.0.0/16 address space to VNet1.	
Remove peering between VNet1 and VNet2.	
Remove VNet1.	

Explanation:

Step 1: Remove peering between Vnet1 and VNet2.

You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network. To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.

Step 2: Add the 10.44.0.0/16 address space to VNet1.

Step 3: Recreate peering between VNet1 and VNet2

References: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

38. You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

Name	Type	Resource group
VNET1	Virtual network	RG1
VM1	Virtual machine	RG1

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com.

For contoso.com, you create a virtual network link named link1 as shown in the exhibit. (Click the Exhibit tab.)

Link name: link1

Link state: Completed

Provisioning state: Succeeded

Virtual network details:

Virtual network ID: /subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG2/prov...

Virtual network: VNET1

Configuration:

Enable auto registration

You discover that VM1 can resolve names in contoso.com but cannot resolve names in adatum.com. VM1 can resolve other hosts on the internet.

You need to ensure that VM1 can resolve host names in adatum.com.

What should you do?

- Update the DNS suffix on VM1 to be adatum.com.
- Create an SRV record in the contoso.com zone.
- Configure the name servers for adatum.com at the domain registrar.
- Modify the Access control (IAM) settings for link1.

Answer: C

Explanation:

Adatum.com is a public DNS zone. The Internet top level domain DNS servers need to know which DNS servers to direct DNS queries for adatum.com to. You configure this by configuring the name servers for adatum.com at the domain registrar.

Reference: <https://docs.microsoft.com/en-us/azure/dns/dns-getstarted-portal>

39. You have an Azure subscription named Subscription that contains the resource groups shown in the following table.

Name	Region
RG1	East Asia
RG2	East US

In RG1, you create a virtual machine named VM1 in the East Asia location.

You plan to create a virtual network named VNET1.

You need to create VNET, and then connect VM1 to VNET1.

What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Create VNET1 in RG2, and then set East Asia as the location.
- B. Create VNET1 in a new resource group in the West US location, and then set West US as the location.
- C. Create VNET1 in RG1, and then set East Asia as the location
- D. Create VNET1 in RG1, and then set East US as the location.
- E. Create VNET1 in RG2, and then set East US as the location.

Answer: A,C

Explanation:

A network interface can exist in the same, or different resource group, than the virtual machine you attach it to, or the virtual network you connect it to.

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, also referred to as a region.

Note, Resource groups can span multiple Regions, but VNets only can hold resources (VMs, Network Adapters) that exists in the same region.

So in this scenario, you need to create VNET1 in any RG and set location as East Asia.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

40. You have an Azure subscription that contains a storage account named account1.

You plan to upload the disk files of a virtual machine to account1 from your on-premises network.

The on-premises network uses a public IP address space of 131.107.1.0/24.

You plan to use the disk files to provision an Azure virtual machine named VM1. VM1 will be attached to a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24.

You need to configure account1 to meet the following requirements:

- Ensure that you can upload the disk files to account1.
- Ensure that you can attach the disks to VM1.
- Prevent all other access to account1.

Which two actions should you perform? Each correct selection presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From the Firewalls and virtual networks blade of account1, add the 131.107.1.0/24 IP address range.
- B. From the Firewalls and virtual networks blade of account1, select Selected networks.
- C. From the Firewalls and virtual networks blade of account1, add VNet1.
- D. From the Firewalls and virtual networks blade of account1, select Allow trusted Microsoft services to access this storage account.
- E. From the Service endpoints blade of VNet1, add a service endpoint.

Answer: A,B

Explanation:

By default, storage accounts accept connections from clients on any network. To limit access to selected networks, you must first change the default action. Azure portal

1. Navigate to the storage account you want to secure.
2. Click on the settings menu called Firewalls and virtual networks.
3. To deny access by default, choose to allow access from 'Selected networks'. To allow traffic from all networks, choose to allow access from 'All networks'.
4. Click Save to apply your changes.

Grant access from a Virtual Network

Storage accounts can be configured to allow access only from specific Azure Virtual Networks. By

enabling a Service Endpoint for Azure Storage within the Virtual Network, traffic is ensured an optimal route to the Azure Storage service. The identities of the virtual network and the subnet are also transmitted with each request.

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

41.HOTSPOT

You plan to deploy five virtual machines to a virtual network subnet.

Each virtual machine will have a public IP address and a private IP address.

Each virtual machine requires the same inbound and outbound security rules.

What is the minimum number of network interfaces and network security groups that you require? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of network interfaces:

5
10
15
20



Minimum number of network security groups:

1
2
5
10



Answer:

Answer Area

Minimum number of network interfaces:

5
10
15
20



Minimum number of network security groups:

1
2
5
10



Explanation:

Box 1: 10

One public and one private network interface for each of the five VMs.

Box 2: 1

You can associate zero, or one, network security group to each virtual network subnet and network

interface in a virtual machine. The same network security group can be associated to as many subnets and network interfaces as you choose.

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

42.HOTSPOT

You have an Azure subscription named Subscription1 that contains the resources in the following table.

Name	Type
VM1	Virtual machine
VM2	Virtual machine
LB1	Load balancer

You install the Web Server server role (IIS) on WM1 and VM2, and then add VM1 and VM2 to LB1.

LB1 is configured as shown in the LB1 exhibit. (Click the Exhibit button.)

Essentials ▾

Resource group (change)	Backend pool
VMRG	Backend1 (2 virtual machines)
Location	Health probe
West Europe	Probe1 (HTTP:80/Probe1.htm)
Subscription name (change)	Load balancing rule
Azure Pass	Rule1 (TCP/80)
Subscription ID	NAT rules
e66d2b22-fde8-4af2-9323-d43516f6eb4e	-
SKU	Public IP address
Basic	104.40.178.194 (LB1)

Rule1 is configured as shown in the Rule1 exhibit. (Click the Exhibit button.)

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

VM1 is in the same availability set as VM2.

If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.

If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.

Answer:

Statements**Yes** **No**

VM1 is in the same availability set as VM2.

If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.

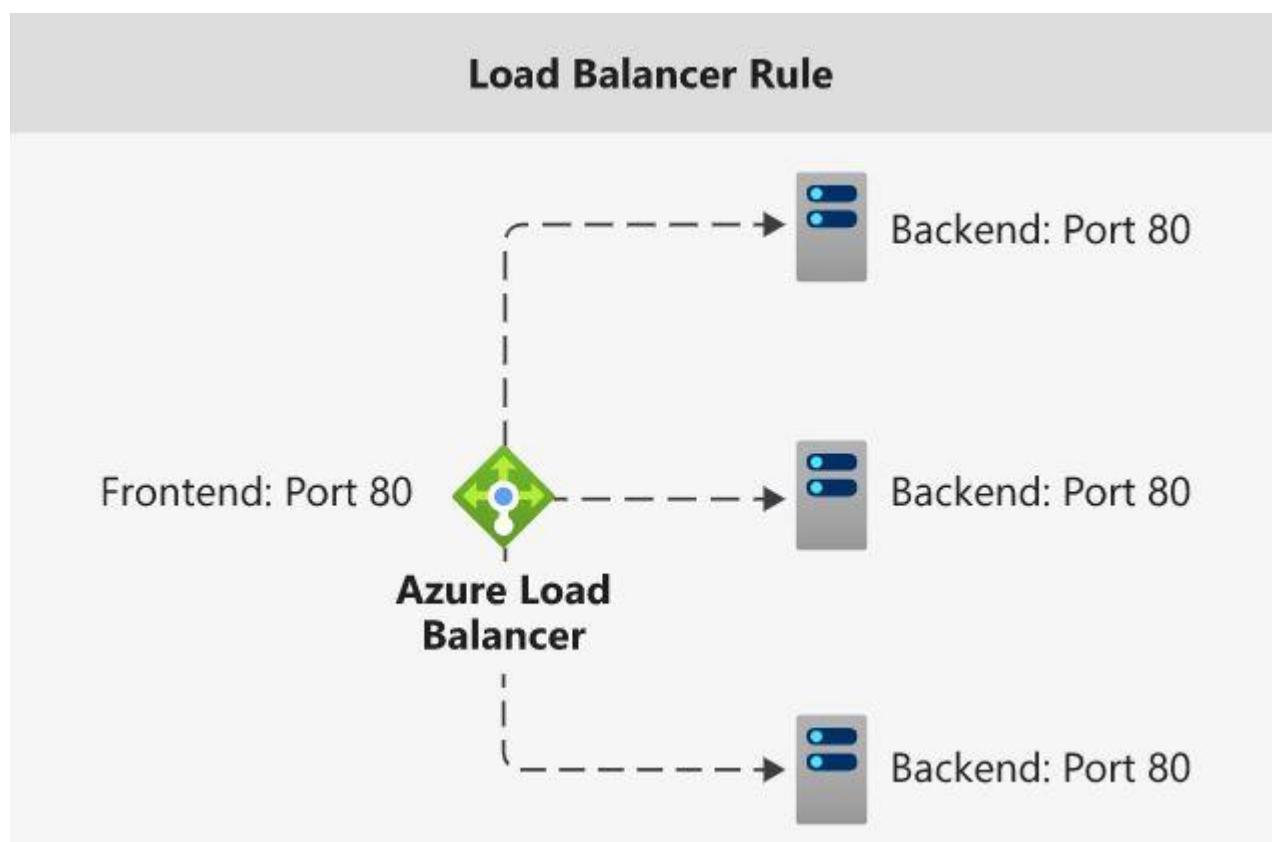
If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.

 Explanation:

To load balance with basic load balancer backend pool virtual machines has to be in a single availability set or virtual machine scale set.

A health probe is used to determine the health status of the instances in the backend pool. During load balancer creation, configure a health probe for the load balancer to use. This health probe will determine if an instance is healthy and can receive traffic.

A Load Balancer rule is used to define how incoming traffic is distributed to the all the instances within the Backend Pool. So if you delete the rule, load balancing won't happen.



Reference: <https://docs.microsoft.com/en-us/azure/load-balancer/skus>

43.HOTSPOT

You have peering configured as shown in the following exhibit.

The screenshot shows the Azure portal interface. On the left, under 'Virtual networks', there is a list of virtual networks: 'test1-vnet', 'testVNET1', 'vNET1', 'vNET2', 'vNET3', 'vNET4', 'vNET5', and 'vNET6'. 'vNET6' is highlighted with a blue selection bar. On the right, under 'vNET6 - Peerings', there is a table with two rows: 'peering1' (Peer: vNET1, Status: Disconnected, Gateway Transit: Enabled) and 'peering2' (Peer: vNET2, Status: Disconnected, Gateway Transit: Disabled).

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

Hosts on vNET6 can communicate with hosts on [answer choice].

vNET6 only	✓
vNET6 and vNET1 only	
vNET6, vNET1, and vNET2 only	
all the virtual networks in the subscription	

To change the status of the peering connection to vNET1 to **Connected**, you must first [answer choice].

add a service endpoint
add a subnet
delete peering1
modify the address space

Answer:

Answer Area

Hosts on vNET6 can communicate with hosts on [answer choice].

vNET6 only
vNET6 and vNET1 only
vNET6, vNET1, and vNET2 only
all the virtual networks in the subscription

To change the status of the peering connection to vNET1 to **Connected**, you must first [answer choice].

add a service endpoint
add a subnet
delete peering1
modify the address space

Explanation:

Box 1: vNET6 only

Peering status to both VNet1 and Vnet2 are disconnected.

Box 2: delete peering1

Peering to Vnet1 is Enabled but disconnected. We need to update or re-create the remote peering to get it back to Initiated state.

Reference:

<https://blog.kloud.com.au/2018/10/19/address-space-maintenance-with-vnet-peering/>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints>

44. Your company has an Azure subscription named Subscription1.

The company also has two on-premises servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a DNS server that has a primary DNS zone named adatum.com.

Adatum.com contains 1,000 DNS records.

You manage Server1 and Subscription1 from Server2.

Server2 has the following tools installed:

- The DNS Manager console
- Azure PowerShell
- Azure CLI 2.0

You need to move the adatum.com zone to Subscription1. The solution must minimize administrative effort.

What should you use?

- A. Azure PowerShell
- B. Azure CLI**
- C. the Azure portal
- D. the DNS Manager console

Answer: B

Explanation:

Azure DNS supports importing and exporting zone files by using the Azure command-line interface (CLI).

Zone file import is not currently supported via Azure PowerShell or the Azure portal.

References: <https://docs.microsoft.com/en-us/azure/dns/dns-import-export>

45. HOTSPOT

You have an Azure subscription that contains the public load balancers shown in the following table.

Name	SKU
LB1	Basic
LB2	Standard

You plan to create six virtual machines and to load balancer requests to the virtual machines.

Each load balancer will load balance three virtual machines.

You need to create the virtual machines for the planned solution.

How should you create the virtual machines? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

The virtual machines that will be load balanced by using LB1 must:

- be connected to the same virtual network.
- be created in the same resource group.
- be created in the same availability set or virtual machine scale set.
- run the same operating system.

The virtual machines that will be load balanced by using LB2 must:

- be connected to the same virtual network.
- be created in the same resource group.
- be created in the same availability set or virtual machine scale set.
- run the same operating system.

Answer:

The virtual machines that will be load balanced by using LB1 must:

- be connected to the same virtual network.
- be created in the same resource group.
- be created in the same availability set or virtual machine scale set.
- run the same operating system.

The virtual machines that will be load balanced by using LB2 must:

- be connected to the same virtual network.
- be created in the same resource group.
- be created in the same availability set or virtual machine scale set.
- run the same operating system.

Explanation:

Box 1: be created in the same availability set or virtual machine scale set.

The Basic tier is quite restrictive. A load balancer is restricted to a single availability set, virtual machine scale set, or a single machine.

Box 2: be connected to the same virtual network

The Standard tier can span any virtual machine in a single virtual network, including blends of scale sets, availability sets, and machines.

References: <https://www.petri.com/comparing-basic-standard-azure-load-balancers>

46.HOTSPOT

You have an Azure virtual network named VNet1 that connects to your on-premises network by using a site-to-site VPN. VMet1 contains one subnet named Subnet1.

Subnet1 is associated to a network security group (NSG) named NSG1. Subnet1 contains a basic internal load balancer named ILB1. ILB1 has three Azure virtual machines in the backend pool.

You need to collect data about the IP addresses that connects to ILB1. You must be able to run interactive queries from the Azure portal against the collected data.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Resource to create:

- An Azure Event Grid
- An Azure Log Analytics workspace
- An Azure Storage account

Resource on which to enable diagnostics:

- ILB1
- NSG1
- The Azure virtual machines

Answer:

Resource to create:

- An Azure Event Grid
- An Azure Log Analytics workspace
- An Azure Storage account

Resource on which to enable diagnostics:

- ILB1
- NSG1
- The Azure virtual machines

Explanation:

Box 1: An Azure Log Analytics workspace

In the Azure portal you can set up a Log Analytics workspace, which is a unique Log Analytics environment with its own data repository, data sources, and solutions

Box 2: ILB1

References:

<https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-quick-create-workspace>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-diagnostics>

47. You have an Azure subscription.

Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by using site-to-site VPNs.

You have a line-of-business app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016.

You need to ensure that the connections to App1 are spread across all the virtual machines.

What are two possible Azure services that you can use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. a public load balancer
- B. Traffic Manager
- C. an Azure Content Delivery Network (CDN)
- D. an internal load balancer**
- E. an Azure Application Gateway**

Answer: D,E

Explanation:

Line-of-business apps means custom apps. Generally these are used by internal staff members of the company.

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Internal Load Balancer provides a higher level of availability and scale by spreading incoming requests across virtual machines (VMs) within the virtual network.

Reference: <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

48. You have an azure subscription that contain a virtual named VNet1. VNet1. contains four subnets named Gatesway, perimeter, NVA, and production.

The NVA contain two network virtual appliance (NVAs) that will network traffic inspection between the perimeter subnet and the production subnet.

You need to implement an Azure load balancer for the NVAs.

The solution must meet the following requirements:

- The NVAs must run in an active-active configuration that uses automatic failover.
- The NVA must load balance traffic to two services on the Production subnet. The services have different IP addresses

Which three actions should you perform? Each correct answer presents parts of the solution. NOTE: Each correct selection is worth one point.

- A. Add two load balancing rules that have HA Ports enabled and Floating IP disabled.
- B. Deploy a standard load balancer.**
- C. Add a frontend IP configuration, two backend pools, and a health prob. 
- D. Add a frontend IP configuration, a backend pool, and a health probe.
- E. Add two load balancing rules that have HA Ports and Floating IP enabled.**
- F. Deploy a basic load balancer.

Answer: B,C,E

Explanation:

A standard load balancer is required for the HA ports.

- Two backend pools are needed as there are two services with different IP addresses.
- Floating IP rule is used where backend ports are reused.

49. You have an Azure subscription that contains a user account named User1.

You need to ensure that User1 can assign a policy to the tenant root management group.

What should you do?

- A. Assign the Owner role to User1, and then instruct User1 to configure access management for Azure resources.
- B. Assign the Global administrator role to User1, and then instruct User1 to configure access management for Azure resources.
- C. Assign the Global administrator role to User1, and then modify the default conditional access policies.
- D. Assign the Owner role to User1, and then modify the default conditional access policies.

Answer: A

Explanation:

To assign a policy to the tenant root management group you have to be an administrator of an Azure subscription. To make a user an administrator of an Azure subscription, assign them the Owner role at the subscription scope. After that assignment user can configure access management for Azure resources.

Reference: <https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

50. You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com – Generic authorization exception."

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- A. From the Roles and administrators blade, assign the Security administrator role to Admin1.
- B. From the Organizational relationships blade, add an identity provider.
- C. From the Custom domain names blade, add a custom domain.
- D. From the Users blade, modify the External collaboration settings.

Answer: D

Explanation:

References:

<https://techcommunity.microsoft.com/t5/Azure-Active-Directory/Generic-authorization-exception-inviting-Azure-AD-gests/td-p/274742>

51. HOTSPOT

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Lock name	Lock type
RG1	None	None
RG2	Lock	Delete

RG1 contains the resources shown in the following table.

Name	Type	Lock name	Lock type
storage1	Storage account	Lock1	Delete
VNET1	Virtual network	Lock2	Read-only
IP1	Public IP address	None	None

RG2 contains the resources shown in the following table.

Name	Type	Lock name	Lock type
storage2	Storage account	Lock1	Delete
VNET2	Virtual network	Lock2	Read-only
IP2	Public IP address	None	None

You need to identify which resources you can move from RG1 to RG2, and which resources you can move from RG2 to RG1.

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

Resources that you can move from RG1 to RG2:

▼

None
IP1 only
IP1 and storage1 only
IP1 and VNET1 only
IP1, VNET1, and storage1

Resources that you can move from RG2 to RG1:

▼

None
IP2 only
IP2 and storage2 only
IP2 and VNET2 only
IP2, VNET2, and storage2

Answer:

Resources that you can move from RG1 to RG2:

None
IP1 only
IP1 and storage1 only
IP1 and VNET1 only
IP1, VNET1, and storage1

Resources that you can move from RG2 to RG1:

None
IP2 only
IP2 and storage2 only
IP2 and VNET2 only
IP2, VNET2, and storage2

Explanation:

Read only and Delete lock won't prevent you from moving resources in different resource groups.

It will prevent you to do the operations in the resource group where the resources are there.

So the correct answer should be

RG1 --> RG2 = IP1, vnet1 and storage1

RG2 --> RG1 = IP2, vnet2 and storage2

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

52.HOTSPOT

You have an Azure subscription named Sub1.

You plan to deploy a multi-tiered application that will contain the tiers shown in the following table.

Tier	Accessible from the Internet	Number of virtual machines
Front-end web server	Yes	10
Business logic	No	100
Microsoft SQL Server database	No	5

You need to recommend a networking solution to meet the following requirements:

- Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines.
- Protect the web servers from SQL injection attacks.

Which Azure resource should you recommend for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines:

▼
an application gateway that uses the Standard tier
an application gateway that uses the WAF tier
an internal load balancer
a network security group (NSG)
a public load balancer

Protect the web servers from SQL injection attacks:

▼
an application gateway that uses the Standard tier
an application gateway that uses the WAF tier
an internal load balancer
a network security group (NSG)
a public load balancer

Answer:

Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines:

▼
an application gateway that uses the Standard tier
an application gateway that uses the WAF tier
an internal load balancer
a network security group (NSG)
a public load balancer

Protect the web servers from SQL injection attacks:

▼
an application gateway that uses the Standard tier
an application gateway that uses the WAF tier
an internal load balancer
a network security group (NSG)
a public load balancer

Explanation:

Box 1: an internal load balancer

Azure Internal Load Balancer (ILB) provides network load balancing between virtual machines that reside inside a cloud service or a virtual network with a regional scope.

Box 2: an application gateway that uses the WAF tier

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities.

References: <https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview>

53.HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named adatum.com.

Adatum.com contains the groups in the following table.

Name	Group type	Membership type	Membership rule
Group1	Security	Dynamic user	(user.city -startsWith "m")
Group2	Microsoft Office 365	Dynamic user	(user.department -notIn ["HR"])
Group3	Microsoft Office 365	Assigned	Not applicable

You create two user accounts that are configured as shown in the following table.

Name	City	Department	Office 365 license assigned
User1	Montreal	Human resources	Yes
User2	Melbourne	Marketing	No

To which groups do User1 and User2 belong? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

User1:

▼

Group1 only
Group2 only
Group3 only
Group1 and Group2 only
Group1 and Group3 only
Group2 and Group3 only
Group1, Group2, and Group3

User2:

▼

Group1 only
Group2 only
Group3 only
Group1 and Group2 only
Group1 and Group3 only
Group2 and Group3 only
Group1, Group2, and Group3

Answer:

User1:

▼

Group1 only
Group2 only
Group3 only
Group1 and Group2 only
Group1 and Group3 only
Group2 and Group3 only
Group1, Group2, and Group3

User2:

▼

Group1 only
Group2 only
Group3 only
Group1 and Group2 only
Group1 and Group3 only
Group2 and Group3 only
Group1, Group2, and Group3

Explanation:

Box 1: Group 1 only

First rule applies

Box 2: Group1 and Group2 only

Both membership rules apply.

References: <https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/create-collections>

54. You have an Azure Active Directory (Azure AD) tenant named contosocloud.onmicrosoft.com.

Your company has a public DNS zone for contoso.com.

You add contoso.com as a custom domain name to Azure AD.

You need to ensure that Azure can verify the domain name.

Which type of DNS record should you create?

A. PTR

B. MX

C. NSEC3

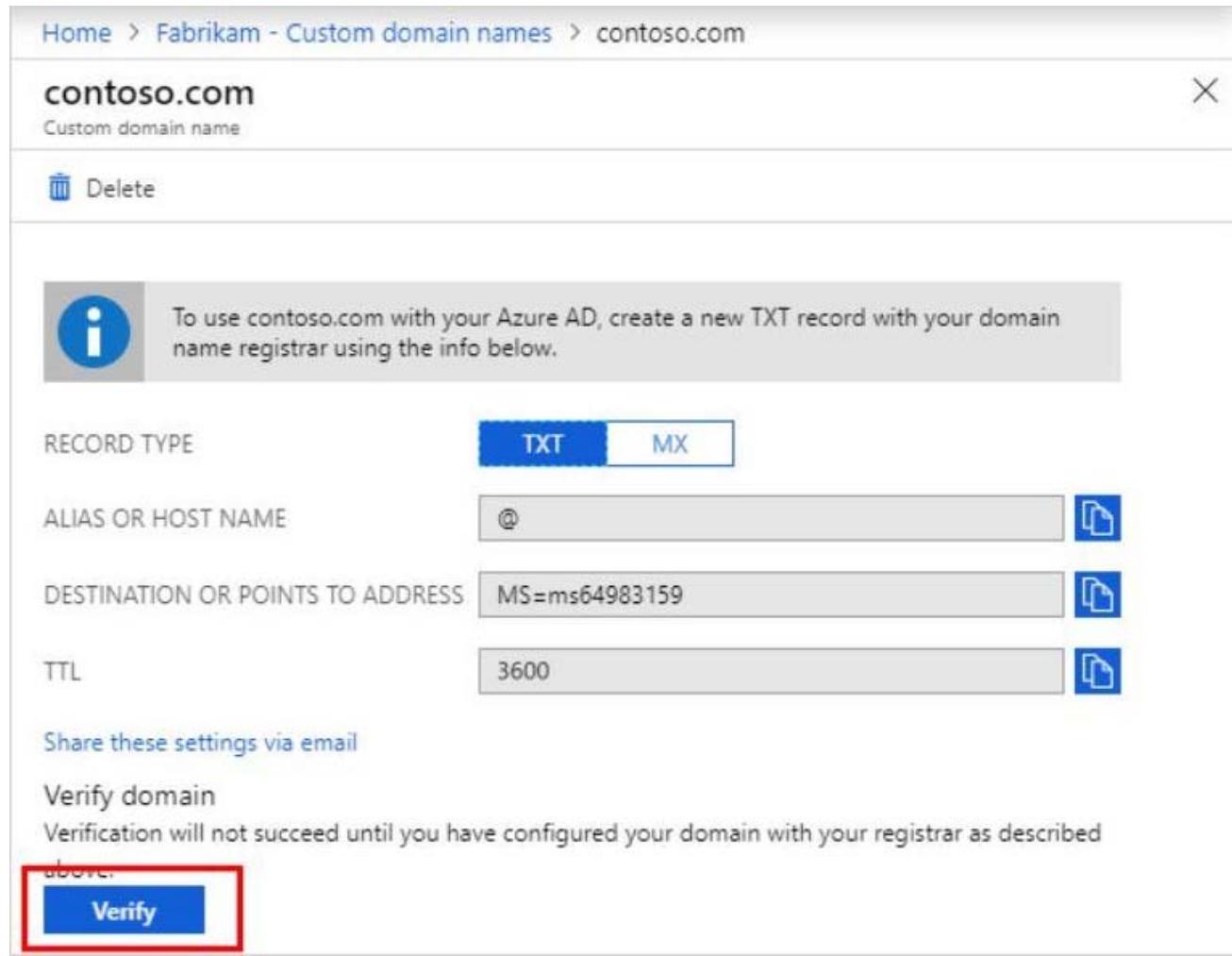
D. RRSIG

Answer: B

Explanation:

TXT or MX: Correct

You can use either a TXT or MX record to verify the custom domain in the Azure AD. MX records can serve the purpose of TXT records



Home > Fabrikam - Custom domain names > contoso.com

contoso.com X

Custom domain name

Delete

RECORD TYPE TXT MX

ALIAS OR HOST NAME Download

DESTINATION OR POINTS TO ADDRESS Download

TTL Download

[Share these settings via email](#)

Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.

Verify

SRV: Incorrect

SRV records are used by various services to specify server locations. When specifying an SRV record in Azure DNS

DNSKEY: Incorrect Choice

This will verify that the records are originating from an authorized sender.

NSEC: Incorrect Choice

This is Part of DNSSEC. This is used for explicit denial-of-existence of a DNS record. It is used to prove a name does not exist.

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#verify-your-custom-domain-name>

[https://www.cloudflare.com/dns/dnssec/how-dnssec-works/#:~:text=DNSKEY%20%2D%20Contains%20a%20public%20signing,s\)%20in%20the%20parent%20zone.](https://www.cloudflare.com/dns/dnssec/how-dnssec-works/#:~:text=DNSKEY%20%2D%20Contains%20a%20public%20signing,s)%20in%20the%20parent%20zone.)

55. You have an Azure subscription that contains a resource group named Test RG.

You use TestRG to validate an Azure deployment.

TestRG contains the following resources:

Name	Type	Description
VM1	Virtual Machine	VM1 is running and configured to back up to Vault1 daily.
VAULT1	Recovery Services Vault	Vault1 includes all backups of VM1.
VNET1	Virtual Network	VNET1 has a resource lock of type Delete.

You need to delete TestRG.

What should you do first?

- A. Modify the backup configurations of VM1 and modify the resource lock type of VNET1.
- B. Turn off VM1 and delete all data in Vault1.
- C. Remove the resource lock from VNET1 and delete all data in Vault1.
- D. Turn off VM1 and remove the resource lock from VNET1.**

Answer: D

Explanation:

When you want to delete the resource, you first need to remove the lock.

References:

<https://docs.microsoft.com/sv-se/azure/azure-resource-manager/management/lock-resources>

56. HOTSPOT

You have an Azure Active Directory tenant named Contoso.com that includes following users:

Name	Role
User1	Cloud device administrator
User2	User administrator

Contoso.com includes following Windows 10 devices:

Name	Join type
Device1	Azure AD registered
Device2	Azure AD joined

You create following security groups in Contoso.com:

Name	Join type	Owner
Group1	Assigned	User1
Group2	Dynamic Device	User2

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
User1 can add Device2 to Group1	<input type="radio"/>	<input type="radio"/>
User2 can add Device1 to Group1	<input type="radio"/>	<input type="radio"/>
User2 can add Device2 to Group2	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can add Device2 to Group1	<input checked="" type="radio"/>	<input type="radio"/>
User2 can add Device1 to Group1	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add Device2 to Group2	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes

User1 is a Cloud Device Administrator.

Device2 is Azure AD joined.

Group1 has the assigned to join type. User1 is the owner of Group1.

Note: Assigned groups - Manually add users or devices into a static group.

Azure AD joined or hybrid Azure AD joined devices utilize an organizational account in Azure AD

Box 2: No

User2 is a User Administrator.

Device1 is Azure AD registered.

Group1 has the assigned join type, and the owner is User1.

Note: Azure AD registered devices utilize an account managed by the end user, this account is either a Microsoft account or another locally managed credential.

Box 3: Yes

User2 is a User Administrator.

Device2 is Azure AD joined.

Group2 has the Dynamic Device join type, and the owner is User2.

References: <https://docs.microsoft.com/en-us/azure/active-directory/devices/overview>

57. You have an Azure policy as shown in the following exhibit.

SCOPE

* Scope (Learn more about setting the scope)

Subscription 1



Exclusions

Subscription 1/ContosoRG1



BASICS

* Policy definition

Not allowed resource types

* Assignment name

Not allowed resource types

Assignment ID

/subscriptions/3eb8d0b6-ce3b-4ce0-a631-9f5321bedabb/providers/Microsoft.Authorization/policyAssignments/0e6fb866b854f54accae2a9

Description

Assigned by:

admin1@contoso.com

PARAMETERS

* Not allowed resource types

Microsoft.Sql/servers



What is the effect of the policy?

Which of the following statements are true?

- A. You can create Azure SQL servers in ContosoRG1 only.
- B. You are prevented from creating Azure SQL servers anywhere in Subscription 1.
- C. You are prevented from creating Azure SQL Servers in ContosoRG1 only.
- D. You can create Azure SQL servers in any resource group within Subscription 1.

Answer: A

Explanation:

You are prevented from creating Azure SQL servers anywhere in Subscription 1 with the exception of ContosoRG1

Reference: <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure>

58.HOTSPOT

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	West US	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
Vault1	Recovery Services vault	Central US	RG1
Vault2	Recovery Services vault	West US	RG2
VM1	Virtual machine	Central US	RG2
storage1	Storage account	West US	RG1
SQL1	Azure SQL database	East US	RG2

In storage1, you create a blob container named blob1 and a file share named share1.

Which resources can be backed up to Vault1 and Vault2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Can use Vault1 for backups:

▼

VM1 only
VM1 and share1 only
VM1 and SQL1 only
VM1, storage1, and SQL1 only
VM1, blob1, share1, and SQL1

Can use Vault2 for backups:

▼

storage1 only
share1 only
VM1 and share1 only
blob1 and share1 only
storage1 and SQL1 only

Answer:

Can use Vault1 for backups:

VM1 only
VM1 and share1 only
VM1 and SQL1 only
VM1, storage1, and SQL1 only
VM1, blob1, share1, and SQL1

Can use Vault2 for backups:

storage1 only
share1 only
VM1 and share1 only
blob1 and share1 only
storage1 and SQL1 only

Explanation:

Box 1: VM1 only

VM1 is in the same region as Vault1.

File1 is not in the same region as Vault1.

SQL is not in the same region as Vault1.

Blobs cannot be backup up to service vaults.

Note: To create a vault to protect virtual machines, the vault must be in the same region as the virtual machines.

Box 2: Share1 only.

Storage1 is in the same region (West USA) as Vault2. Share1 is in Storage1.

Note: After you select Backup, the Backup pane opens and prompts you to select a storage account from a list of discovered supported storage accounts. They're either associated with this vault or present in the same region as the vault, but not yet associated to any Recovery Services vault.

References:

<https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault>

<https://docs.microsoft.com/en-us/azure/backup/backup-afs>

59.DRAG DROP

You have an Azure Linux virtual machine that is protected by Azure Backup.

One week ago, two files were deleted from the virtual machine.

You need to restore the deleted files to an on-premises computer as quickly as possible.

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

Actions	Answer Area
Mount a VHD.	
Copy the files by using File Explorer.	
Download and run a script.	
Select a restore point.	
Copy the files by using AzCopy.	
From the Azure portal, click Restore VM from the vault.	
From the Azure portal, click File Recovery from the vault.	

Answer:

Actions	Answer Area
Mount a VHD.	
Copy the files by using File Explorer.	
Download and run a script.	
Select a restore point.	
Copy the files by using AzCopy.	
From the Azure portal, click Restore VM from the vault.	
From the Azure portal, click File Recovery from the vault.	

Explanation:

To restore files or folders from the recovery point, go to the virtual machine and choose the desired recovery point.

Step 0. In the virtual machine's menu, click **Backup** to open the **Backup dashboard**.

Step 1. In the **Backup dashboard** menu, click **File Recovery**.

Step 2. From the **Select recovery point** drop-down menu, select the recovery point that holds the files you want. By default, the latest recovery point is already selected.

Step 3: To download the software used to copy files from the recovery point, click **Download Executable** (for Windows Azure VM) or **Download Script** (for Linux Azure VM, a python script is generated).

Step 4: Copy the files by using AzCopy

[AzCopy is a command-line utility designed for copying data to/from Microsoft Azure Blob, File, and Table storage, using simple commands designed for optimal performance. You can copy data between a file system and a storage account, or between storage accounts.](#)

References:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy>

60. You have an Azure virtual machine named VM1.

Azure collects events from VM1.

You are creating an alert rule in Azure Monitor to notify an administrator when an error is logged in the System event log of VM1.

You need to specify which resource type to monitor.

What should you specify?

A. metric alert

B. Azure Log Analytics workspace

- C. virtual machine
- D. virtual machine extension

Answer: B

Explanation:

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for analysis of details and correlations. Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.

Azure Log Analytics workspace is also used for on-premises computers monitored by System Center Operations Manager.

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm>

61.HOTSPOT

You have an Azure subscription that contains an Azure Storage account named storage1 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1

You plan to monitor storage1 and to configure email notifications for the signals shown in the following table.

Name	Type	Users to notify
Ingress	Metric	User1 and User3 only
Egress	Metric	User1 only
Delete storage account	Activity log	User1, User2, and User3
Restore blob ranges	Activity log	User1 and User3 only

You need to identify the minimum number of alert rules and action groups required for the planned monitoring.

How many alert rules and action groups should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

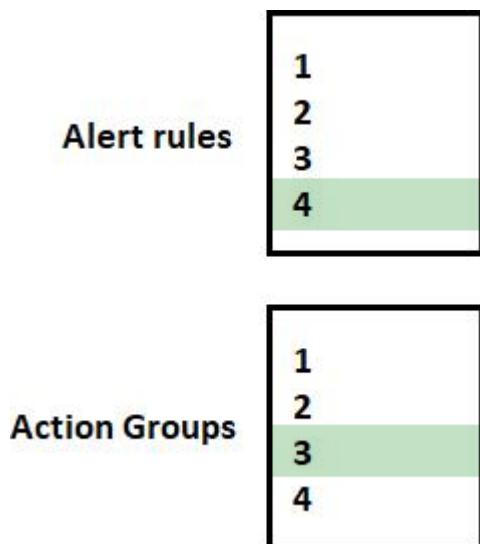
Alert rules

- 1
- 2
- 3
- 4

Action Groups

- 1
- 2
- 3
- 4

Answer:



Explanation:

Box 1: 4

As there are 4 distinct set of resource types (Ingress, Egress, Delete storage account, Restore blob ranges), so you need 4 alert rules. In one alert rule you can't specify different type of resources to monitor. So you need 4 alert rules.

Box 2: 3

There are 3 distinct set of "Users to notify" as (User 1 and User 3), (User1 only), and (User1, User2, and User3). You can't set the action group based on existing group (Group1 and Group2) as there is no specific group for User1 only. So you need to create 3 action group.

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

62. You have two Azure virtual machines named VM1 and VM2.

You have two Recovery Services vaults named RSV1 and RSV2.

VM2 is protected by RSV1.

You need to use RSV2 to protect VM2.

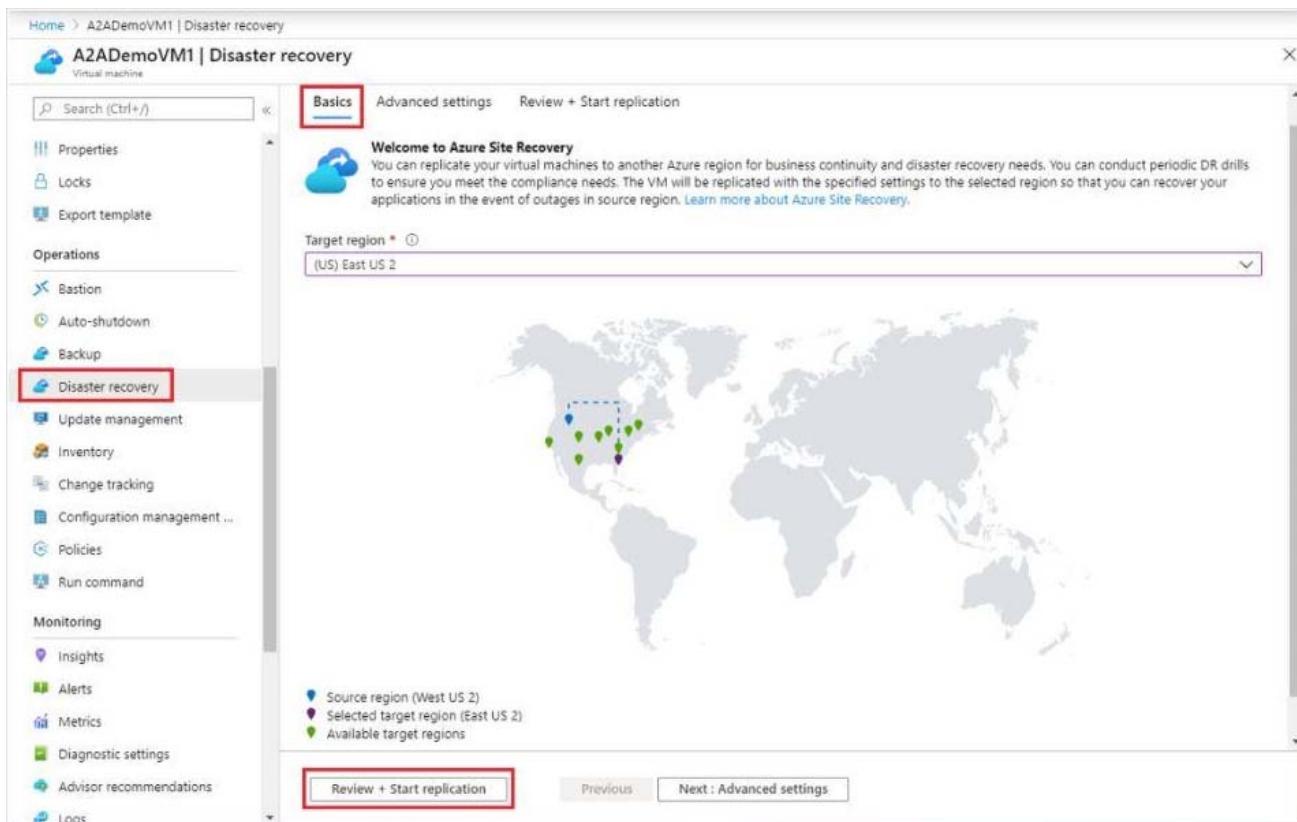
What should you do first?

- A. From the RSV1 blade, click Backup items and stop the VM2 backup.
- B. From the RSV1 blade, click Backup Jobs and export the VM2 backup.
- C. From the RSV1 blade, click Backup. From the Backup blade, select the backup for the virtual machine, and then click Backup.
- D. From the VM2 blade, click Disaster recovery, click Replication settings, and then select RSV2 as the Recovery Services vault.**

Answer: D

Explanation:

The Azure Site Recovery service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and fallback of on-premises machines and Azure virtual machines (VMs).



Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-quickstart>

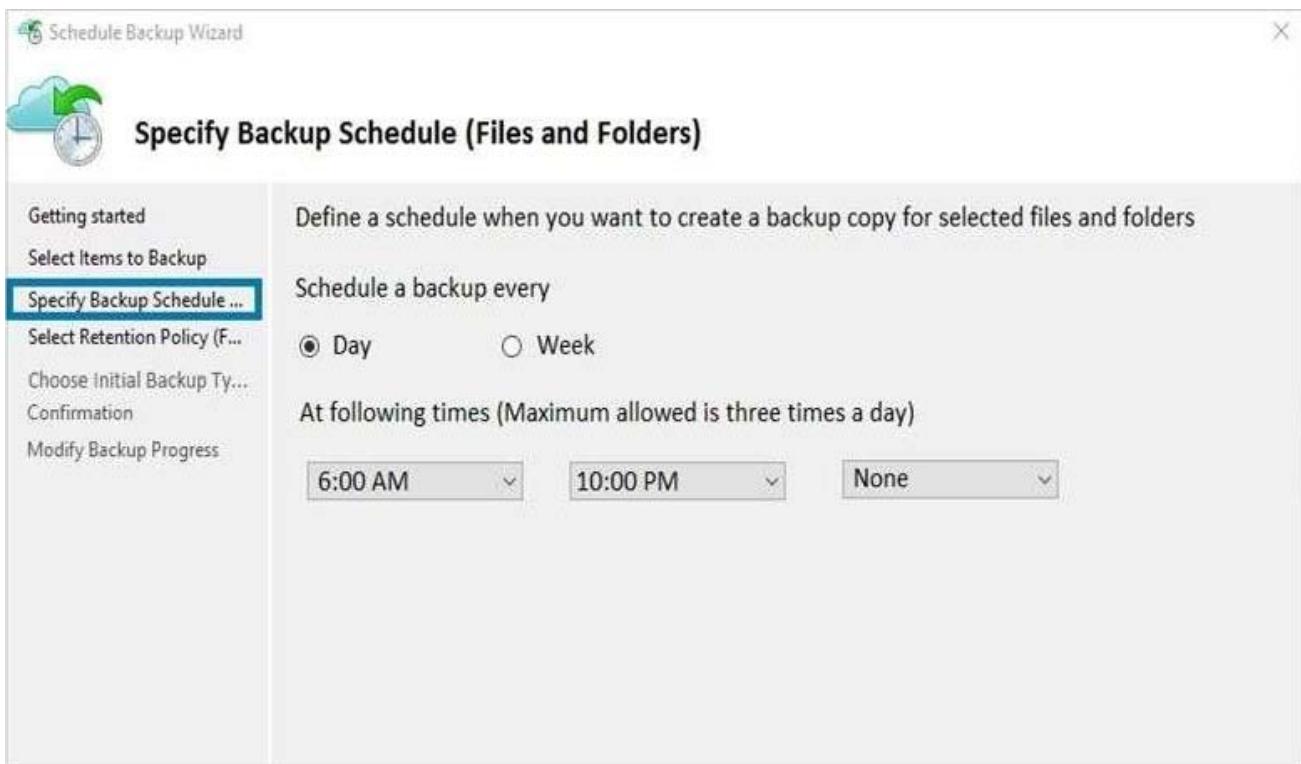
<https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-enable-replication>

63. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group	Location
Vault1	Recovery services vault	RG1	East US
VM1	Virtual machine	RG1	East US
VM2	Virtual machine	RG1	West US

All virtual machines run Windows Server 2016.

On VM1, you back up a folder named Folder1 as shown in the following exhibit.



You plan to restore the backup to a different virtual machine.

You need to restore the backup to VM2.

What should you do first?

- A. From VM2, install the Microsoft Azure Recovery Services Agent
- B. From VM1, install the Windows Server Backup feature
- C. From VM2, install the Windows Server Backup feature
- D. From VM1, install the Microsoft Azure Recovery Services Agent

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-windows-server>

64.HOTSPOT

You have an Azure subscription that contains an Azure Availability Set named WEBPROD-AS-USE2 as shown in the following exhibit.

```
PS Azure:\> az vm availability-set list --resource-group RG1
[
  {
    "id": "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1/providers/Microsoft.Compute/availabilitySets/WEBPROD-AS-USE2",
    "location": "eastus2",
    "name": "WEBPROD-AS-USE2",
    "platformFaultDomainCount": 2,
    "platformUpdateDomainCount": 10,
    "proximityPlacementGroup": null,
    "resourceGroup": "RG1",
    "sku": {
      "capacity": null,
      "name": "Aligned",
      "tier": null
    },
    "statuses": null,
    "tags": {},
    "type": "Microsoft.Compute/availabilitySets",
    "virtualMachines": []
  }
]
Azure:/
```

You add 14 virtual machines to WEBPROD-AS-USE2.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

When Microsoft performs planned maintenance in East US 2, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

If the server rack in the Azure datacenter that hosts WEBPROD-AS-USE2 experiences a power failure, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

Answer:

Answer Area

When Microsoft performs planned maintenance in East US 2, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

If the server rack in the Azure datacenter that hosts WEBPROD-AS-USE2 experiences a power failure, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

Explanation:

Box 1: 2

There are 10 update domains. The 14 VMs are shared across the 10 update domains so four update domains will have two VMs and six update domains will have one VM. Only one update domain is rebooted at a time.

Therefore, a maximum of two VMs will be offline.

Box 2: 7

There are 2 fault domains. The 14 VMs are shared across the 2 fault domains, so 7 VMs in each fault domain.

A rack failure will affect one fault domain so 7 VMs will be offline.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

65.HOTSPOT

You deploy an Azure Kubernetes Service (AKS) cluster that has the network profile shown in the following exhibit.

Network profile

Type (plugin)	Basic (Kubnet)
Pod CIDR	10.244.0.0/16
Service CIDR	10.0.0.0/16
DNS service IP	10.0.0.10
Docker bridge CIDR	172.17.0.1/16

Network options

HTTP application routing ⓘ

Enabled Disabled

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Containers will be assigned an IP address in the [answer choice] subnet.

10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Services in the AKS cluster will be assigned an IP address in the [answer choice] subnet.

10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Answer:

Containers will be assigned an IP address in the [answer choice] subnet.

10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Services in the AKS cluster will be assigned an IP address in the [answer choice] subnet.

10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Explanation:

Box 1: Containers will get the IP address from the virtual network subnet CIDR which is 10.244.0.0/16

Box 2: Services in the AKS cluster will be assigned an IP address in the service CIDR which is 10.0.0.0/16

Reference: <https://docs.microsoft.com/en-us/azure/aks/configure-azure-cni>

66. You plan to create an Azure virtual machine named VM1 that will be configured as shown in the following exhibit.

Create a virtual machine

⚠️ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Basics **Disks** **Networking** **Management** **Advanced** **Tags** **Review + create**

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * MyDev-Test Subscription

Resource group * RG1

[Create new](#)

Instance details

Virtual machine name * ✓

Region * ✓

Availability options ▼

Image * ▼
[Browse all public and private images](#)

Azure Spot instance Yes No

Size *
 1 vcpu, 3.5 GiB memory (ZAR 632.47/month)
[Change size](#)

The planned disk configurations for VM1 are shown in the following exhibit.

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

The planned disk configurations for VM1 are shown in the following exhibit.

Disk options

OS disk type * ▼
 The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Enable Ultra Disk compatibility Yes No
 Ultra Disks are only available when using Managed Disks.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

Advanced

Use managed disks No Yes

Storage account * ▼
[Create new](#)

You need to ensure that VM1 can be created in an Availability Zone.

Which two settings should you modify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Use managed disks
- B. Availability options
- C. OS disk type
- D. Size
- E. Image

Answer: A,E

67. You have an Azure subscription that contains a web app named webapp1. You need to add a custom domain named www.contoso.com to webapp1.

What should you do first?

- A. Upload a certificate.
- B. Add a connection string.
- C. Stop webapp1.
- D. Create a DNS record.**

Answer: B

68. You create an App Service plan named App1 and an Azure web app named webapp1. You discover that the option to create a staging slot is unavailable. You need to create a staging slot for App1.

What should you do first?

- A. From webapp1, modify the Application settings.
- B. From webapp1, add a custom domain.
- C. From App1, scale up the App Service plan.**
- D. From App1, scale out the App Service plan.

Answer: C

Explanation:

Scale up: Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more. You scale up by changing the pricing tier of the App Service plan that your app belongs to.

Reference: <https://docs.microsoft.com/en-us/azure/app-service/manage-scale-up>

69. You download an Azure Resource Manager template based on an existing virtual machine. The template will be used to deploy 100 virtual machines.

You need to modify the template to reference an administrative password. You must prevent the password from being stored in plain text.

What should you create to store the password?

- A. Azure Active Directory (AD) Identity Protection and an Azure policy
- B. a Recovery Services vault and a backup policy
- C. an Azure Key Vault and an access policy**
- D. an Azure Storage account and an access policy

Answer: C

Explanation:

You can use a template that allows you to deploy a simple Windows VM by retrieving the password that is stored in a Key Vault. Therefore the password is never put in plain text in the template parameter file.

References: <https://azure.microsoft.com/en-us/resources/templates/101-vm-secure-password/>

70.HOTSPOT

You plan to deploy an Azure container instance by using the following Azure Resource Manager template.

```
{
  "type": "Microsoft.ContainerInstance/containerGroups",
  "apiVersion": "2018-10-01",
  "name": "webprod",
  "location": "westus",
  "properties": {
    "containers": [
      {
        "name": "webprod",
        "properties": {
          "image": "microsoft/iis:nanoserver",
          "ports": [
            {
              "protocol": "TCP",
              "port": 80
            }
          ],
          "environmentVariables": [],
          "resources": {
            "requests": {
              "memoryInGB": 1.5,
              "cpu": 1
            }
          }
        }
      }
    ],
    "restartPolicy": "OnFailure",
    "ipAddress": [
      "ports": [
        {
          "protocol": "TCP",
          "port": 80
        }
      ],
      "ip": "[parameters('IPAddress')]",
      "type": "Public"
    ]
  }
}
```

```

        "protocol": "TCP",
        "port": 80
    },
    "ip": "[parameters('IPAddress')]",
    "type": "Public"
),
"osType": "Windows"
}

```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the template.

Answer Area

Internet users [answer choice].

can connect to the container from any device
cannot connect to the container
can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, [answer choice].

the container will restart automatically
the container will only restart manually
the container must be redeployed

Answer:

Answer Area

Internet users [answer choice].

can connect to the container from any device
cannot connect to the container
can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, [answer choice].

the container will restart automatically
the container will only restart manually
the container must be redeployed

Explanation:

Box 1: can connect to the container from any device

In the policy "osType": "window" refer that it will create a container in a container group that runs Windows but it won't block access depending on device type.

Box 2: the container will restart automatically

Docker provides restart policies to control whether your containers start automatically when they exit, or when Docker restarts. Restart policies ensure that linked containers are started in the correct order.

Docker recommends that you use restart policies, and avoid using process managers to start containers.

on-failure: Restart the container if it exits due to an error, which manifests as a non-zero exit code.

As the flag is mentioned as "on-failure" in the policy, so it will restart automatically

Reference:

<https://docs.microsoft.com/en-us/cli/azure/container?view=azure-cli-latest>

<https://docs.docker.com/config/containers/start-containers-automatically/>

71. You create an Azure subscription named Subscription1 and an associated Azure Active Directory (Azure AD) tenant named Tenant1.

Tenant1 contains the users in the following table.

Name	Tenant role	Subscription role
ContosoAdmin1@hotmail.com	Global Administrator	Owner
Admin1@contoso.onmicrosoft.com	Global Administrator	Contributor
Admin2@contoso.onmicrosoft.com	Security Administrator	Security Admin
Admin3@contoso.onmicrosoft.com	Conditional Access Administrator	Security Admin

You need to add an Azure AD Privileged Identity Management application to Tenant1.

Which account can you use?

- A. Admin3@contoso.onmicrosoft.com
- B. Admin1@contoso.onmicrosoft.com**
- C. Admin2@contoso.onmicrosoft.com
- D. ContosoAdmin1@hotmail.com

Answer: B

Explanation:

For Azure AD roles in Privileged Identity Management, only a user who is in the Privileged role administrator or Global administrator role can manage assignments for other administrators. You can grant access to other administrators to manage Privileged Identity Management. Global Administrators, Security Administrators, Global readers, and Security Readers can also view assignments to Azure AD roles in Privileged Identity Management.

Only owner can create an subscription and only global administrator can perform Privileged Identity Management changes. So you can create subscription with external user and then promote him to global administrator to get things done.

As it is mentioned as it is associated with azure tenant so that tenant has an AD domain. So in azure AD the default domain ends with onmicrosoft.com. So you can't have Hotmail IDs there. Moreover always remember the principle of least privileges, when you can get your job done with Global Administrator then you should not look for owner for security purpose.

Admin1@contoso.onmicorosft.com : Correct Choice

As Admin1 is Global Administrator and part of default AD domain so Admin1 can add an Azure AD Privileged Identity Management application to Tenant1

Admin3@contoso.onmicrosoft.com : Incorrect Choice

As per the above explanation Admin3 is not Global Administrator, so this option is incorrect.

Admin2@contoso.onmicorosft.com : Incorrect Choice

As per the above explanation Admin2 is not Global Administrator, so this option is incorrect.

ContosoAdmin1@hotmail.com : Incorrect Choice

Although this user is Global Administrator but referring to the least privileges principal and default domain consideration this option is incorrect.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-start>

ed

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance>

72.HOTSPOT

You have an Azure Migrate project that has the following assessment properties:

- Target location: East US
- Storage redundancy: Locally redundant
- Comfort factor: 2.0
- Performance history: 1 month
- Percentile utilization: 95th
- Pricing tier: Standard
- Offer: Pay as you go

You discover the following two virtual machines:

- A virtual machine named VM1 that runs Windows Server 2016 and has 10 CPU cores at 20 percent utilization
- A virtual machine named VM2 that runs Windows Server 2012 and has four CPU cores at 50 percent utilization

How many CPU cores will Azure Migrate recommend for each virtual machine? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

VM1:	2
	4
	10
	20

VM2:	1
	2
	4
	8

Answer:

VM1:	2
	4
	10
	20

VM2:	1
	2
	4
	8

Explanation:

The equation is: 'core usage x comfort factor'. The comfort factor is 2.0.

So VM 1 is 10 cores at 20% utilization which equals 2 cores. Multiply that the comfort factor and you get 4 cores.

VM 2 is 4 cores at 50% utilization which equals 2 cores. Multiply that the comfort factor and you get 4 cores.

73.DRAG DROP

You have an Azure subscription. The subscription includes a virtual network named VNet1.

Currently, VNet1 does not contain any subnets.

You plan to create subnets on VNet1 and to use application security groups to restrict the traffic between the subnets. You need to create the application security groups and to assign them to the subnets.

Which four cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Cmdlets

Answer Area

New-AzureRmVirtualNetwork

New-AzureRmNetworkSecurityGroup

New-AzureRmApplicationSecurityGroup

New-AzureRmNetworkSecurityRuleConfig

Add-AzureRmVirtualNetworkSubnetConfig

Answer:

Cmdlets	Answer Area
New-AzureRmVirtualNetwork	New-AzureRmNetworkSecurityRuleConfig
New-AzureRmNetworkSecurityGroup	New-AzureRmNetworkSecurityGroup
New-AzureRmApplicationSecurityGroup	Add-AzureRmVirtualNetworkSubnetConfig
New-AzureRmNetworkSecurityRuleConfig	New-AzureRmVirtualNetwork
Add-AzureRmVirtualNetworkSubnetConfig	

Explanation:

Step 1: New-AzureRmNetworkSecurityRuleConfig

Step 2: New-AzureRmNetworkSecurityGroup

Step 3: New-AzureRmVirtualNetworkSubnetConfig

Step 4: New-AzureRmVirtualNetwork

Example: Create a virtual network with a subnet referencing a network security group

```
New-AzureRmResourceGroup -Name TestResourceGroup -Location centralus
```

```
$rdpRule = New-AzureRmNetworkSecurityRuleConfig -Name rdp-rule -Description "Allow RDP" -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 3389
```

```
$networkSecurityGroup = New-AzureRmNetworkSecurityGroup -ResourceGroupName
```

```
TestResourceGroup -Location centralus -Name "NSG-FrontEnd" -SecurityRules $rdpRule
```

```
$frontendSubnet = New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix "10.0.1.0/24" -NetworkSecurityGroup $networkSecurityGroup
```

```
$backendSubnet = New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix "10.0.2.0/24" -NetworkSecurityGroup $networkSecurityGroup
```

```
New-AzureRmVirtualNetwork -Name MyVirtualNetwork -ResourceGroupName TestResourceGroup -Location centralus -AddressPrefix "10.0.0.0/16" -Subnet $frontendSubnet,$backendSubnet
```

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.network/new-azurermvirtualnetwork?view=azurerm-powershell-6.7.0>

74.HOTSPOT

You create a virtual machine scale set named Scale1.

Scale1 is configured as shown in the following exhibit.

INSTANCES* Instance count 4 * Instance size (View full pricing details) DS1_v2 (1 vCPU, 3.5 GB) Deploy as low priority 

No

Yes

Use managed disks 

No

Yes

[+ Show advanced settings](#)**AUTOSCALE**Autoscale 

Disabled

Enabled * Minimum number of VMs 2 * Maximum number of VMs 20 

Scale out

* CPU threshold (%) 80 * Number of VMs to increase by 2 

Scale in

* CPU threshold (%) 30 * Number of VMs to decrease by 4 

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

If Scale1 is utilized at 85 percent for six minutes, Scale1 will be running [answer choice].

2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

If Scale1 is first utilized at 25 percent for six minutes, and then utilized at 50 percent for six minutes, Scale1 will be running [answer choice].

2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

Answer:

If Scale1 is utilized at 85 percent for six minutes, Scale1 will be running [answer choice].

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

If Scale1 is first utilized at 25 percent for six minutes, and then utilized at 50 percent for six minutes, Scale1 will be running [answer choice].

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

Explanation:

As cooling period and scale in and scale out durations are not displayed in the graphical view, so we need to consider the default values as below for these settings.

Cool down (minutes): The amount of time to wait before the rule is applied again so that the autoscale actions have time to take effect. Default is 5 minutes.

Duration: The amount of time monitored before the metric and threshold values are compared.

Default is 10 minutes.

Box 1: 4 virtual machines

The Autoscale scale out rule increases the number of VMs by 2 if the CPU threshold is 80% or higher for more than or equals to 10 mins due to default duration for scale in and out is 10 minutes. Since CPU utilization at 85% only lasts for 6 mins, it does not trigger the rules. Hence no of virtual machines will be same as the initial value which is 4.

Box 2: 4 virtual machines

The Autoscale scale in rule decreases the number of VMs by 4 if the CPU threshold is 30% or lower for more than or equal to 10 mins. due to default duration for scale in and out is 10 minutes. Since CPU utilization at 30% only lasts for 6 mins, it does not trigger the rules. Hence after first 6 mins instance count will be same as initial count as 4. After that CPU utilization reached to 50% for 6 mins, which again would not trigger the scale in rule. Therefore no of virtual machines will be same as the initial value which is 4.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-overview>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-best-practices>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-common-scale-patterns>

75.HOTSPOT

You need to create an Azure Storage account that meets the following requirements:

- Minimizes costs
- Supports hot, cool, and archive blob tiers

- Provides fault tolerance if a disaster affects the Azure region where the account resides

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

`az storage account create -g RG1 -n storageaccount1`

--kind	BlobStorage Storage StorageV2	--sku	Standard_GRS Standard_LRS Standard_RAGRS Premium_LRS
--------	-------------------------------------	-------	---

Answer:

Answer Area

`az storage account create -g RG1 -n storageaccount1`

--kind	BlobStorage Storage StorageV2	--sku	Standard_GRS Standard_LRS Standard_RAGRS Premium_LRS
--------	-------------------------------------	-------	---

Explanation:

Box 1: StorageV2

You may only tier your object storage data to hot, cool, or archive in Blob storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts do not support tiering.

General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices.

Box 2: Standard_GRS

Geo-redundant storage (GRS): Cross-regional replication to protect against region-wide unavailability.

76.DRAG DROP

You have an Azure subscription that contains an Azure file share.

You have an on-premises server named Server1 that runs Windows Server 2016.

You plan to set up Azure File Sync between Server1 and the Azure file share.

You need to prepare the subscription for the planned Azure File Sync.

Which two actions should you perform in the Azure subscription? To answer, drag the appropriate actions to the correct targets. Each action 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.

Actions

- Create a Storage Sync Service
- Create a sync group
- Install the Azure File Sync agent
- Run Server Registration

Answer Area

First action:

Action

Second action:

Action

Answer:

Actions

- Create a Storage Sync Service
- Create a sync group
- Install the Azure File Sync agent
- Run Server Registration

Answer Area

First action:

Create a Storage Sync Service

Second action:

Run Server Registration

Explanation:

As per the official MS doc:

The recommended steps to onboard on Azure File Sync for the first with zero downtime while preserving full file fidelity and access control list (ACL) are as follows:

1. Deploy a Storage Sync Service. --> This needs to be done on Azure .
 2. Create a sync group. --> This needs to be done on Azure
 3. Install Azure File Sync agent on the server with the full data set. --> This needs to be done on server1.
 4. Register that server and create a server endpoint on the share. --> This needs to be done on server1.
 5. Let sync do the full upload to the Azure file share (cloud endpoint).
 6. After the initial upload is complete, install Azure File Sync agent on each of the remaining servers.
 7. Create new file shares on each of the remaining servers.
 8. Create server endpoints on new file shares with cloud tiering policy, if desired. (This step requires additional storage to be available for the initial setup.)
 9. Let Azure File Sync agent do a rapid restore of the full namespace without the actual data transfer.
- After the full namespace sync, sync engine will fill the local disk space based on the cloud tiering policy for

the server endpoint.

10. Ensure sync completes and test your topology as desired.
11. Redirect users and applications to this new share.
12. You can optionally delete any duplicate shares on the servers.

First action: Create a Storage Sync Service

The deployment of Azure File Sync starts with placing a Storage Sync Service resource into a resource group of your selected subscription.



Second action: Create a sync group

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on a registered server. A server can have server endpoints in multiple sync groups. You can create as many sync groups as you need to appropriately describe your desired sync topology.

Portal PowerShell Azure CLI

To create a sync group, in the [Azure portal](#), go to your Storage Sync Service, and then select **+ Sync group**:

The screenshot shows the Azure portal interface for a Storage Sync Service named "AFSTest". The left sidebar has navigation links: "Overview" (selected), "Activity log", "Access control (IAM)", and "Tags". The main content area is titled "Sync groups" and shows a table with columns "SYNC GROUP NAME" and "HEALTH". A message at the bottom says "No items to display."

Third action: **Run Server Registration**

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service. A server can only be registered to one Storage Sync Service and can sync with other servers and Azure file shares associated with the same Storage Sync Service.)

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal>

77.HOTSPOT

You have several Azure virtual machines on a virtual network named VNet1.

You configure an Azure Storage account as shown in the following exhibit.

Home > Storage accounts > contoso > Firewalls and virtual networks

contoso – Firewalls and virtual networks

Storage account

Save Discard

Allow access from

All networks Selected networks

Configure network security for your storage accounts. [Learn more](#).

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
VNet1	1	10.2.0.0/16	Enabled	DemoRG	Production subscript....
Prod	10.2.0.0/24	Enabled	Enabled	DemoRG	Production subscript....

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

ADDRESS RANGE

IP address or CIDR

Exceptions

Allow trusted Microsoft services to access this storage account [?](#)

Allow read access to storage logging from any network

Allow read access to storage metrics from any network

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

The virtual machines on the 10.2.0.0/24 subnet will have network connectivity to the file shares in the storage account.

▼

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account.

▼

always
during a backup
never

Answer:

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account.

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account.

always
during a backup
never

Explanation:

Box 1: never

For Subnet 10.2.9.0/24, endpoint (Refer to first endpoint) is not enabled into the storage account shown in the exhibit. Hence there would not be any connectivity to the file shares in storage account. To establish this connection you must have to enable the endpoint.

Box 2: never

After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account. As this required setting is missing, so Azure backup will not be able to take backup of unmanaged disks.

sogupstorage - Firewalls and virtual networks

Allow access from: Selected networks

Virtual networks: No network selected.

Firewall: Add IP ranges to allow access from the internet or your on-premises networks.

ADDRESS RANGE: IP address or CIDR: ...

Exceptions:

- Allow trusted Microsoft services to access this storage account
- Allow read access to storage logging from any network
- Allow read access to storage metrics from any network

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

<https://azure.microsoft.com/en-us/blog/azure-backup-now-supports-storage-accounts-secured-with-azure-firewalls-and-virtual-networks/>

78. You plan to use the Azure Import/Export service to copy files to a storage account.

Which two files should you create before you prepare the drives for the import job? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. an XML manifest file
- B. a driveset CSV file**
- C. a dataset CSV file**
- D. a PowerShell PS1 file
- E. a JSON configuration file

Answer: B,C

Explanation:

B: Modify the driveset.csv file in the root folder where the tool resides.

C: Modify the dataset.csv file in the root folder where the tool resides. Depending on whether you want to import a file or folder or both, add entries in the dataset.csv file

References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-to-files>

79. HOTSPOT

You have an Azure subscription that contains an Azure Storage account.

You plan to copy an on-premises virtual machine image to a container named vmimages.

You need to create the container for the planned image.

Which command should you run? To answer, select the appropriate options in the answer area. NOTE:

Each correct selection is worth one point.

azcopy

make
sync
copy

<https://mystorageaccount.>

blob
dfs
queue
table
images
file

.core.windows.net/vmimages'

Answer:

azcopy

make
sync
copy

<https://mystorageaccount.core.windows.net/vmimages>

blob
dfs
queue
table
images
file

Explanation:

Box 1: make

Here the purpose is to 'create a container'. So the correct command would be azcopy make.

Box 2: blob

The requirement is for storing that image, it's not used to build AKS. So blob is correct option.

Reference: <https://adamtheautomator.com/azcopy-copy-files/>

80.HOTSPOT

You have a sync group that has the endpoints shown in the following table.

Name	Type
Endpoint1	Cloud endpoint
Endpoint2	Server endpoint
Endpoint3	Server endpoint

Cloud tiering is enabled for Endpoint3.

You add a file named File1 to Endpoint1 and a file named File2 to Endpoint2.

You need to identify on which endpoints File1 and File2 will be available **within 24 hours** of adding the files.

What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

File1:

Endpoint1 only
Endpoint3 only
Endpoint2 and Endpoint3 only
Endpoint1, Endpoint2, and Endpoint3

File2:

Endpoint1 only
Endpoint3 only
Endpoint2 and Endpoint3 only
Endpoint1, Endpoint2, and Endpoint3

Answer:

File1:



Endpoint1 only
Endpoint3 only
Endpoint2 and Endpoint3 only
Endpoint1, Endpoint2, and Endpoint3

File2:

Endpoint1 only
Endpoint3 only
Endpoint2 and Endpoint3 only
Endpoint1, Endpoint2, and Endpoint3

Explanation:

File1: Endpoint3 only

Cloud Tiering: A switch to enable or disable cloud tiering. When enabled, cloud tiering will tier files to your Azure file shares. This converts on-premises file shares into a cache, rather than a complete copy of the dataset, to help you manage space efficiency on your server. With cloud tiering, infrequently used or accessed files can be tiered to Azure Files.

File2: Endpoint1, Endpoint2, and Endpoint3

References: <https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-cloud-tiering>

81.HOTSPOT

You have an Azure subscription that contains an Azure Directory (Azure AD) tenant named contoso.com. The tenant is synced to the on-premises Active Directory domain. The domain contains the users shown in the following table.

Name	Role
SecAdmin1	Security administrator
BillAdmin1	Billing administrator
User1	Reports reader

You enable self-service password reset (SSPR) for all users and configure SSPR to have the following authentication methods:

- Number of methods required to reset: 2
- Methods available to users: Mobile phone, Security questions
- Number of questions required to register: 3
- Number of questions required to reset: 3

You select the following security questions:

- What is your favorite food?
- In what city was your first job?
- What was the name of your first pet?

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
SecAdmin1 must answer the following question if he wants to reset his password: In what city was your first job?	<input type="radio"/>	<input type="radio"/>
BillAdmin1 must answer the following question if he wants to reset his password: What is your favorite food?	<input type="radio"/>	<input type="radio"/>
User1 must answer the following question if he wants to reset his password: What was the name of your first pet?	<input type="radio"/>	<input type="radio"/>
Answer:		
Statements	Yes	No
SecAdmin1 must answer the following question if he wants to reset his password: In what city was your first job?	<input type="radio"/>	<input checked="" type="checkbox"/>
BillAdmin1 must answer the following question if he wants to reset his password: What is your favorite food?	<input type="radio"/>	<input checked="" type="checkbox"/>
User1 must answer the following question if he wants to reset his password: What was the name of your first pet?	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

Box 1: No

Administrator accounts are special accounts with elevated permissions. To secure them, the following restrictions apply to changing passwords of administrators:

On-premises enterprise administrators or domain administrators cannot reset their password through Self-service password reset (SSPR). They can only change their password in their on-premises environment. Thus, we recommend not syncing on-prem AD admin accounts to Azure AD.

An administrator cannot use secret Questions & Answers as a method to reset password.

Box 2: Yes

Self-service password reset (SSPR) is an Azure Active Directory feature that enables employees to reset their passwords without needing to contact IT staff.

Box 3: Yes

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

82. You have an Azure Active Directory (Azure AD) tenant named contoso.com that is synced to an Active Directory domain.

The tenant contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account
User4	Member	Windows Server Active Directory

The users have the attributes shown in the following table.

Name	Office phone	Mobile phone
User1	222-555-1234	222-555-2345
User2	null	null
User3	222-555-1234	222-555-2346
User4	222-555-1234	null

You need to ensure that you can enable Azure Multi-Factor Authentication (MFA) for all four users.

Solution: You add an office phone number for User2.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

User3 requires a user account in Azure AD.

Note: Your Azure AD password is considered an authentication method. It is the one method that cannot be disabled.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

83. You have an Azure Active Directory (Azure AD) tenant named contoso.com that is synced to an Active Directory domain.

The tenant contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account
User4	Member	Windows Server Active Directory

The users have the attribute shown in the following table.

Name	Office phone	Mobile phone
User1	222-555-1234	222-555-2345
User2	null	null
User3	222-555-1234	222-555-2346
User4	222-555-1234	null

You need to ensure that you can enable Azure Multi-Factor Authentication (MFA) for all four users.

Solution: You add a mobile phone number for User2 and User4.

Does this meet the Goal?

A. Yes

B. No

Answer: B

Explanation:

User3 requires a user account in Azure AD.

Note: Your Azure AD password is considered an authentication method. It is the one method that cannot be disabled.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

84. You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

A. Azure Data Lake Store

B. a virtual machine

C. the Azure File Sync Storage Sync Service

D. Azure Blob storage

Answer: D

Explanation:

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

The maximum size of an Azure Files Resource of a file share is 5 TB.

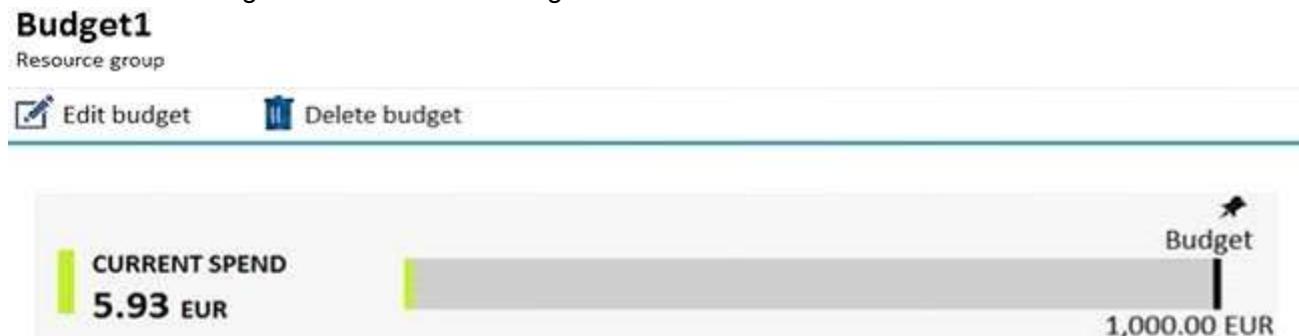
Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

85. HOTSPOT

You have a pay-as-you-go Azure subscription that contains the virtual machines shown in the following table.

Name	Resource group	Daily cost
VM1	RG1	20 euros
VM2	RG2	30 euros

You create the budget shown in the following exhibit.



The AG1 action group contains a user named `admin@contoso.com` only.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

When the maximum amount in Budget1 is reached.

[answer choice].

VM1 and VM2 are turned off
VM1 and VM2 continue to run
VM1 is turned off, and VM2 continues to run

Based on the current usage costs of the virtual machines. [answer choice].

no email notifications will be sent each month
one email notification will be sent each month
two email notifications will be sent each month
three email notifications will be sent each month

Answer:

When the maximum amount in Budget1 is reached.

[answer choice].

VM1 and VM2 are turned off
VM1 and VM2 continue to run
VM1 is turned off, and VM2 continues to run

Based on the current usage costs of the virtual machines. [answer choice].

no email notifications will be sent each month
one email notification will be sent each month
two email notifications will be sent each month
three email notifications will be sent each month

Explanation:

Box 1: VM1 and VM2 continues to run

When the budget thresholds you've created are exceeded, only notifications are triggered. None of your resources are affected and your consumption isn't stopped. You can use budgets to compare and track spending as you analyze costs.

Box 2: one email notification will be sent each month

Budget alerts for Resource Group RG1, which include VM1, but not VM2. VM1 consumes 20 Euro/day.

The 50% ,500 Euro limit, will be reached in 25 days, and an email will be sent.

The 70% and 100% alert conditions will not be reached within a month, and they don't trigger email actions anyway.

References:

<https://docs.microsoft.com/en-gb/azure/cost-management-billing/costs/tutorial-acm-create-budgets>

<https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending>

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

Name	Role
User1	<i>None</i>
User2	Global administrator
User3	Cloud device administrator
User4	Intune administrator

Adatum.com has the following configurations:

Users may join devices to Azure AD is set to User1.

Additional local administrators on Azure AD joined devices is set to None.

You deploy Windows 10 to a computer named Computer. User1 joins Computer1 to adatum.com.

You need to identify which users are added to the local Administrators group on Computer1.

- A. User1 only
- B. User1, User2, and User3 only
- C. User1 and User2 only**
- D. User1, User2, User3, and User4
- E. User2 only

Answer: C

Explanation:

Users may join devices to Azure AD - This setting enables you to select the users who can register their devices as Azure AD joined devices. The default is All.

Additional local administrators on Azure AD joined devices - You can select the users that are granted local administrator rights on a device. Users added here are added to the Device Administrators role in Azure AD. Global administrators, here User2, in Azure AD and device owners are granted local administrator rights by default.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

87.HOTSPOT

You have a sync group named Sync1 that has a cloud endpoint. The cloud endpoint includes a file named File1.txt.

You on-premises network contains servers that run Windows Server 2016.

The servers are configured as shown in the following table.

Name	Share	Share contents
Server1	Share1	File1.txt, File2.txt
Server2	Share2	File2.txt, File3.txt

You add Share1 as an endpoint for Sync1. One hour later, you add Share2 as an endpoint for Sync1.

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
On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.	<input type="radio"/>	<input type="radio"/>
On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.	<input type="radio"/>	<input type="radio"/>
File1.txt Share1 replicates to Share2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
File1.txt Share1 replicates to Share2.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Explanation:

Statement 1: Yes

If you add an Azure file share that has an existing set of files as a cloud endpoint to a sync group, the existing files are merged with any other files that are already on other endpoints in the sync group.

Statement 2: No

Files present in any server endpoint will not be overwritten by the files present in cloud endpoint.

Hence this statement is false.

If you add a server location with an existing set of files as a server endpoint to a sync group, those files will be merged with any other files already on other endpoints in the sync group but not vice versa.

Statement 3: Yes

Azure File Sync has a simple architecture : cloud endpoints, which is the Azure File Sync service and server endpoints, which are the registered servers with the service. On top of that, we have Sync Groups, which combine one cloud endpoint with one or more server endpoints. All members of this group will receive the replicated data where the central location will be the cloud endpoint.

References:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning>

<http://techgenix.com/azure-file-sync-replicating-data/>

88. You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Kind	Performance	Replication	Access tier
Storage1	Storage (general purpose v1)	Premium	Geo-redundant storage (GRS)	None
Storage2	StorageV2 (general purpose v2)	Standard	Locally-redundant storage (LRS)	Cool
Storage3	StorageV2 (general purpose v2)	Premium	Read-access geo-redundant storage (RA-GRS)	Hot
Storage4	BlobStorage	Standard	Locally-redundant storage (LRS)	Hot

You need to identify which storage account can be converted to zone-redundant storage (ZRS) replication by requesting a live migration from Azure support.

What should you identify?

- A. Storage1
- B. Storage2
- C. Storage3
- D. Storage4

Answer: B

Explanation:

ZRS currently supports standard general-purpose v2, FileStorage and BlockBlobStorage storage account types.

89.HOTSPOT

You have an Azure virtual machine named VM1 and a Recovery Services vault named Vault1.

You create a backup Policy1 as shown in the exhibit. (Click the Exhibit tab.)

Policy1

 Associated items

 Delete

 Save

 Discard

Backup schedule

* Frequency

Daily

* Time

2:00 AM

* Timezone

(UTC) Coordinated Universal Time

Retention range

Retention of daily backup point.

* At

For

2:00 AM

5

Day(s)

Retention of weekly backup point.

* On

* At

For

Sunday

2:00 AM

20

Week(s)

Retention of monthly backup point.

Week Based **Day Based**

* On

* At

For

2

2:00 AM

24

Month(s)

Retention of yearly backup point.

Week Based **Day Based**

* In

* On

* At

For

January

9

2:00 AM

5

Year(s)

You configure the backup of VM1 to use Policy1 on Thursday, January 1.

You need to identify the number of available recovery points for VM1.

How many recovery points are available on January 8 and on January 15? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

January 8 at 14:00:

	▼
5	
6	
8	
9	

January 15 at 14:00:

	▼
5	
8	
17	
19	

Answer:

January 8 at 14:00:

	▼
5	
6	
8	
9	

January 15 at 14:00:

	▼
5	
8	
17	
19	

Explanation:

Box 1: 6

4 daily + 1 weekly + monthly

Box 2: 8

4 daily + 2 weekly + monthly + yearly

90.HOTSPOT

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
Vault1	Recovery Services vault	West Europe	RG1
storage1	Storage account	East US	RG2
storage2	Storage account	West US	RG1
storage3	Storage account	West Europe	RG2
Analytics1	Log Analytics workspace	East US	RG1
Analytics2	Log Analytics workspace	West US	RG2
Analytics3	Log Analytics workspace	West Europe	RG1

You plan to configure Azure Backup reports for Vault1.

You are configuring the Diagnostics settings for the AzureBackupReports log.

Which storage accounts and which Log Analytics workspaces can you use for the Azure Backup reports of Vault1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Storage accounts:

storage1 only	▼
storage2 only	▼
storage3 only	▼
storage1, storage2, and storage3	▼

Log Analytics workspaces:

Analytics1 only	▼
Analytics2 only	▼
Analytics3 only	▼
Analytics1, Analytics2, and Analytics3	▼

Answer:

Storage accounts:

storage1 only
storage2 only
storage3 only
storage1, storage2, and storage3



Log Analytics workspaces:

Analytics1 only
Analytics2 only
Analytics3 only
Analytics1, Analytics2, and Analytics3



Explanation:

Log Analytics are independent of locations

Box 1: storage3 only

Vault1 and storage3 are both in West Europe.

Box 2: Analytics3

Vault1 and Analytics3 are both in West Europe.

References: <https://docs.microsoft.com/en-us/azure/backup/backup-azure-configure-reports>

91.HOTSPOT

You have Azure subscription that includes following Azure file shares:

Name	In storage account	Location
share1	storage1	West US
share2	storage1	West US

You have the following on-premises servers:

Name	Folders
Server1	D:\Folder1, E:\Folder2
Server2	D:\Data

You create a Storage Sync Service named Sync1 and an Azure File Sync group named Group1.

Group1 uses share1 as a cloud endpoint.

You register Server1 and Server2 in Sync1.

You add D:\Folder1 on Server1 as a server endpoint of Group1.

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
share2 can be added as a cloud endpoint for Group1	<input type="radio"/>	<input type="radio"/>

E:\Folder2 on Server1 can be added as a server endpoint for Group1	<input type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------

D:\Data on Server2 can be added as a server endpoint for Group1	<input type="radio"/>	<input type="radio"/>
---	-----------------------	-----------------------

Answer:

Statements	Yes	No
share2 can be added as a cloud endpoint for Group1	<input type="radio"/>	<input checked="" type="radio"/>

Azure File Sync does not support more than one server endpoint from the same server in the same Sync Group.

E:\Folder2 on Server1 can be added as a server endpoint for Group1	<input checked="" type="radio"/>	<input type="radio"/>	
--	----------------------------------	-----------------------	---

D:\Data on Server2 can be added as a server endpoint for Group1	<input checked="" type="radio"/>	<input type="radio"/>
---	----------------------------------	-----------------------

Explanation:

Box 1: No

Group1 already has a cloud endpoint named Share1.

A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints.

Box 2: Yes

Yes, one or more server endpoints can be added to the sync group.

Box 3: Yes

Yes, one or more server endpoints can be added to the sync group.

References: <https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

92. You have an Azure subscription that contains the following resources:

- 100 Azure virtual machines
- 20 Azure SQL databases
- 50 Azure file shares

You need to create a daily backup of all the resources by using Azure Backup.

What is the minimum number of backup policies that you must create?

- A. 1
- B. 2
- C. 3**
- D. 150
- E. 170

Answer: C**Explanation:**

There is a limit of 100 VMs that can be associated to the same backup policy from portal. We recommend

that for more than 100 VMs, create multiple backup policies with same schedule or different schedule.

One policy for VMS, one for SQL databases, and one for the file shares.

References: <https://docs.microsoft.com/en-us/azure/backup/backup-azure-vm-backup-faq>

93. You have an Azure subscription that includes data in following locations:

Name	Type
container1	Blob container
share1	Azure files share
DB1	SQL database
Table1	Azure Table

You plan to export data by using Azure import/export job named Export1.

You need to identify the data that can be exported by using Export1.

Which data should you identify?

- A. DB1
- B. Table1
- C. container1**
- D. Share1

Answer: C

Explanation:

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage.

Only the Blob service is supported with the Export job feature

Supported storage types

The following list of storage types is supported with Azure Import/Export service.

Job	Storage Service	Supported	Not supported
Import	Azure Blob storage	Block Blobs and Page blobs supported	Azure Files not supported
	Azure File storage	Files supported	
Export	Azure Blob storage	Block blobs, Page blobs, and Append blobs supported	Azure Files not supported

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements>

94. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System log on VM1 within an hour.

Solution: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Alerts in Azure Monitor can identify important information in your Log Analytics repository. They are created by alert rules that automatically run log searches at regular intervals, and if results of the log search match particular criteria, then an alert record is created and it can be configured to perform an automated response.

The Log Analytics agent collects monitoring data from the guest operating system and workloads of virtual machines in Azure, other cloud providers, and on-premises. It collects data into a Log Analytics workspace.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-response>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

95. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System log on VM1 within an hour.

Solution: You create an event subscription on VM1. You create an alert in Azure Monitor and specify VM1 as the source.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

References: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

96. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG1 and West US.

Does this meet the goal?

A. Yes

B. NO

Answer: A

Explanation:

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

References: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

97. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location
VNET1	Virtual network	East US
IP1	Public IP address	West Europe
RT1	Route table	North Europe

You need to create a network interface named NIC1.

In which location can you create NIC1?

A. East US and North Europe only.

B. East US and West Europe only.

C. East US, West Europe, and North Europe.

D. East US only.

Answer: D

Explanation:

A virtual network is required when you create a NIC. Select the virtual network for the network interface.

You can only assign a network interface to a virtual network that exists in the same subscription and location as the network interface. Once a network interface is created, you cannot change the virtual network it is assigned to. The virtual machine you add the network interface to must also exist in the same location and subscription as the network interface.

References: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

98.DRAG DROP

You need to use Azure Automation State Configuration to manage the ongoing consistency of virtual machine configurations.

Which five actions should you perform in sequence? To answer, move the appropriate action from the list of actions to the answer area and arrange them in the correct order. NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Answer Area

Compile a configuration into a node configuration.

Onboard the virtual machines to Azure Automation State Configuration.

Upload a configuration to Azure Automation State Configuration.

Check the compliance status of the node.

Assign tags to the virtual machines.

Assign the node configuration.

Create a management group.

Answer:

Actions

Answer Area

Compile a configuration into a node configuration.

Onboard the virtual machines to Azure Automation State Configuration.

Onboard the virtual machines to Azure Automation State Configuration.

Upload a configuration to Azure Automation State Configuration.

Upload a configuration to Azure Automation State Configuration.

Compile a configuration into a node configuration.

Check the compliance status of the node.

Assign the node configuration.

Assign tags to the virtual machines.

Check the compliance status of the node.

Assign the node configuration.

Create a management group.

Explanation:

Step 1: Upload a configuration to Azure Automation State Configuration.

Import the configuration into the Automation account.

Step 2: Compile a configuration into a node configuration.

A DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

Step 3: Onboard the virtual machines to Azure Automation State Configuration. Onboard the Azure VM for management with Azure Automation State Configuration

Step 4: Assign the node configuration

Step 5: Check the compliance status of the node

Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node. On the blade for an individual report, you can see the following status information for the corresponding consistency check:

The report status — whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant"

References: <https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

99. You have an Azure virtual machine named VM1.

You use Azure Backup to create a backup of VM1 named Backup1.

After creating Backup1, you perform the following changes to VM1:

- Modify the size of VM1.
- Copy a file named Budget.xls to a folder named Data.
- Reset the password for the built-in administrator account.
- Add a data disk to VM1.

An administrator uses the Replace existing option to restore VM1 from Backup1.

You need to ensure that all the changes to VM1 are restored.

Which change should you perform again?

- A. Modify the size of VM1.
- B. Add a data disk.
- C. Reset the password for the built-in administrator account.
- D. Copy Budget.xls to Data.**

Answer: D

Explanation:

The scenario mentioned in the question, we are using the replace option. So in this case we would lose the existing data written to the disk after the backup was taken. The file was copied to the disk after the backup was taken. Hence, we would need to copy the file once again.

References:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms#replace-existing-disks>

100. You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Region	Resource group
RG1	Resource group	West Europe	<i>Not applicable</i>
RG2	Resource group	North Europe	<i>Not applicable</i>
Vault1	Recovery Services vault	West Europe	RG1

You create virtual machines in Subscription1 as shown in the following table.

Name	Resource group	Region	Operating system
VM1	RG1	West Europe	Windows Server 2016
VM2	RG1	North Europe	Windows Server 2016
VM3	RG2	West Europe	Windows Server 2016
VMA	RG1	West Europe	Ubuntu Server 18.04
VMB	RG1	North Europe	Ubuntu Server 18.04
VMC	RG2	West Europe	Ubuntu Server 18.04

You plan to use Vault1 for the backup of as many virtual machines as possible.

Which virtual machines can be backed up to Vault1?

- A. VM1, VM3, VMA, and VMC only
- B. VM1 and VM3 only
- C. VM1, VM2, VM3, VMA, VMB, and VMC
- D. VM1 only
- E. VM3 and VMC only

Answer: A

Explanation:

To create a vault to protect virtual machines, the vault must be in the same region as the virtual machines. If you have virtual machines in several regions, create a Recovery Services vault in each region.

References: <https://docs.microsoft.com/bs-cyril-ba/azure/backup/backup-create-rs-vault>

101. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100
- Source: Any

- Source port range: *
- Destination: *
- Destination port range: 3389
- Protocol: UDP
- Action: Allow

VM1 connects to Subnet1. NSG1-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You modify the custom rule for NSG-VM1 to use the internet as a source and TCP as a protocol.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

NSGs deny all inbound traffic except from virtual network or load balancers. For inbound traffic, Azure processes the rules in a network security group associated to a subnet first, and then the rules in a network security group associated to the network interface.

By default NSG rule to allow traffic through RDP port 3389 is not created automatically during the creation of VM, unless you change the setting during creation. Subnets usually do not have any NSG associated unless you go out of the way to do so, which this scenario does. When you create that extra NSG, it won't have an RDP rule by default, thus blocking inbound connections. Request first goes to NSG-Subnet1 and as there is no allow rule for RDP so it will block the request by default. Since the Subnet NSG (the one with the default rules) is evaluated first, it blocks the inbound RDP connection.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

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

102. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100
- Source: Any
- Source port range: *
- Destination: *
- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 connects to Subnet1. NSG1-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

103. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1

- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100

- Source: Any

- Source port range: *

- Destination: *

- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 connects to Subnet1. NSG1-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

104.HOTSPOT

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

Name	Operating system	Connects to
VM1	Windows Server 2019	Subnet1
VM2	Windows Server 2019	Subnet2

VM1 and VM2 use public IP addresses. From Windows Server 2019 on VM1 and VM2, you allow inbound Remote Desktop connections.

Subnet1 and Subnet2 are in a virtual network named VNET1.

The subscription contains two network security groups (NSGs) named NSG1 and NSG2. NSG1 uses only the default rules.

NSG2 uses the default and the following custom incoming rule:

- Priority: 100
- Name: Rule1
- Port: 3389
- Protocol: TCP
- Source: Any
- Destination: Any
- Action: Allow

NSG1 connects to Subnet1. NSG2 connects to the network interface of VM2.

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

Answer Area

Statements	Yes	No
From the Internet, you can connect to VM1 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to VM2 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to VM2 by using Remote Desktop	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

1. VM1 has default rules which denies any port open for inbound rules

Statements	Yes	No
From the Internet, you can connect to VM1 by using Remote Desktop.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to VM2 by using Remote Desktop. NSG2 has custom Rule1, allowing RDP port 3389 with TCP.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can connect to VM2 by using Remote Desktop	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

VM1 and VM2 are in the same Vnet. By default, communication is allowed.

Box 1: No

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Box 2: Yes

NSG2 will allow this.

Box 3: Yes

NSG2 will allow this.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

105.HOTSPOT

You manage two Azure subscriptions named Subscription1 and Subscription2.

Subscription1 has following virtual networks:

Name	Address space	Location
VNET1	10.10.10.0/24	West Europe
VNET2	172.16.0.0/16	West US

The virtual networks contain the following subnets:

Name	Address space	Location
Subnet11	10.10.10.0/24	VNET1
Subnet21	172.16.0.0/18	VNET2
Subnet22	172.16.128.0/18	VNET2

Subscription2 contains the following virtual network:

- Name: VNETA
- Address space: 10.10.128.0/17
- Location: Canada Central

VNETA contains the following subnets:

Name	Address range
SubnetA1	10.10.130.0/24
SubnetA2	10.10.131.0/24

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
A Site-to-Site connection can be established between VNET1 and VNET2.	<input type="radio"/>	<input type="radio"/>

VNET1 and VNET2 can be peered.	<input type="radio"/>	<input type="radio"/>
--------------------------------	-----------------------	-----------------------

VNET1 and VNETA can be peered.	<input type="radio"/>	<input type="radio"/>
--------------------------------	-----------------------	-----------------------

Answer:

Statements	Yes	No
A Site-to-Site connection can be established between VNET1 and VNET2.		

VNET1 and VNET2 can be peered.		<input type="radio"/>
--------------------------------	--	-----------------------

VNET1 and VNETA can be peered.		
--------------------------------	--	--

Explanation:

Box 1: Yes

With VNet-to-VNet you can connect Virtual Networks in Azure across Different regions.

Box 2: Yes

Azure supports the following types of peering:

Virtual network peering: Connect virtual networks within the same Azure region.

Global virtual network peering: Connecting virtual networks across Azure regions.

Box 3: No

The virtual networks you peer must have non-overlapping IP address spaces.

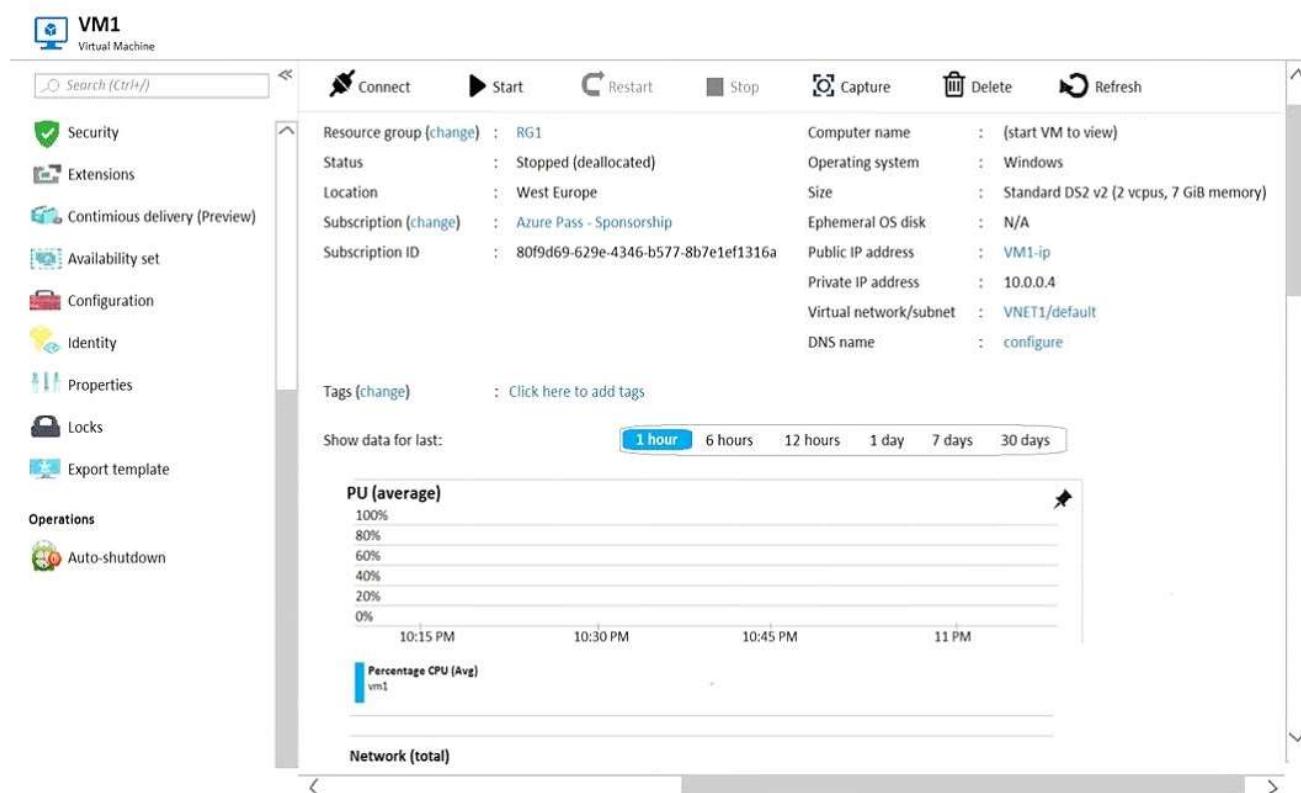
References:

<https://azure.microsoft.com/en-us/blog/vnet-to-vnet-connecting-virtual-networks-in-azure-across-different-regions/>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints>

106. You create an Azure VM named VM1 that runs Windows Server 2019.

VM1 is configured as shown in the exhibit. (Click the Exhibit button.)



You need to enable Desired State Configuration for VM1.

What should you do first?

- Configure a DNS name for VM1.
- Start VM1.
- Connect to VM1.
- Capture a snapshot of VM1.

Answer: B

Explanation:

Status is Stopped (Deallocated).

The DSC extension for Windows requires that the target virtual machine is able to communicate with Azure.

The VM needs to be started.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-windows>

107. You have an Azure subscription that contains the resources shown in the following table.

Name	Type
LB1	Load balancer
VM1	Virtual machine
VM2	Virtual machine

VM1 and VM2 run a website that is configured as shown in the following table.

Name	Physical path	Alias
Root folder	C:\inetpub\wwwroot\SiteA	/
Temp	C:\inetpub\wwwroot\Temp	Temp

LB1 is configured to balance requests to VM1 and VM2.

You configure a health probe as shown in the exhibit. (Click the Exhibit tab.)

Probe1

LB1

Save
 Discard
 Delete

* Name

IP version

Protocol

* Port

* Path

* Interval seconds

* Unhealthy threshold cumulative failures

Used by

You need to ensure that the health probe functions correctly.

What should you do?

- A. On LB1, change the Unhealthy threshold to 65536.
- B. On LB1, change the port to 8080.
- C. On VM1 and VM2, create a file named Probe1.htm in the C:\inetpub\wwwroot\Temp folder.
- D. On VM1 and VM2, create a file named Probe1.htm in the C:\inetpub\wwwroot\SiteA\Temp folder.

Answer: D

Explanation:

Load balancing provides a higher level of availability and scale by spreading incoming requests across virtual machines (VMs). You can use the Azure portal to create a Standard load balancer and balance

internal traffic among VMs.

To load balance successfully between VM1 and VM2 you have to place the html file in the path mentioned in the Probe1 configuration.

References:

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-internal-portal>

108. You have a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to grant three users named User1, User2, and User3 access to a temporary Microsoft SharePoint document library named Library1.

You need to create groups for the users. The solution must ensure that the groups are deleted automatically after 180 days.

Which two groups should you create? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. a Security group that uses the Assigned membership type
- B. an Office 365 group that uses the Assigned membership type**
- C. an Office 365 group that uses the Dynamic User membership type**
- D. a Security group that uses the Dynamic User membership type
- E. a Security group that uses the Dynamic Device membership type

Answer: B,C

Explanation:

You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).

Note: With the increase in usage of Office 365 Groups, administrators and users need a way to clean up unused groups. Expiration policies can help remove inactive groups from the system and make things cleaner.

When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, etc.) are also deleted.

You can set up a rule for dynamic membership on security groups or Office 365 groups.

109. You have an Azure Active Directory (Azure AD) tenant named contoso.com. Multi-factor authentication (MFA) is enabled for all users.

You need to provide users with the ability to bypass MFA for 10 days on devices to which they have successfully signed in by using MFA.

What should you do?

- A. From the multi-factor authentication page, configure the users' settings.
- B. From Azure AD, create a conditional access policy.
- C. From the multi-factor authentication page, configure the service settings.**
- D. From the MFA blade in Azure AD, configure the MFA Server settings.

Answer: C

Explanation:

Enable remember Multi-Factor Authentication

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

110. You have a hybrid infrastructure that contains an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The tenant contains the users shown in the following table.

Name	User name	Type	Source
User1	User1@contoso.onmicrosoft.com	Member	Azure Active Directory
User2	User2@contoso.onmicrosoft.com	Member	Windows Server AD
User3	User3@outlook.com	Guest	Microsoft Account
User4	User4@gmail.com	Guest	Microsoft Account

You plan to share a cloud resource to the All Users group.

You need to ensure that User1, User2, User3, and User4 can connect successfully to the cloud resource.

What should you do first?

- A. Create a user account of the member type for User4.
- B. Create a user account of the member type for User3.
- C. Modify the Directory-wide Groups settings.**
- D. Modify the External collaboration settings.

Answer: C

Explanation:

Ensure that "Enable an 'All Users' group in the directory" policy is set to "Yes" in your Azure Active Directory (AD) settings in order to enable the "All Users" group for centralized access administration. This group represents the entire collection of the Active Directory users, including guests and external users, that you can use to make the access permissions easier to manage within your directory.

111. You have an Azure subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.com.onmicrosoft.com.

Solution: You instruct User2 to create the user accounts.

- A. Yes

- B. No**

Answer: X

Explanation:

Only a global administrator can add users to this tenant.

References:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

112. You have an Azure subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.com.onmicrosoft.com.

Solution: You instruct User3 to create the user accounts.

A. Yes

B. No

Answer: B

Explanation:

Only a global administrator can add users to this tenant.

References:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

113. You have an Azure subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.com.onmicrosoft.com.

Solution: You instruct User1 to create the user accounts.

A. Yes

B. No

Answer: A

Explanation:

Only a global administrator can add users to this tenant.

References:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

114. Your on-premises network contains an Active Directory domain named adatum.com that is synced to Azure Active Directory (Azure AD). Password writeback is disabled.

In adatum.com, you create the users shown in the following table.

Name	Account option
User1	User must change password at next logon.
User2	Store password by using reversible encryption.
User3	A smart card is required for interactive logon.

Which users must sign in from a computer joined to adatum.com?

- A. User2 only
- B. User1 and User3 only
- C. User1, User2, and User3
- D. User2 and User3 only
- E. User1 only**

Answer: E

Explanation:

Password writeback is a feature enabled with Azure AD Connect that allows password changes in the cloud to be written back to an existing on-premises directory in real time.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

115. You have an Azure virtual machine named VM1 that runs Windows Server 2019.

You sign in to VM1 as a user named User 1 and perform the following actions:

- * Create files on drive C.
- * Create files on drive 0.
- * Modify the screen saver timeout.
- * Change the desktop background. You plan to redeploy VM1.

Which changes will be lost after you redeploy VM1?

- A. the modified screen saver timeout
- B. the new desktop background
- C. the new files on drive **the new files on drive D**
- D. The new files on drive C

Answer: D

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

Name	IP address	Connected to
VM1	10.1.0.4	VNET1/Subnet1
VM2	10.1.10.4	VNET1/Subnet2
VM3	172.16.0.4	VNET2/SubnetA
VM4	10.2.0.8	VNET3/SubnetB

A DNS service is installed on VM1.

You configure the DNS server settings for each virtual network as shown in the following exhibit.

DNS servers ⓘ

- Default (Azure-provided)
- Custom

You need to ensure that all the virtual machines can resolve DNS names by using the DNS service on VM1.

What should you do?

- A. Add service endpoints on VNET2 and VNET3.
- B. Configure peering between VNET1, VNET2, and VNET3.**
- C. Configure a conditional forwarder on VM1
- D. Add service endpoints on VNET1.

Answer: C

Explanation:

An Azure AD DS DNS zone should only contain the zone and records for the managed domain itself.

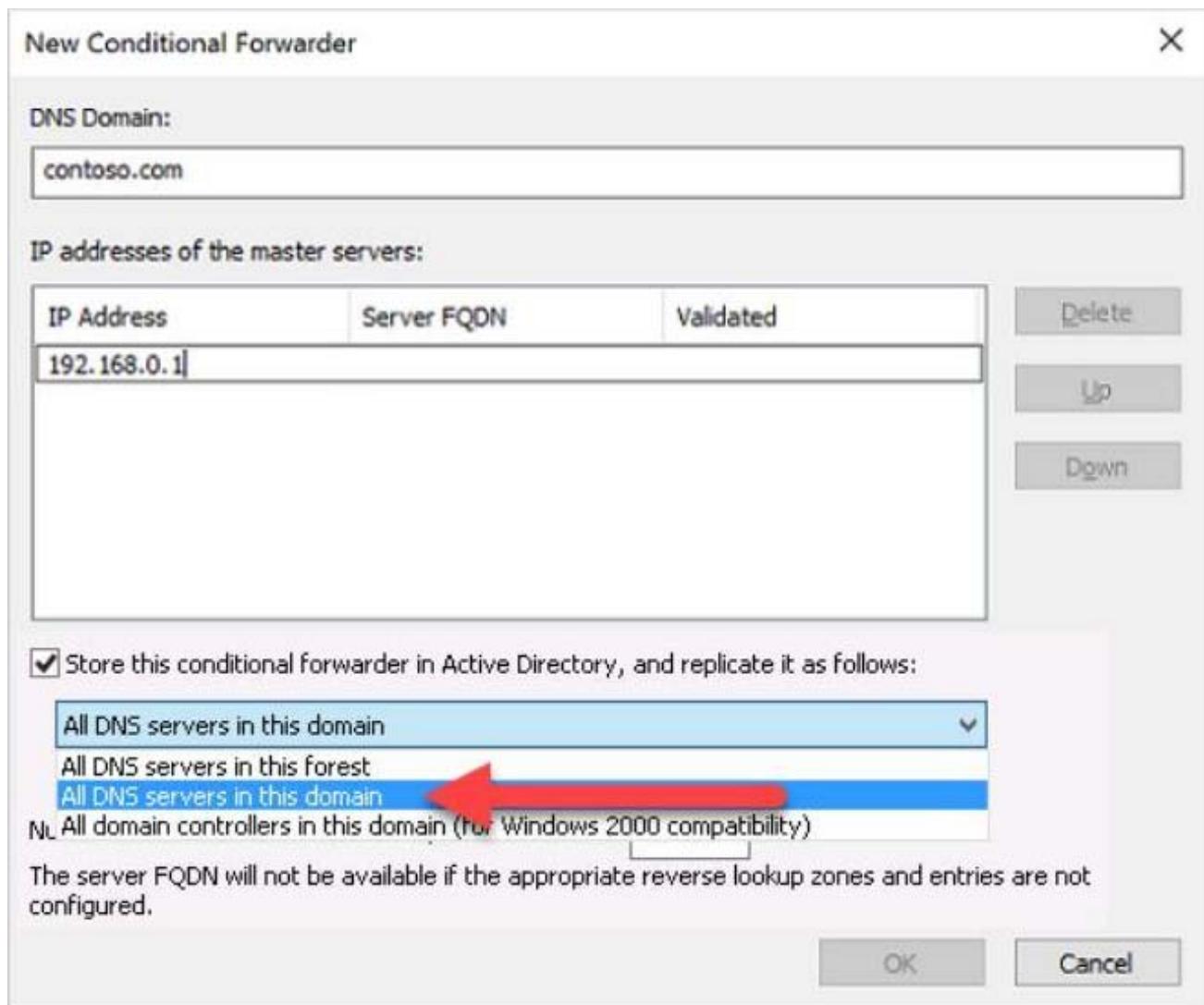
A conditional forwarder is a configuration option in a DNS server that lets you define a DNS domain, such as contoso.com, to forward queries to. Instead of the local DNS server trying to resolve queries for records in that domain, DNS queries are forwarded to the configured DNS for that domain. This configuration makes sure that the correct DNS records are returned, as you don't create a local DNS zone with duplicate records in the managed domain to reflect those resources.

To create a conditional forwarder in your managed domain, complete the following steps:

1. Select your DNS zone, such as aaddscontoso.com.
2. Select Conditional Forwarders, then right-select and choose New Conditional Forwarder...
3. Enter your other DNS Domain, such as contoso.com, then enter the IP addresses of the DNS servers for that namespace, as shown in the following example:

IP Address	Server FQDN	Validated
192.168.0.1		

4. Check the box for Store this conditional forwarder in Active Directory, and replicate it as follows, then select the option for All DNS servers in this domain, as shown in the following example:



5. To create the conditional forwarder, select OK.

Name resolution of the resources in other namespaces from VMs connected to the managed domain should now resolve correctly. Queries for the DNS domain configured in the conditional forwarder are passed to the relevant DNS servers.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances>

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-dns>

117. You have an Azure virtual machine named VM1.

The network interface for VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

APPLICATION SECURITY GROUPS  Configure the application security groups**INBOUND PORT RULES** 

 Network security group **VM1-nsg** (attached to network interface: **vm1175**)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
300	 RDP	3389	TCP	Any	Any	 Allow	...
400	 Rule1	80	TCP	Any	Any	 Deny	...
500	Rule2	80,443	TCP	Any	Any	 Deny	...
1000	Rule4	50-100,400-500	UDP	Any	Any	 Allow	...
2000	Rule5	50-5000	Any	Any	VirtualNetwork	 Deny	...
3000	Rule6	150-300	Any	Any	Any	 Allow	...
4000	Rule3	60-500	Any	Any	VirtualNetwork	 Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow	...
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBala...	Any	 Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	 Deny	...

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol VM1 is used as a web server only.

HTTPS uses port 443.

You need to ensure that users can connect to the website from the Internet.

What should you do?

- Change the priority of Rule3 to 450.
- Change the priority of Rule6 to 100
- DeleteRule1.
- Create a new inbound rule that allows TCP protocol 443 and configure the protocol to have a priority of 501.

 For Rule5, change the Action to Allow and change the priority to 401
Answer: 

Priority is a number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority.

118.HOTSPOT You have an Azure subscription named Subscription1 that contains a resource group named RG1.

In RG1. you create an internal load balancer named LB1 and a public load balancer named 162.

You need to ensure that an administrator named Admin 1 can manage LB1 and LB2. The solution must follow the principle of least privilege.

Which role should you assign to Admin1 for each task? To answer, select the appropriate options in the answer area. NOTE: Caen correct selection is worth one point.

Answer Area

To add a backend pool to LB1:

Contributor on LB1
Network Contributor on LB1
Network Contributor on RG1
Owner on LB1

To add a health probe to LB2:

Contributor on LB2
Network Contributor on LB2
Network Contributor on RG1
Owner on LB2

Answer:

Answer Area

To add a backend pool to LB1:

Contributor on LB1
Network Contributor on LB1
Network Contributor on RG1
Owner on LB1

To add a health probe to LB2:

Contributor on LB2
Network Contributor on LB2
Network Contributor on RG1
Owner on LB2

Explanation:

Box 1: Network Contributor on RG1

To add to the backend pool, write permission is required on the Resource Group because it writes deployment information. To add a backend pool, you need network contributor role on the LB and on the VMs that will be part of the backend pool.

For this reason the network contributor role must be assigned to the RG where the LB and the VM resides. So the correct answer is Network Contributor on RG1 .

Box 2: Network Contributor on RG1

For Health Probe also, without having access to RG1, no health probe can be added. If only Network Contributor role is assigned to LB then the user would not be able to access the IP addresses of the member pools.

Owner/Contributor can give the user access for everything. So it will not fit into the principle of least privilege. Hence Owner and contributor role is incorrect choices for the question.

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

119.HOTSPOT

You have an Azure virtual machine that runs Windows Server 2019 and has the following configurations:

- * Name: VM1
- * Location: West US
- * Connected to: VNet1
- * Private IP address: 10.1.0.4
- * Public IP address: 52.186.85.63
- * DNS suffix in Windows Server: Adatum.com

You create the Azure DNS zones shown in the following table.

Name	Type	Location
Adatum.pri	Private	West Europe
Contoso.pri	Private	Central US
Adatum.com	Public	West Europe
Contoso.com	Public	North Europe

Answer Area

You can only link VNETs to private DNS zones only and accordingly auto register a VNET only to a private DNS zones. Private DNS zones can be linked with VNETs (not public ones). And VM can auto-register to any private DNS zone linked with the Vnet and with auto-registration option set.

To resolve the records of a private DNS zone from your virtual network, you must link the virtual network with the zone. Linked virtual networks have full access and can resolve all DNS records published in the private zone

DNS zones that you can link to VNET1:

Suggested Answer:

Answer Area

DNS zones that you can link to VNET1:

Adatum.com only

Adatum.pri and adatum.com only

The private zones only

The public zones only

DNS zones to which VM1 can automatically register:

Adatum.com only

Adatum.pri and adatum.com only

The private zones only

The public zones only

120.HOTSPOT

You have Azure subscriptions named Subscription1 and Subscription2.

Subscription1 has following resource groups:

Name	Region	Lock type
RG1	West Europe	None
RG2	West Europe	Read Only

RG1 includes a web app named App1 in the West Europe location.

Subscription2 contains the following resource groups:

Name	Region	Lock type	the lock is only effecting the resources itself with edit/delete.
RG3	East Europe	Delete	
RG4	Central US	none	

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
App1 can be moved to RG2	<input type="radio"/>	<input type="radio"/>
App1 can be moved to RG3	<input type="radio"/>	<input type="radio"/>
App1 can be moved to RG4	<input type="radio"/>	<input type="radio"/>

Answer: A read-only lock on a resource group prevents you from moving existing resources in or out of the resource group.

Statements	Yes	No
App1 can be moved to RG2		
App1 can be moved to RG3		<input type="radio"/>
App1 can be moved to RG4		<input type="radio"/>

Explanation:

App1 present in RG1 and in RG1 there is no lock available. So you can move App1 to other resource groups, RG2, RG3, RG4.

You can move Azure App services across RGs and subscriptions

App Service resources can only be moved from the resource group in which they were originally created.

If an App Service resource is no longer in its original resource group, move it back to its original resource group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations>

121. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100
- Source: Any
- Source port range: *
- Destination: *
- Destination port range: 3389
- Protocol: UDP
- Action: Allow

VM1 connects to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Internet source to the VirtualNetwork destination for port range 3389 and uses the UDP protocol.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation: The default port for RDP is TCP port 3389 not UDP.

NSGs deny all inbound traffic except from virtual network or load balancers. For inbound traffic, Azure processes the rules in a network security group associated to a subnet first, and then the rules in a network security group associated to the network interface.

By default NSG rule to allow traffic through RDP port 3389 is not created automatically during the creation of VM, unless you change the setting during creation.

Here in the solution UDP traffic is allowed at virtual network level which is not tcp/rdp protocol. So this will not work to achieve the goal.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

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

122. You have an Active Directory domain named contoso.com that contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
User3	User	OU1
Group1	Security Group – Global	OU1
User4	User	OU2
Group2	Security Group – Global	OU2

The groups have the memberships shown in the following table.

Group	Member
Group1	User1
Group2	User2, Group1

OU1 and OU2 are synced to Azure Active Directory (Azure AD).

You modify the synchronization settings and remove OU1 from synchronization. You sync Active Directory and Azure AD.

Which objects are in Azure AD?

- A. User4 and Group2 only
- B. User2, Group1, User4, and Group2 only
- C. User1, User2, Group1, User4, and Group2 only**
- D. User1, User2, User3, User4, Group1, and Group2

Answer: C

123. You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant contains 500 user accounts.

You deploy Microsoft Office 365. You configure Office 365 to use the user accounts in adatum.com.

You configure 60 users to connect to mailboxes in Microsoft Exchange Online.

You need to ensure that the 60 users use Azure Multi-Factor Authentication (MFA) to connect to the Exchange Online mailboxes. The solution must only affect connections to the Exchange Online mailboxes.

What should you do?

- A. From the multi-factor authentication page, configure the Multi-Factor Auth status for each user**
- B. From Azure Active Directory admin center, create a conditional access policy
- C. From the multi-factor authentication page, modify the verification options
- D. From the Azure Active Directory admin center, configure an authentication method

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

124. Your network contains an on-premises Active Directory domain named adatum.com. The domain contains an organizational unit (OU) named OU1.

OU1 contains the objects shown in the following table.

Name	Type	Member of
User1	User	Group1
Group1	Global security group	None
Group2	Universal distribution group	None
Computer1	Computer	Group1

You sync OU1 to Azure Active Directory (Azure AD) by using Azure AD Connect.

You need to identify which objects are synced to Azure AD.

Which objects should you identify?

- A. User1 and Group1 only
- B. User1, Group1, and Group2 only**
- C. User1, Group1, Group2, and Computer1
- D. Computer1 only

Answer: B

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization>

125. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User4 to create the user accounts.

Does that meet the goal?

- A. yes

- B. No**

Answer: B

Explanation:

Only a global administrator can add users to this tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

126. You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com and an Azure Kubernetes Service (AKS) cluster named AKS1.

An administrator reports that she is unable to grant access to AKS1 to the users in contoso.com.

You need to ensure that access to AKS1 can be granted to the contoso.com users.

What should you do first?

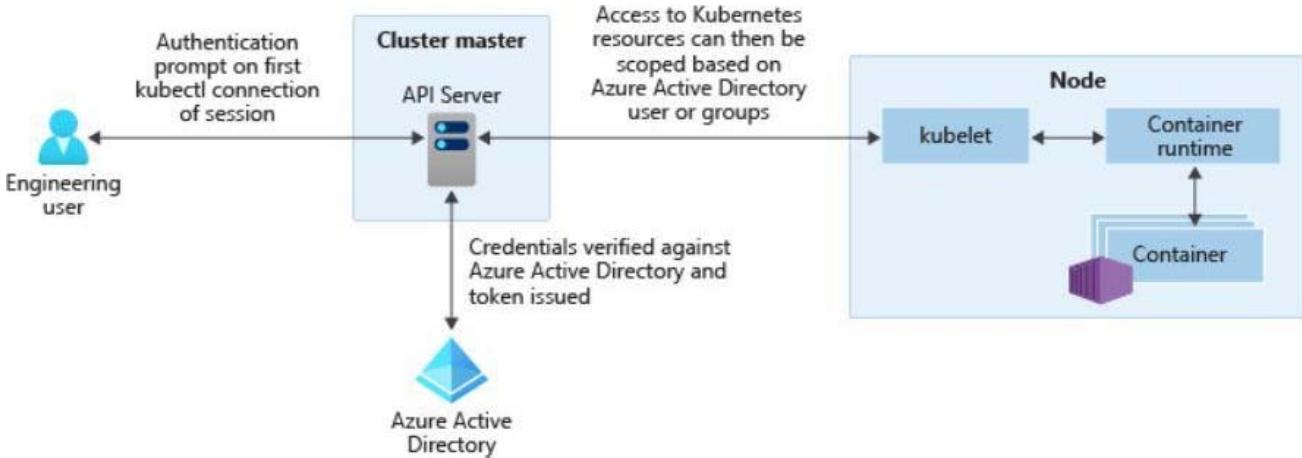
- A. From contoso.com, modify the Organization relationships settings.
- B. From contoso.com, create an OAuth 2.0 authorization endpoint.**
- C. Recreate AKS1.
- D. From AKS1, create a namespace.

Answer: B

Explanation:

With Azure AD-integrated AKS clusters, you can grant users or groups access to Kubernetes resources within a namespace or across the cluster. To obtain a kubectl configuration context, a user can run the az aks get-credentials command. When a user then interacts with the AKS cluster with kubectl, they're prompted to sign in with their Azure AD credentials. This approach provides a single source for user account management and password credentials. The user can only access the resources as defined by the cluster administrator.

Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol. For more information on OpenID Connect, see the Open ID connect documentation. From inside of the Kubernetes cluster, Webhook Token Authentication is used to verify authentication tokens. Webhook token authentication is configured and managed as part of the AKS cluster.



Reference:

<https://kubernetes.io/docs/reference/access-authn-authz/authentication/>

<https://docs.microsoft.com/en-us/azure/aks/concepts-identity>

127. Topic 5, Misc. Questions Set B

HOTSPOT

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

Name	Type	Member of
User1	Member	Group1
User2	Guest	Group1
User3	Member	None
UserA	Member	Group2
UserB	Guest	Group2

User3 is the owner of Group1.

Group2 is a member of Group1.

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

Create an access review

Access reviews enable reviewers to attest user's membership in a group or access to an application.

*** Review name**

Description

*** Start date**

Frequency

Duration (in days)

End

*** Number of times**

*** End date**

Users

Users to review

Scope Guest users only
 Everyone

*** Group**

Reviewers

Reviewers

Programs

Link to program

Default program

Upon completion settings

Advanced settings

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
User3 can perform an access review of User1	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserB	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

User1 is a Member and not a Guest Account, Access Review specified Guests only.

Statements	Yes	No
User3 can perform an access review of User1	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserB	<input type="radio"/>	<input type="radio"/>

Explanation:

In the Users section, specify the users that the access review applies to. Access reviews can be for the members of a group or for users who were assigned to an application. You can further scope the access review to review only the guest users who are members (or assigned to the application), rather than reviewing all the users who are members or who have access to the application.

Users

Users to review: Members of a group

Scope: Guest users only Everyone

* Group: Select a group >

Present Use Case:

Group2 is a member of Group1 and User3 is the owner of Group1 So User3 can review both Group 1 and 2.

But for review the scope says only Guest.

Solution:

User1 is a member not a guest so 1st statement ==> NO

UserA is member not the guest so 2nd statement ==> No

UserB is a guest so 3rd statement ==> Yes

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

128.HOTSPOT

You have the Azure management groups shown in the following table.

Name	In management group
Tenant Root Group	<i>Not applicable</i>
ManagementGroup11	Tenant Root Group
ManagementGroup12	Tenant Root Group
ManagementGroup21	ManagementGroup11

You add Azure subscriptions to the management groups as shown in the following table.

Name	Management group
Subscription1	ManagementGroup21
Subscription2	ManagementGroup12

You create the Azure policies shown in the following table.

Name	Parameter	Scope
Not allowed resource types	virtualNetworks	Tenant Root Group
Allowed resource types	virtualNetworks	ManagementGroup12

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
------------	-----	----

You can create a virtual network in Subscription1.

You can create a virtual machine in Subscription2.

You can add Subscription1 to ManagementGroup11.

Answer:

Statements The azure policy (not allowed resource types – Virtual networks) is inherited to Subscription1. So, Virtual networks are not allowed to create in Subscription1.

You can create a virtual network in Subscription1.

You can create a virtual machine in Subscription2.

You can add Subscription1 to ManagementGroup11.

Explanation:

Box 1: No

Virtual networks are not allowed at the root and is inherited. Deny overrides allowed.

Box 2: Yes

Virtual Machines can be created on a Management Group provided the user has the required RBAC permissions.

Box 3: Yes

Subscriptions can be moved between Management Groups provided the user has the required RBAC permissions. **you cannot ADD Subscription1 to ManagementGroup11, but you can MOVE subscription1 from ManagementGroup21 to ManagementGroup11. Subscriptions can only be a member of ONE managementGroup at a time.**

Reference: <https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>

<https://docs.microsoft.com/en-us/azure/governance/management-groups/manage#moving-management-groups-and-subscriptions>

129. You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.

You need to view the error events from a table named Event.

Which query should you run in Workspace1?

- A. Event | where EventType is "error"
- B. Event | search "error"**
- C. select * from Event where EventType == "error"
- D. Get-Event Event | where {\$_.EventType -eq "error"}

- 1. search in (Event) "error"
- 2. Event | search "error"
- 3. Event | where EventType == "error"

Answer: B

Explanation:

To search a term in a specific table, add in (table-name) just after the search operator

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries>

130. You have an Azure virtual machine named VM1 that runs Windows Server 2019.

You save VM1 as a template named Template1 to the Azure Resource Manager library.

You plan to deploy a virtual machine named VM2 from Template1.

What can you configure during the deployment of VM2?

- A. virtual machine size
- B. operating system
- C. administrator username
- D. resource group**

Answer: D

Explanation:

When deploying a virtual machine from a template, you must specify:

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/ps-template>

131. HOTSPOT

You have an Azure subscription named Subscription1. Subscription1 contains two Azure virtual machines named VM1 and VM2. VM1 and VM2 run Windows Server 2016.

VM1 is backed up daily by Azure Backup without using the Azure Backup agent.

VM1 is affected by ransomware that encrypts data.

You need to restore the latest backup of VM1.

To which location can you restore the backup? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

You can perform a file recovery of VM1 to:

VM1 only
VM1 or a new Azure virtual machine only
VM1 and VM2 only
A new Azure virtual machine only
Any Windows computer that has Internet connectivity

You can restore VM1 to:

VM1 only
VM1 or a new Azure virtual machine only
VM1 and VM2 only
Any Windows computer that has Internet connectivity

Answer:

You can perform a file recovery of VM1 to:

VM1 only
VM1 or a new Azure virtual machine only
VM1 and VM2 only
A new Azure virtual machine only
Any Windows computer that has Internet connectivity

You can restore VM1 to:

VM1 only
VM1 or a new Azure virtual machine only
VM1 and VM2 only
Any Windows computer that has Internet connectivity

Explanation:

Box 1: VM1 and VM2 only

When recovering files, you can't restore files to a previous or future operating system version. You can restore files from a VM to the same server operating system, or to the compatible client operating system. Therefore - "VM1 and VM2 only" is the best answer since both run on Windows Server 2016.

"A new Azure virtual machine only", this will also work but why to create unnecessary new VM in Azure if existing VM will do the task. So this option is incorrect.

Box 2: VM1 or A new Azure virtual machine only

When restoring a VM, you can't use the replace existing VM option for encrypted VMs. This option is only supported for unencrypted managed disks. And also You can restore files from a VM to the same server operating system, or to the compatible client operating system only. Hence "VM1 or A new Azure virtual machine only" is correct answer.

References:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms>

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm#system-requirements>

132. You have an Azure subscription that has a Recovery Services vault named Vault1.

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

Name	Operating system	Auto-shutdown
VM1	Windows Server 2012 R2	Off
VM2	Windows Server 2016	19:00
VM3	Ubuntu Server 18.04 LTS	Off
VM4	Windows 10	19:00

You plan to schedule backups to occur every night at 23:00.

Which virtual machines can you back up by using Azure Backup?

- A. VM1 only
- B. VM1 and VM3 only
- C. VM1, VM2, VM3 and VM4**
- D. VM1 and VM2 only

Answer: C

Explanation:

Azure Backup supports backup of 64-bit Windows server operating system from Windows Server 2008.

Azure Backup supports backup of 64-bit Windows 10 operating system.

Azure Backup supports backup of 64-bit Ubuntu Server operating system from Ubuntu 12.04.

Azure Backup supports backup of VM that are shutdown or offline.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas>

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros>

133. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System log on VM1 within an hour.

Solution: You create an Azure Log Analytics workspace and configure the data settings. You add an extension to VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

- A. Yes

- B. No**

Answer: B

Explanation:

Instead: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

134. HOTSPOT

You have an Azure virtual machine that runs Windows Server 2019 and has the following configurations:

- Name: VM1
- Location: West US
- Connected to: VNET1
- Private IP address: 10.1.0.4
- Public IP address: 52.186.85.63
- DNS suffix in Windows Server: Adatum.com

You create the Azure DNS zones shown in the following table.

Name	Type	Location
Adatum.pri	Private	West Europe
Contoso.pri	Private	Central US
Adatum.com	Public	West Europe
Contoso.com	Public	North Europe

You need to identify which DNS zones you can link to VNET1 and the DNS zones to which VM1 can automatically register.

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

DNS zones that you can link to VNET1:

Adatum.com only
Adatum.pri and adatum.com only
The private zones only
The public zones only

DNS zones to which VM1 can automatically register:

Adatum.com only
Adatum.pri and adatum.com only
The private zones only
The public zones only

Answer:

DNS zones that you can link to VNET1:

Adatum.com only
Adatum.pri and adatum.com only
The private zones only
The public zones only

DNS zones to which VM1 can automatically register:

Adatum.com only
Adatum.pri and adatum.com only
The private zones only
The public zones only

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/dns/private-dns-overview>

135.HOTSPOT

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

Name	Private IP address	Public IP address	Virtual network name	DNS suffix configured in Windows Server
VM1	10.1.0.4	52.186.85.63	VNET1	Adatum.com
VM2	10.1.0.5	13.92.168.13	VNET1	Contoso.com

You create a private Azure DNS zone named adatum.com. You configure the adatum.com zone to allow auto registration from VNET1.

Which A records will be added to the adatum.com zone for each virtual machine? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A records for VM1:

None

Private IP address only

Public IP address only

Private IP address and public IP address

A records for VM2:

None

Private IP address only

Public IP address only

Private IP address and public IP address

Answer:

A records for VM1:

None

Private IP address only

Public IP address only

Private IP address and public IP address

A records for VM2:

None

Private IP address only

Public IP address only

Private IP address and public IP address

Explanation:

The virtual machines are registered (added) to the private zone as A records pointing to their private IP addresses.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-overview>

<https://docs.microsoft.com/en-us/azure/dns/private-dns-scenarios>

136. Your network contains an on-premises Active Directory forest named contoso.com that contains two domains named contoso.com and east.contoso.com.

The forest contains the users shown in the following table.

Name	Domain	Member of
User1	Contoso.com	Enterprise Admins
User2	Contoso.com	Domain Admins
User3	East.contoso.com	Domain Admins
User4	East.contoso.com	Domain Users

You plan to sync east.contoso.com to an Azure Active Directory (Azure AD) tenant by using Azure AD Connect.

You need to select an account for Azure AD Connect to use to connect to the forest.

Which account should you select?

- A. User1
- B. User2
- C. User3
- D. User4**

Answer: D

Explanation:

It is no longer supported to use an enterprise admin or a domain admin account as the AD DS Connector account.

Reference:

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

137.HOTSPOT

You have an Azure subscription that contains the resources shown in the following table:

Name	Type	Resource group	Tag
RG6	Resource group	<i>Not applicable</i>	<i>None</i>
VNET1	Virtual network	RG6	Department: D1

You assign a policy to RG6 as shown in the following table:

Section	Setting	Value
Scope	Scope	Subscription1/RG6
	Exclusions	<i>None</i>
Basics	Policy definition	Apply tag and its default value
	Assignment name	Apply tag and its default value
Parameters	Tag name	Label
	Tag value	Value1

To RG6, you apply the tag: RGroup: RG6.

You deploy a virtual network named VNET2 to RG6.

Which tags apply to VNET1 and VNET2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VNET1:

None
Department: D1 only
Department: D1, and RGroup: RG6 only
Department: D1, and Label: Value1 only
Department: D1, RGroup: RG6, and Label: Value1

VNET2:

None
RGroup: RG6 only
Label: Value1 only
RGroup: RG6, and Label: Value1

Answer:

Answer Area

resources created before policy creation will not inherit the policy rules.

VNET1:

None
Department: D1 only
Department: D1, and RGroup: RG6 only
Department: D1, and Label: Value1 only
Department: D1, RGroup: RG6, and Label: Value1



VNET2:

None
RGroup: RG6 only
Label: Value1 only
RGroup: RG6, and Label: Value1

Explanation:

VNET1: Department: D1, and Label: Value1 only.

Tags applied to the resource group or subscription are not inherited by the resources.

Note: Azure Policy allows you to use either built-in or custom-defined policy definitions and assign them to either a specific resource group or across a whole Azure subscription.

VNET2: Label: Value1 only.

Reference: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

138. You have an Azure subscription named AZPT1 that contains the resources shown in the following table:

Name	Type
storage1	Azure Storage account
VNET1	Virtual network
VM1	Azure virtual machine
VM1Managed	Managed disk for VM1
RVAULT1	Recovery Services vault for the site recovery of VM1

You create a new Azure subscription named AZPT2.

You need to identify which resources can be moved to AZPT2.

Which resources should you identify?

- A. VM1, storage1, VNET1, and VM1Managed only
- B. VM1 and VM1Managed only
- C. VM1, storage1, VNET1, VM1Managed, and RVAULT1**
- D. RVAULT1 only

Answer: C

Explanation:

You can move a VM and its associated resources to a different subscription by using the Azure portal.

You can now move an Azure Recovery Service (ASR) Vault to either a new resource group within the

current subscription or to a new subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription>

<https://docs.microsoft.com/en-us/azure/key-vault/general/keyvault-move-subscription>

139. You have an Azure Active Directory (Azure AD) domain that contains 5,000 user accounts. You create a new user account named AdminUser1.

You need to assign the User administrator administrative role to AdminUser1.

What should you do from the user account properties?

- A. From the Directory role blade, modify the directory role.
- B. From the Groups blade, invite the user account to a new group.
- C. From the Licenses blade, assign a new license.

Answer: A

Explanation:

Assign a role to a user

References:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>

140. You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains 100 user accounts.

You purchase 10 Azure AD Premium P2 licenses for the tenant.

You need to ensure that 10 users can use all the Azure AD Premium features.

What should you do?

- A. From the Groups blade of each user, invite the users to a group.
- B. From the Licenses blade of Azure AD, assign a license.
- C. From the Directory role blade of each user, modify the directory role.
- D. From the Azure AD domain, add an enterprise application.

Answer: B

Explanation:

Many Azure Active Directory (Azure AD) services require you to license each of your users or groups (and associated members) for that service. Only users with active licenses will be able to access and use the licensed Azure AD services for which that's true. Licenses are applied per tenant and do not transfer to other tenants.

Not all Microsoft services are available in all locations. Before a license can be assigned to a group, you must specify the Usage location for all members. You can set this value in the Azure Active Directory > Users > Profile > Settings area in Azure AD. Any user whose usage location is not specified inherits the location of the Azure AD organization.

You can add the licensing rights to users or to an entire group. Check the reference link for the steps.

References: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups>

141. You have an Azure subscription named Subscription 1 and an on-premises deployment of Microsoft System Center Service Manager Subscription! contains a virtual machine named VM1.

You need to ensure that an alert is set in Service Manager when the amount of available memory on VM1 is below 10 percent.

What should you do first?

- A. Create a notification.
- B. Create an automation runbook.
- C. Deploy the IT Service Management Connector (ITSM).**
- D. Deploy a function app.

Answer: C

Explanation:

The IT Service Management Connector (ITSMC) allows you to connect Azure and a supported IT Service Management (ITSM) product/service, such as the Microsoft System Center Service Manager.

With ITSMC, you can create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).

References: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview>

142.HOTSPOT

You have an Azure subscription named Subscription1.

In Subscription1, you create an Azure file share named share1.

You create a shared access signature (SAS) named SAS1 as shown in the following exhibit.

Allowed services 1

Blob File Queue Table

Allowed resource types 1

Service Container Object

Allowed permissions 1

Read Write Delete List Add Create Update Process

Start and expiry date/time 1

Start

2018-09-01

2:00:00 PM

End

2018-09-14

2:00:00 PM

(UTC + 02:00) — Current Timezone —

Allowed IP addresses 1

193.77.134.10-193.77.134.50

Allowed protocols 1

HTTPS only HTTPS and HTTP

Signing key 1key1

Generate SAS and connection string

To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

If on September 2, 2018, you run Microsoft Azure Storage Explorer on a computer that has an IP address of 193.77.134.1, and you use SAS1 to connect to the storage account, you [answer choice].

<input type="checkbox"/>
will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

If on September 10, 2018, you run the net use command on a computer that has an IP address of 193.77.134.50, and you use SAS1 as the password to connect to share1, you [answer choice].

<input type="checkbox"/>
will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

Answer:

Answer Area

If on September 2, 2018, you run Microsoft Azure Storage Explorer on a computer that has an IP address of 193.77.134.1, and you use SAS1 to connect to the storage account, you [answer choice].

will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

If on September 10, 2018, you run the `net use` command on a computer that has an IP address of 193.77.134.50, and you use SAS1 as the password to connect to share1, you [answer choice].

will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

using "net use" where it uses SMB. The SMB (Server Message Broker) protocol does not support SAS. it still asks for username/password.

Explanation:

Box 1: will have no access

The IP 193.77.134.1 does not have access on the SAS since this IP falls outside of the allowed IP address range for SAS. Hence "will have no access" is correct.

Box 2: will be prompted for credentials

The net use command is used to connect to file shares. To mount an Azure file share, you will need the primary (or secondary) storage key. SAS keys are not currently supported for mounting. Based on the provided SAS exhibit, IP address is an allowed IP and also on given date SAS is active, but account storage key is must to have to run the "net use" command , which is not provided in the question. Hence "will be prompted for credentials" is correct option for this. net use R:

`\rebelsa1.file.core.windows.net\rebelshare <storage key> /user:Azure\rebelsa1`

References:

<https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows>

<https://feedback.azure.com/forums/217298-storage/suggestions/14498352-allow-azure-files-shares-to-be-mounted-using-sas-s>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

<http://www.rebeladmin.com/2018/03/step-step-guide-create-azure-file-share-map-windows-10/>

143. You have an on-premises server that contains a folder named D:\Folder1.

You need to copy the contents of D:\Folder1 to the public container in an Azure Storage account named contoso data.

Which command should you run?

- A. `https://contosodata.blob.core.windows.net/public`
- B. `azcopy sync D:\folder1 https://contosodata.blob.core.windows.net/public --snapshot`
- C. `azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive`**
- D. `az storage blob copy start-batch D:\Folder1 https://contosodata.blob.core.windows.net/public`

Answer: C

Explanation:

The azcopy copy command copies a directory (and all of the files in that directory) to a blob container. The result is a directory in the container by the same name.

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>

144. You have an Azure subscription named Subscription1 that contains the storage accounts shown in the following table:

Name	Account kind	Azure service that contains data
storage1	Storage	File
storage2	StorageV2 (general purpose v2)	File, Table
storage3	StorageV2 (general purpose v2)	Queue
storage4	BlobStorage	Blob

You plan to use the Azure Import/Export service to export data from Subscription1.

You need to identify which storage account can be used to export the data.

What should you identify?

- A. storage1
- B. storage2
- C. storage3
- D. storage4**

Answer: D

Explanation:

Azure Import/Export service supports the following of storage accounts:

Azure Import/Export service supports the following storage types:

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements>

145. DRAG DROP

You have an Azure subscription named Subscription1.

You create an Azure Storage account named Contoso storage, and then you create a file share named data.

Which UNC path should you include in a script that references files from the data file share? To answer, drag the appropriate values to the correct targets. Each value 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.

Values**Answer Area**

blob	W	Value	.	Value	\	Value
blob.core.windows.net						
contosostorage						
data						
file						
file.core.windows.net						
portal.azure.com						
subscription1						

Answer:**Values****Answer Area**

blob	W	contosostorage	.	file.core.windows.net	\	data
blob.core.windows.net						
contosostorage						
data						
file						
file.core.windows.net						
portal.azure.com						
subscription1						

Explanation:

Box 1: contosostorage

The name of account

Box 2: file.core.windows.net

Box 3: data

The name of the file share is data.

Example:

References: <https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

146.DRAG DROP

You have an on-premises file server named Server1 that runs Windows Server 2016.

You have an Azure subscription that contains an Azure file share.

You deploy an Azure File Sync Storage Sync Service, and you create a sync group.

You need to synchronize files from Server1 to Azure.

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 Azure on-premises data gateway.

Install the Azure File Sync agent on Server1.

Create a Recovery Services vault.

Register Server1.

Install the DFS Replication server role on Server1.

Add a server endpoint.

Answer:

Actions

Answer Area

Create an Azure on-premises data gateway.

Install the Azure File Sync agent on Server1.

Install the Azure File Sync agent on Server1.

Register Server1.

Create a Recovery Services vault.

Add a server endpoint.

Register Server1.

Install the DFS Replication server role on Server1.

Add a server endpoint.

Explanation:

Step 1: Install the Azure File Sync agent on Server1

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share

Step 2: Register Server1.

Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

Step 3: Add a server endpoint

Create a sync group and a cloud endpoint.

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

References: <https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

147.HOTSPOT

You plan to create an Azure Storage account in the Azure region of East US 2.

You need to create a storage account that meets the following requirements:

- Replicates synchronously
- Remains available if a single data center in the region fails

How should you configure the storage account? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Replication:

- Geo-redundant storage (GRS)
- Locally-redundant storage (LRS)
- Read-access geo-redundant storage (RA GRS)
- Zone-redundant storage (ZRS)

Account kind:

- Blob storage
- Storage (general purpose v1)
- StorageV2 (general purpose v2)

Answer:

Answer Area

Replication:

LRS would not remain available if a data center in the region fails

- Geo-redundant storage (GRS)
- Locally-redundant storage (LRS)
- Read-access geo-redundant storage (RA GRS)
- Zone-redundant storage (ZRS)

Account kind:

GRS and RA GRS use asynchronous replication.

- Blob storage
- Storage (general purpose v1)
- StorageV2 (general purpose v2)

ZRS only support GPv2.

Explanation:

Box 1: Zone-redundant storage (ZRS)

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region.

LRS would not remain available if a data center in the region fails GRS and RA GRS use asynchronous replication.

Box 2: StorageV2 (general purpose V2)

ZRS only support GPv2.

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs>

148. You have an Azure Storage account named storage1.

You plan to use AzCopy to copy data to storage1.

You need to identify the storage services in storage1 to which you can copy the data.

What should you identify?

A. blob, file, table, and queue

B. blob and file only

C. file and table only

D. file only

E. blob, table, and queue only

Answer: B

Explanation:

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

149. HOTSPOT

You have an Azure Storage account named storage1 that uses Azure Blob storage and Azure File storage.

You need to use AzCopy to copy data to the blob storage and file storage in storage1.

Which authentication method should you use for each type of storage? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Blob storage:

- Azure Active Directory (Azure AD) only
- Shared access signatures (SAS) only
- Access keys and shared access signatures (SAS) only
- Azure Active Directory (Azure AD) and shared access signatures (SAS) only
- Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)

File storage:

- Azure Active Directory (Azure AD) only
- Shared access signatures (SAS) only
- Access keys and shared access signatures (SAS) only
- Azure Active Directory (Azure AD) and shared access signatures (SAS) only
- Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)

Answer:

Answer Area

Blob storage:

- Azure Active Directory (Azure AD) only
- Shared access signatures (SAS) only
- Access keys and shared access signatures (SAS) only
- Azure Active Directory (Azure AD) and shared access signatures (SAS) only
- Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)

File storage:

- Azure Active Directory (Azure AD) only
- Shared access signatures (SAS) only
- Access keys and shared access signatures (SAS) only
- Azure Active Directory (Azure AD) and shared access signatures (SAS) only
- Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)

Explanation:

You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.

Box 1:

Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage.

Box 2:

Only Shared Access Signature (SAS) token is supported for File storage.

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

150. You have an Azure subscription that contains an Azure Storage account.

You plan to create an Azure container instance named container1 that will use a Docker image named Image1. Image1 contains a Microsoft SQL Server instance that requires persistent storage.

You need to configure a storage service for Container1.

What should you use?

- A. Azure Files
- B. Azure Blob storage
- C. Azure Queue storage
- D. Azure Table storage

Answer: A

Explanation:

Microsoft have Docker Volume Plugin for Azure file storage which provides exactly this and it is used for Azure file shares.

Azure File Storage volume plugin is not limited to ease of container migration. It also allows a file share to be shared among multiple containers (even though they are on different hosts) to collaborate on workloads, share configuration or secrets of an application running on multiple hosts. Another use case is uploading metrics and diagnostics data such as logs from applications to a file share for further processing.

Reference: <https://azure.microsoft.com/en-gb/blog/persistent-docker-volumes-with-azure-file-storage/>

151. You have an app named App1 that runs on two Azure virtual machines named VM1 and VM2.

You plan to implement an Azure Availability Set for App1. The solution must ensure that App1 is available during planned maintenance of the hardware hosting VM1 and VM2.

What should you include in the Availability Set?

- A. one update domain
- B. two fault domains
- C. one fault domain
- D. two update domains

Answer: D

Explanation:

Microsoft updates, which Microsoft refers to as planned maintenance events, sometimes require that VMs be rebooted to complete the update. To reduce the impact on VMs, the Azure fabric is divided into update domains to ensure that not all VMs are rebooted at the same time.

152. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the Subscriptions blade, you select the subscription, and then click Programmatic deployment.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell>

Through activity logs, you can determine:

§ what operations were taken on the resources in your subscription

§ who started the operation

§ when the operation occurred

§ the status of the operation

§ the values of other properties that might help you research the operation

On the Azure portal menu, select Monitor, or search for and select Monitor from any page

2. Select Activity Log.

3. You see a summary of recent operations. A default set of filters is applied to the operations. Notice the information on the summary includes who started the action and when it happened.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs>

153. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the RG1 blade, you click Automation script.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell>

Through activity logs, you can determine:

§ what operations were taken on the resources in your subscription

§ who started the operation

§ when the operation occurred

§ the status of the operation

§ the values of other properties that might help you research the operation

1. On the Azure portal menu, select Monitor, or search for and select Monitor from any page

2. Select Activity Log.

3. You see a summary of recent operations. A default set of filters is applied to the operations. Notice the information on the summary includes who started the action and when it happened.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs>

154. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the RG1 blade, you click Deployments.

Does this meet the goal?

A. Yes

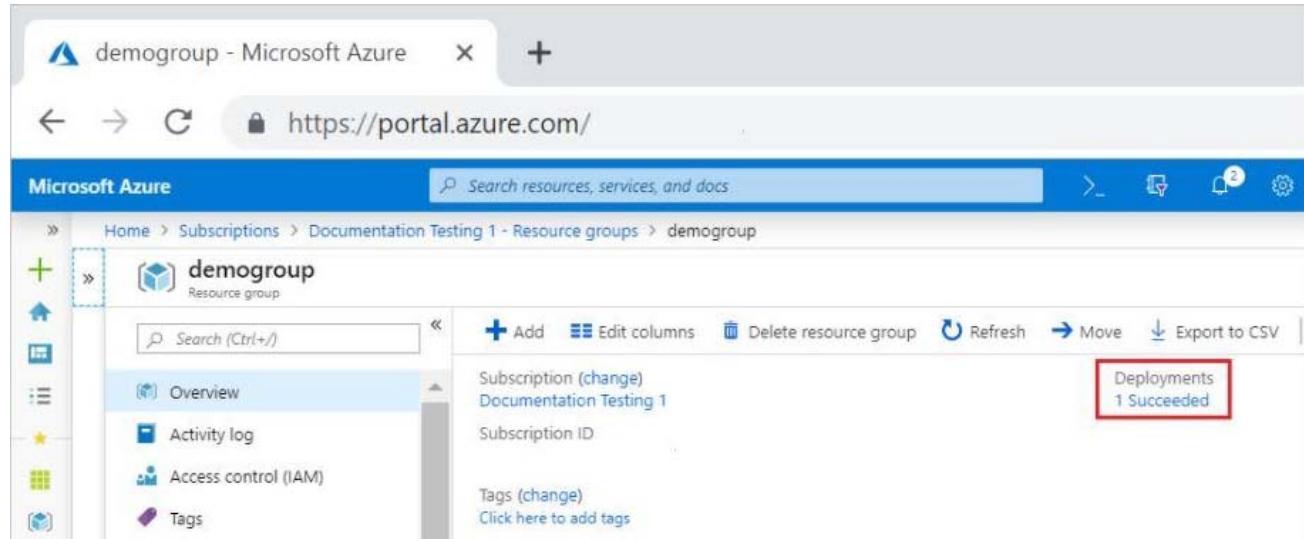
B. No

Answer: A

Explanation:

1. Select the resource group (Here RG1) you want to examine.

2. Select the link under Deployments.



The screenshot shows the Microsoft Azure portal interface. The browser address bar shows 'https://portal.azure.com/'. The main content area displays the 'demogroup' resource group under 'Subscriptions > Documentation Testing 1 - Resource groups > demogroup'. The left sidebar shows navigation options like Home, Create, and Resource groups. The main panel shows the 'demogroup' details, including 'Overview', 'Activity log', 'Access control (IAM)', and 'Tags'. At the top of this panel are buttons for 'Add', 'Edit columns', 'Delete resource group', 'Refresh', 'Move', and 'Export to CSV'. A red box highlights the 'Deployments' link, which is currently selected and shows '1 Succeeded'.

3. Select one of the deployments from the deployment history.

demogroup - Deployments

Resource group

Search (Ctrl+ /)

Delete Cancel Redeploy View template

Filter by deployment name or resources in the deployment...

DEPLOYMENT NAME	STATUS
CreateVm-MicrosoftWindowsServer.Win	Succeeded

Overview

Activity log

Access control (IAM)

Tags

4. You will see a history of deployment for the resource group, including the correlation ID.

Delete Cancel Redeploy Refresh

>Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-20191122141922
Subscription: Documentation Testing 1
Resource group: examplegroup

Start time: 11/22/2019 2:20:02 PM
Correlation ID: c2451693-bcbc-4119-b1ae-752b543cf7ca

Deployment details (Download)

Resource	Type	Status	Operation details
examplevnet	Microsoft.Network/Virtu...	OK	Operation details

Next steps

[Go to resource](#)

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-history?tabs=azure-portal>

155. You have an Azure subscription named Subscription1.

You deploy a Linux virtual machine named VM1 to Subscription1.

You need to monitor the metrics and the logs of VM1.

What should you use?

- A. **Linux Diagnostic Extension (LAD) 3.0**
- B. Azure Analysis Services
- C. the AzurePerformanceDiagnostics extension
- D. Azure HDInsight

Answer: A

Explanation:

You can use extensions to configure diagnostics on your VMs to collect additional metric data. The basic host metrics are available, but to see more granular and VM-specific metrics, you need to install the Azure diagnostics extension on the VM. The Azure diagnostics extension allows additional monitoring and

diagnostics data to be retrieved from the VM.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-monitor>

156.HOTSPOT

You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1.

You install and configure a web server and a DNS server on VM1.

VM1 has the effective network security rules shown in the following exhibit.

 Network Interface: **vm1900** [Effective security rules](#) [Topology](#) 
 Virtual network/subnet: **VMRG-vnet/default** Public IP: **104.40.215.211** Private IP: **10.0.0.5** Accelerated networking: **Disabled**

INBOUND PORT RULES

 Network security group **VM1-nsg** (attached to network interface: **vm1900**) [Add inbound port rule](#)
 Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
900	⚠ Rule2	50-60	Any	Any	Any	 Deny ...
1000	⚠ default-allow-rdp	3389	TCP	Any	Any	 Allow ...
1010	Rule1	50-500	TCP	Any	Any	 Allow ...
65000	AllowVnetInBound	Any	Any	VirtualNet...	VirtualNet...	 Allow ...
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoad...	Any	 Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	 Deny ...

OUTBOUND PORT RULES

 Network security group **VM1-nsg** (attached to network interface: **vm1900**) [Add outbound port](#)
 Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
1000	Rule3	80	Any	Any	Any	 Deny ...
65000	AllowVnetOutBound	Any	Any	VirtualNet...	VirtualNet...	 Allow ...
65001	AllowInternetOutBou...	Any	Any	Any	Internet	 Allow ...
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny ...

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Internet users [answer choice].

can connect to only the DNS server on VM1
can connect to only the web server on VM1
can connect to the web server and the DNS server on VM1
cannot connect to the web server and the DNS server on VM1

If you delete Rule2, Internet users [answer choice].

can connect to only the DNS server on VM1
can connect to only the web server on VM1
can connect to the web server and the DNS server on VM1
cannot connect to the web server and the DNS server on VM1

Answer:

Internet users [answer choice].

can connect to only the DNS server on VM1
can connect to only the web server on VM1
can connect to the web server and the DNS server on VM1
cannot connect to the web server and the DNS server on VM1

If you delete Rule2, Internet users [answer choice].

can connect to only the DNS server on VM1
can connect to only the web server on VM1
can connect to the web server and the DNS server on VM1
cannot connect to the web server and the DNS server on VM1

Explanation:

Box 1:

Rule2 blocks ports 50-60, which includes port 53, the DNS port. Internet users can reach the Web server, since it uses port 80.

Box 2:

If Rule2 is removed internet users can reach the DNS server as well.

Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

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

157. You plan to deploy three Azure virtual machines named VM1, VM2, and VM3. The virtual machines will host a web app named App1.

You need to ensure that at least two virtual machines are available if a single Azure datacenter becomes unavailable.

What should you deploy?

- A. all three virtual machines in a single Availability Zone
- B. all virtual machines in a single Availability Set
- C. each virtual machine in a separate Availability Zone**
- D. each virtual machine in a separate Availability Set

Answer: 

Explanation:

Availability sets are a datacenter configuration to provide VM redundancy and availability. This configuration within a datacenter ensures that during either a planned or unplanned maintenance event,

at least one virtual machine is available.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets>

158. You have an Azure subscription that contains an Azure virtual machine named VM1. VM1 runs a financial reporting app named App1 that does not support multiple active instances.

At the end of each month, CPU usage for VM1 peaks when App1 runs.

You need to create a scheduled runbook to increase the processor performance of VM1 at the end of each month.

What task should you include in the runbook?

- A. Add the Azure Performance Diagnostics agent to VM1.
- B. Modify the VM size property of VM1.**
- C. Add VM1 to a scale set.
- D. Increase the vCPU quota for the subscription.
- E. Add a Desired State Configuration (DSC) extension to VM1.

Answer: B

Explanation:

If you have a CPU/performance issue then the solution is to scale up (increase VM size) or to scale out (scale set) given that the App does not support multiple instances then scale up is the obvious choice.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/resize-vm>

159. You recently created a new Azure subscription that contains a user named Admin1.

Admin1 attempts to deploy an Azure Marketplace resource by using an Azure Resource Manager template. Admin1 deploys the template by using Azure PowerShell and receives the following error message: "User failed validation to purchase resources. Error message: "Legal terms have not been accepted for this item on this subscription. To accept legal terms, please go to the Azure portal (<http://go.microsoft.com/fwlink/?LinkId=534873>) and configure programmatic deployment for the Marketplace item or create it there for the first time."

You need to ensure that Admin1 can deploy the Marketplace resource successfully.

What should you do?

- A. From Azure PowerShell, run the Set-AzApiManagementSubscription cmdlet
- B. From the Azure portal, register the Microsoft.Marketplace resource provider
- C. From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet**
- D. From the Azure portal, assign the Billing administrator role to Admin1

Answer: C

Explanation:

The Set-AzMarketplaceTerms cmdlet saves the terms object for given publisher id(Publisher), offer id(Product) and plan id(Name) tuple.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-4.5.0>

160. You have an Azure virtual machine named VM1 that runs Windows Server 2019.

You sign in to VM1 as a user named User 1 and perform the following actions:

- * Create files on drive C.
- * Create files on drive D.
- * Modify the screen saver timeout.
- * Change the desktop background. You plan to redeploy VM1.

Which changes will be lost after you redeploy VM1?

- A. the modified screen saver timeout
- B. the new desktop background
- C. the new files on drive D**
- D. The new files on drive C

Answer: C

Explanation:

As D drive is temporary storage so new files on D drive will be lost. The screensaver, wall paper, new files on C drive are available after Redeploy.

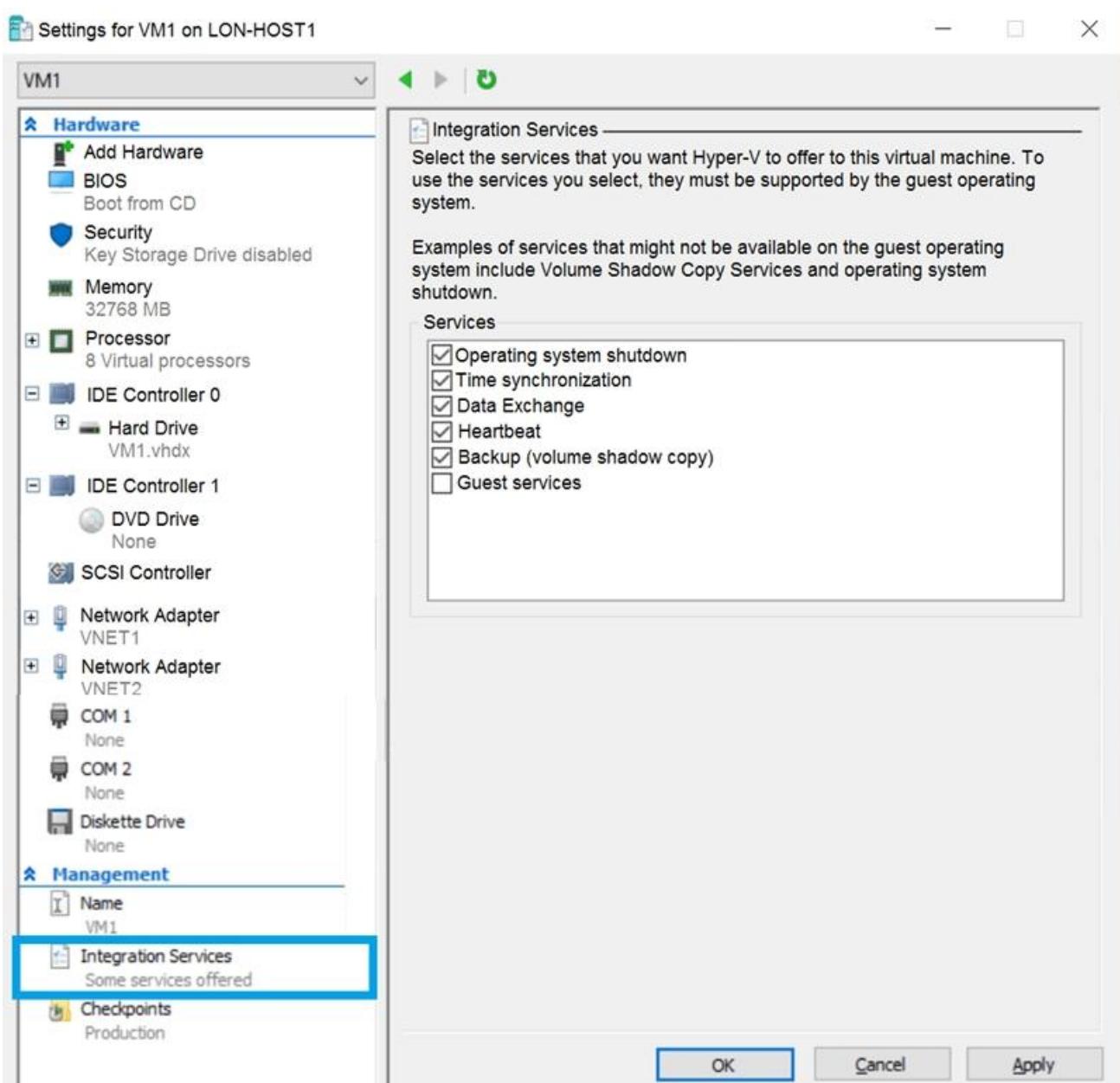
Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/redeploy-to-new-node-windows>

161. You have an Azure subscription.

You have an on-premises virtual machine named VM1.

The settings for VM1 are shown in the exhibit. (Click the Exhibit button.)



You need to ensure that you can use the disks attached to VM1 as a template for Azure virtual machines.

What should you modify on VM1?

- A. Integration Services
- B. the network adapters
- C. the memory
- D. the hard drive**
- E. the processor

Answer: D

Explanation:

From the exhibit we see that the disk is in the VHDX format.

Before you upload a Windows virtual machines (VM) from on-premises to Microsoft Azure, you must prepare the virtual hard disk (VHD or VHDX). Azure supports only generation 1 VMs that are in the VHD file format and have a fixed sized disk. The maximum size allowed for the VHD is 1,023 GB. You can

convert a generation 1 VM from the VHDX file system to VHD and from a dynamically expanding disk to fixed-sized.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image?toc=%2fazure%2fvirtual-machines%2fwindows%2ftoc.json>

162. HOTSPOT

You have an Azure subscription that contains a virtual machine scale set.

The scale set contains four instances that have the following configurations:

- Operating system: Windows Server 2016
- Size: Standard_D1_v2

You run the `get-azvmss` cmdlet as shown in the following exhibit:

```
PS Azure:> (Get-AzVmss -Name WebProd -ResourceGroupName RG1).VirtualMachineProfile.OsProfile.WindowsConfiguration
ProvisionVMAgent : True
EnableAutomaticUpdates : False
TimeZone :
AdditionalUnattendContent :
WinRM :

Azure:/
PS Azure:> Get-AzVmss -Name WebProd -ResourceGroupName RG1 | Select -ExpandProperty UpgradePolicy
Mode RollingUpgradePolicy AutomaticOSUpgradePolicy
----- Microsoft.Azure.Management.Compute.Models.AutomaticOSUpgradePolicy
Automatic

Azure:/
PS Azure:> []
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

When an administrator changes the virtual machine size, the size will be changed on up to [answer choice] virtual machines simultaneously.

▼
0
1
2
4

When a new build of the Windows Server 2016 image is released, the new build will be deployed to up to [answer choice] virtual machines simultaneously.

▼
0
1
2
4

Answer:

Answer Area

When an administrator changes the virtual machine size, the size will be changed on up to **[answer choice]** virtual machines simultaneously.

0
1
2
4



When a new build of the Windows Server 2016 image is released, the new build will be deployed to up to **[answer choice]** virtual machines simultaneously.

UpgradePolicy = Automatic: 20% of VMs will be upgrade at the same time (Min=1) => 1 VM

0
1
2
4

Explanation:

The Get-AzVmssVM cmdlet gets the model view and instance view of a Virtual Machine Scale Set (VMSS) virtual machine.

Box 1: 0

The enableAutomaticUpdates parameter is set to false. To update existing VMs, you must do a manual upgrade of each existing VM.

Box 2: 1

Below is clearly mentioned in the official Website

"The upgrade orchestrator identifies the batch of VM instances to upgrade, with any one batch having a maximum of 20% of the total instance count, subject to a minimum batch size of one virtual machine."

So, 20% from 4 ~1

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-upgrade-scale-set>

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-automatic-upgrade>

163. You have an Azure subscription named Subscription1 that is used by several departments at your company.

Subscription1 contains the resources in the following table:

Name	Type
Storage1	Storage account
RG1	Resource group
Container1	Blob container
Share1	File share

Another administrator deploys a virtual machine named VM1 and an Azure Storage account named Storage2 by using a single Azure Resource Manager template.

You need to view the template used for the deployment.

From which blade can you view the template that was used for the deployment?

- A. RG1
- B. VM1
- C. Storage1
- D. Container1

Answer: A

Explanation:

1. View template from deployment history

Go to the resource group for your new resource group. Notice that the portal shows the result of the last deployment. Select this link.

2. You see a history of deployments for the group. In your case, the portal probably lists only one deployment. Select this deployment.

The portal displays a summary of the deployment. The summary includes the status of the deployment and its operations and the values that you provided for parameters. To see the template that you used for the deployment, select View template.

Microsoft Azure < exportsite - Deployments > Microsoft.WebSiteSQLDatabased13386b0-9908 Deployment

Microsoft.WebSiteSQLDatabased13386b0-9908 Deployment

Summary

DEPLOYMENT DATE: 7/5/2017 4:01:15 PM

STATUS: Succeeded

DURATION: 1 minute 30 seconds

RESOURCE GROUP: exportsite

RELATED: Events

References:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template>

164. You have an Azure web app named App1.

App1 has the deployment slots shown in the following table:

Name	Function
webapp1-prod	Production
webapp1-test	Staging

In webapp1-test, you test several changes to App1.

You back up App1.

You swap webapp1-test for webapp1-prod and discover that App1 is experiencing performance issues.

You need to revert to the previous version of App1 as quickly as possible.

What should you do?

- A. Redeploy App1
- B. Swap the slots**
- C. Clone App1
- D. Restore the backup of App1

Answer: B

Explanation:

When you swap deployment slots, Azure swaps the Virtual IP addresses of the source and destination slots, thereby swapping the URLs of the slots. We can easily revert the deployment by swapping back.

You can validate app changes in a staging deployment slot before swapping it with the production slot.

Deploying an app to a slot first and swapping it into production makes sure that all instances of the slot are warmed up before being swapped into production. This eliminates downtime when you deploy your app. The traffic redirection is seamless, and no requests are dropped because of swap operations. You can automate this entire workflow by configuring auto swap when pre-swap validation isn't needed.

After a swap, the slot with previously staged app now has the previous production app. If the changes swapped into the production slot aren't as you expect, you can perform the same swap immediately to get your "last known good site" back.

Reference: <https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots>

165. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: From the Resource providers blade, you unregister the Microsoft.ClassicNetwork provider.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You should use a policy definition.

Reference: <https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

166.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You configure a custom policy definition, and then you assign the policy to the subscription.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

References: <https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

167.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You create a resource lock, and then you assign the lock to the subscription.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

How can I freeze or lock my production/critical Azure resources from accidental deletion? There is way to do this with both ASM and ARM resources using Azure resource lock.

References:

<https://blogs.msdn.microsoft.com/azureedu/2016/04/27/using-azure-resource-manager-policy-and-azure>

-lock-to-control-your-azure-resources/

168. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You assign a built-in policy definition to the subscription.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. However, there are no built-in policy definitions. Though there are sample policy definitions.

Reference: <https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

169. You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2.

VM1 hosts a frontend application that connects to VM2 to retrieve data.

Users report that the frontend application is slower than usual.

You need to view the average round-trip time (RTT) of the packets from VM1 to VM2.

Which Azure Network Watcher feature should you use?

A. NSG flow logs

B. Connection troubleshoot

C. IP flow verify

D. Connection monitor

Answer: D

Explanation:

The Connection Monitor feature in Azure Network Watcher is now generally available in all public regions.

Connection Monitor provides you RTT values on a per-minute granularity. You can monitor a direct TCP connection from a virtual machine to a virtual machine, FQDN, URI, or IPv4 address.

References:

<https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/>

170. You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named VNet1.

You need to ensure that you can configure a point-to-site connection from an on-premises computer to VNet1.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add a service endpoint to VNet1
- B. Reset GW1
- C. Create a route-based virtual network gateway**
- D. Add a connection to GW1
- E. Delete GW1**

F. Add a public IP address space to VNet1

Answer: C,E

Explanation:

C: A VPN gateway is used when creating a VPN connection to your on-premises network. Route-based VPN devices use any-to-any (wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface).

E: Policy-based VPN devices use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering.

IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/create-routebased-vpn-gateway-portal>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

171.HOTSPOT

You have an Azure subscription named Subscription1.

Subscription1 contains the resources in the following table.

Name	Type
VMRG	Resource group
VNet1	Virtual network
VNet2	Virtual network
VM5	Virtual machine connected to VNet1
VM6	Virtual machine connected to VNet2

In Azure, you create a private DNS zone named adatum.com. You set the registration virtual network to VNet2.

The adatum.com zone is configured as shown in the following exhibit.

Resource group ([change](#))
vmrg

Name server 1

-

Subscription ([change](#))
Azure Pass

Name server 2

-

Subscription ID
a4fde29b-d56a-4f6c-8298-6c53cd0b720c

Name server 3

-

Tags ([change](#))
[Click here to add tags](#)

Name server 4

-

 [Search record sets](#)

Name	Type	TTL	VALUE
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: internal.cloudapp.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1
vm1	A	3600	10.1.0.4
vm9	A	3600	10.1.0.12

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
The A record for VM5 will be registered automatically in the adatum.com zone.	<input type="radio"/>	<input type="radio"/>
VM5 can resolve VM9.adatum.com.	<input type="radio"/>	<input type="radio"/>
VM6 can resolve VM9.adatum.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Azure DNS provides automatic registration of virtual machines from a single virtual network that's linked to a private zone as a registration virtual network. VM5 does not belong to the registration virtual network though.

Statements

Yes

No

The A record for VM5 will be registered automatically in the adatum.com zone.

VM5 can resolve VM9.adatum.com.

VM6 can resolve VM9.adatum.com.

Explanation:

Box 1: No

Azure DNS provides automatic registration of virtual machines from a single virtual network that's linked to a private zone as a registration virtual network. VM5 does not belong to the registration virtual network though.

Box 2: No

Forward DNS resolution is supported across virtual networks that are linked to the private zone as resolution virtual networks. VM5 does belong to a resolution virtual network.

Box 3: Yes

VM6 belongs to registration virtual network, and an A (Host) record exists for VM9 in the DNS zone.

By default, registration virtual networks also act as resolution virtual networks, in the sense that DNS resolution against the zone works from any of the virtual machines within the registration virtual network.

References: <https://docs.microsoft.com/en-us/azure/dns/private-dns-overview>

172.HOTSPOT

You have an Azure subscription that contains a virtual network named VNet1.

VNet1 uses an IP address space of 10.0.0.0/16 and contains the subnets in the following table.

Name	IP address range
Subnet0	10.0.0.0/24
Subnet1	10.0.1.0/24
Subnet2	10.0.2.0/24
GatewaySubnet	10.0.254.0/24

Subnet1 contains a virtual appliance named VM1 that operates as a router.

You create a routing table named RT1.

You need to route all inbound traffic to VNet1 through VM1.

How should you configure RT1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Address prefix

10.0.0.0/16
10.0.1.0/24
10.0.254.0/24

Next hop type

Virtual appliance
Virtual network
Virtual network gateway

Assigned to

GatewaySubnet
Subnet0
Subnet1 and Subnet2

Answer:

Answer Area

Address prefix

10.0.0.0/16
10.0.1.0/24
10.0.254.0/24

Next hop type

Virtual appliance
Virtual network
Virtual network gateway

Assigned to

GatewaySubnet
Subnet0
Subnet1 and Subnet2

Explanation:

Box1: 10.0.0.0/16

Address prefix in networking refer to the destination IP address range. In this scenario, destination is Vnet1, hence Address prefix will be the address space of Vnet1.

Box 2: Virtual appliance

Next hop gets the next hop type and IP address of a packet from a specific VM and NIC. Knowing the next hop helps you determine if traffic is being directed to the intended destination, or whether the traffic is being sent nowhere

Next Hop --> VM1 --> Virtual Appliance (You can specify IP address of VM 1 when configuring next hop as virtual appliance)

Box 3: GatewaySubnet

In the scenario it is asked for all the inbound traffic to Vnet1. Inbound traffic is flowing through SubnetGW. You need to route all inbound traffic from the VPN gateway to VNet1 through VM1. So its traffic from Gateway subnet only.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/manage-route-table#create-a-route-table>

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-next-hop-overview>

173. You have a virtual network named VNet1 as shown in the exhibit. (Click the Exhibit tab.)

Refresh	Move	Delete
Resource group (change) Production		Address space 10.2.0.0/16
Location West US		DNS servers Azure provided DNS service
Subscription (change) Production subscription		
Subscription ID 14d26092-8e42-4ea7-b770-9dcef70fb1ea		
Tags (change) Click here to add tags		

Connected devices

 Search connected devices
--

DEVICE	TYPE	IP ADDRESS	SUBNET
No results.			

No devices are connected to VNet1.

You plan to peer VNet1 to another virtual network named VNet2 in the same region. VNet2 has an address space of 10.2.0.0/16.

You need to create the peering.

What should you do first?

- A. Configure a service endpoint on VNet2.
- B. Modify the address space of VNet1.**
- C. Add a gateway subnet to VNet1.
- D. Create a subnet on VNet1 and VNet2.

Answer: B

Explanation:

The virtual networks you peer must have non-overlapping IP address spaces. The exhibit indicates that VNet1 has an address space of 10.2.0.0/16, which is the same as VNet2, and thus overlaps. We need to change the address space for VNet1.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints>

174. You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Floating IP (direct server return) to Enabled
- B. Idle Time-out (minutes) to 20
- C. Protocol to UDP
- D. Session persistence to Client IP and Protocol**

Answer: D

Explanation: With Sticky Sessions when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For Sticky Sessions set Session persistence to Client IP or to Client IP and protocol.

On the following image you can see sticky session configuration:

Note:

§ Client IP and protocol specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.

§ Client IP specifies that successive requests from the same client IP address will be handled by the same virtual machine.

Reference: <https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/>

175. HOTSPOT

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

Name	Operating system	Connects to
VM1	Windows Server 2019	Subnet1
VM2	Windows Server 2019	Subnet2

VM1 and VM2 use public IP addresses. From Windows Server 2019 on VM1 and VM2, you allow inbound Remote Desktop connections.

Subnet1 and Subnet2 are in a virtual network named VNET1.

The subscription contains two network security groups (NSGs) named NSG1 and NSG2. NSG1 uses only the default rules.

NSG2 uses the default rules and the following custom incoming rule:

- Priority: 100
- Name: Rule1
- Port: 3389
- Protocol: TCP
- Source: Any
- Destination: Any
- Action: Allow

NSG1 is associated to Subnet1. NSG2 is associated to the network interface of VM2.

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

NSG1 has default rules, which denies any port open for inbound rules

Statements	Yes	No
From the Internet, you can connect to VM1 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to VM2 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to VM2 by using Remote Desktop	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
From the Internet, you can connect to VM1 by using Remote Desktop.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to VM2 by using Remote Desktop.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can connect to VM2 by using Remote Desktop	<input checked="" type="radio"/>	<input type="radio"/>

Explanation: VM1 and VM2 are in the same Vnet. By default, communication is allowed.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

176.HOTSPOT

You have a virtual network named VNET1 that contains the subnets shown in the following table:

Name	Subnet	Network security group (NSG)
Subnet1	10.10.1.0/24	NSG1
Subnet2	10.10.2.0/24	None

You have two Azure virtual machines that have the network configurations shown in the following table:

Name	Subnet	IP address	NSG
VM1	Subnet1	10.10.1.5	NSG2
VM2	Subnet2	10.10.2.5	None
VM3	Subnet2	10.10.2.6	None

For NSG1, you create the inbound security rule shown in the following table:

Priority	Source	Destination	Destination port	Action
101	10.10.2.0/24	10.10.1.0/24	TCP/1433	Allow

For NSG2, you create the inbound security rule shown in the following table:

Priority	Source	Destination	Destination port	Action
125	10.10.2.5	10.10.1.5	TCP/1433	Block

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

The priority of the rules is only relevant within the same NSG, not across different NSG

Answer Area

Statements	Yes	No
VM2 can connect to the TCP port 1433 services on VM1.	<input type="radio"/>	<input type="radio"/>
VM1 can connect to the TCP port 1433 services on VM2.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to the TCP port 1433 services on VM3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM2 can connect to the TCP port 1433 services on VM1.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
VM1 can connect to the TCP port 1433 services on VM2.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can connect to the TCP port 1433 services on VM3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes

The inbound security rule for NSG1 allows TCP port 1433 from 10.10.2.0/24 (or Subnet2 where VM2 and VM3

are located) to 10.10.1.0/24 (or Subnet1 where VM1 is located) while the inbound security rule for NSG2 blocks TCP port 1433 from 10.10.2.5 (or VM2) to 10.10.1.5 (or VM1). However, the NSG1 rule has a higher

priority (or lower value) than the NSG2 rule.

Box 2: Yes

No rule explicitly blocks communication from VM1. The default rules, which allow communication, are thus

applied.

Box 3: Yes

No rule explicitly blocks communication between VM2 and VM3 which are both on Subnet2. The default rules, which allow communication, are thus applied.

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

177.HOTSPOT

You have an Azure subscription named Subscription1.

Subscription1 contains the virtual machines in the following table.

Name	IP address
VM1	10.0.1.4
VM2	10.0.2.4
VM3	10.0.3.4

Subscription1 contains a virtual network named VNet1 that has the subnets in the following table.

Name	Address space	Connected virtual machine
Subnet1	10.0.1.0/24	VM1
Subnet2	10.0.2.0/24	VM2
Subnet3	10.0.3.0/24	VM3

VM3 has a network adapter named NIC3. IP forwarding is enabled on NIC3. Routing is enabled on VM3.

You create a route table named RT1.

RT1 is associated to Subnet1 and Subnet2 and contains the routes in the following table.

Address prefix	Next hop type	Next hop address
10.0.1.0/24	Virtual appliance	10.0.3.4
10.0.2.0/24	Virtual appliance	10.0.3.4

You apply RT1 to Subnet1.

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
Network traffic from VM3 can reach VM1.	<input type="radio"/>	<input type="radio"/>
If VM3 is turned off, network traffic from VM2 can reach VM1.	<input type="radio"/>	<input type="radio"/>
Network traffic from VM1 can reach VM2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

The routing table allows connections from VM3 to VM1 and VM2. And as IP forwarding is enabled on VM3, VM3 can connect to VM1.

Statements	Yes	No
Network traffic from VM3 can reach VM1.	<input checked="" type="radio"/>	<input type="radio"/>
VM3, which has IP forwarding, must be turned on, in order for VM2 to connect to VM1.	<input type="radio"/>	<input checked="" type="radio"/>
If VM3 is turned off, network traffic from VM2 can reach VM1.	<input type="radio"/>	<input checked="" type="radio"/>
Network traffic from VM1 can reach VM2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation: The routing table allows connections from VM1 and VM2 to VM3. IP forwarding on VM3 allows VM1 to connect to VM2 via VM3.

Box 1: Yes

Traffic from VM1 and VM2 can reach VM3 thanks to the routing table, and as IP forwarding is enabled on VM3, traffic from VM3 can reach VM1.

Box 2: No

VM3, which has IP forwarding, must be turned on, in order for traffic from VM2 to reach VM1.

Box 3: Yes

The traffic from VM1 will reach VM3, which thanks to IP forwarding, will send the traffic to VM2.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

178.Your on-premises network contains an SMB share named Share1.

You have an Azure subscription that contains the following resources:

A web app named webapp1

A virtual network named VNET1

You need to ensure that webapp1 can connect to Share1.

What should you deploy?

A. an Azure Application Gateway

B. an Azure Active Directory (Azure AD) Application Proxy

C. an Azure Virtual Network Gateway

Answer: C

Explanation:

A Site-to-Site VPN gateway connection can be used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.

This type of connection requires a VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

179.You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

A. Azure Active Directory (Azure AD) Application Proxy

B. Azure Application Insights

C. Azure Custom Script Extension

D. the New-AzConfigurationAssignment cmdlet

Answer: C

Explanation:

The Custom Script Extension downloads and executes scripts on Azure VMs. This extension is useful for post deployment configuration, software installation, or any other configuration / management task. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run time.

The Custom Script extension integrates with Azure Resource Manager templates, and can also be run using the Azure CLI, PowerShell, Azure portal, or the Azure Virtual Machine REST API. You can use the

Custom Script Extension with both Windows and Linux VMs.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-automate-vm-deployment?toc=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-machines%2Fextensions%2Ftoc.json&bc=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fbread%2Ftoc.json>

180. You have an Azure web app named webapp1.

Users report that they often experience HTTP 500 errors when they connect to webapp1.

You need to provide the developers of webapp1 with real-time access to the connection errors.

The solution must provide all the connection error details.

What should you do first?

- A. From webapp1, enable Web server logging
- B. From Azure Monitor, create a workbook
- C. From Azure Monitor, create a Service Health alert
- D. From webapp1, turn on Application Logging

Answer: A

Explanation:

To resolve this you need to catch connection error. When the connection fails for webapp, it happens on web server, not within application.

You can find out the web server log by below steps:

Open the web application --> Go to Application Service logs --> Go to Web server logging (there are multiple switches there)

You can also see the errors live going to "Log stream" pane.

To ensure that you will get web server log, you have to enable it.

Web server logging	Windows logging	App Service file system or Azure Storage blobs	Raw HTTP request data in the W3C extended log file format . Each log message includes data such as the HTTP method, resource URI, client IP, client port, user agent, response code, and so on.
-----------------------	--------------------	--	---

Reference: <https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs>

181.HOTSPOT

You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit:

Policy1

Associated items Delete Save Discard

Backup schedule

* Frequency * Time * Timezone

Daily 11:00 PM (UTC) Coordinated Universal Time

Retention range

Retention of daily backup point

* At For
 11:00 PM 30 Day(s)

Retention of weekly backup point

* On * At For
 Sunday 11:00 PM 10 Week(s)

Retention of monthly backup point

Week Based Day Based

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

Answer:

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

Explanation:

Box 1: 10 years

The yearly backup point occurs to 1 March and its retention period is 10 years.

Box 2: 36 months

The monthly backup point occurs on the 1st of every month and its retention period is 36 months.

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

Name	Azure region
VM1	West Europe
VM2	West Europe
VM3	North Europe
VM4	North Europe

You have a Recovery Services vault that protects VM1 and VM2.

You need to protect VM3 and VM4 by using Recovery Services.

What should you do first?

- A. Configure the extensions for VM3 and VM4.
- B. Create a new Recovery Services vault.**
- C. Create a storage account.
- D. Create a new backup policy.

VM3 and VM4 are in a different region from VM1 and VM2. So, we need to create a new Recovery Services Vault in the same region with VM3 and VM4.

Answer: B

Explanation:

A Recovery Services vault is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services

References:

<https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-enable-replication>

183. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Subscription1, you assign the Logic App Operator role to the Developers group.

Does this meet the goal?

- A. Yes **Logic App Operator - Lets you read, enable, and disable logic apps, but not edit or update them.**

B. No

Answer: B Logic App Contributor - Lets you create, manage logic apps, but not access to them.

The Logic App Operator role only lets you read, enable and disable logic app. With it you can view the logic app and run history, and enable/disable. Cannot edit or update the definition.

You would need the Logic App Contributor role.

References:

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

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app>

184.HOTSPOT

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1.

You add the users in the following table.

User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

User1: The Owner Role lets you manage everything, including access to resources.

User3: The Network Contributor role lets you manage networks, including creating subnets

Add a subnet to VNet1:

- User1 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Assign a user the Reader role to VNet1:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Answer:

Add a subnet to VNet1:

- User1 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Assign a user the Reader role to VNet1:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Explanation:

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

185. You have an Azure subscription that contains a user account named User1.

You need to ensure that User1 can assign a policy to the [tenant root management group](#).

What should you do?

- A. Create a new management group and delegate User1 as the owner of the new management group.

B. Assign the Owner role for the Azure subscription to User1, and then instruct User1 to configure access management for Azure resources.

C. Assign the Owner role for the Azure subscription to User1, and then modify the default conditional access policies.

D. Assign the Global administrator role to User1, and then instruct User1 to configure access management for Azure resources.

Answer: B

186.HOTSPOT

You have an Azure subscription named Subscription1 that contains the following resource group:

- Name: RG1
- Region: West US
- Tag: "tag1": "value1"

You assign an Azure policy named Policy1 to Subscription1 by using the following configurations:

- Exclusions: None
- Policy definition: Append tag and its default value
- Assignment name: Policy1
- Parameters:
- Tag name: Tag2
- Tag value: Value2

After Policy1 is assigned, you create a storage account that has the following configurations:

- Name: storage1
- Location: West US
- Resource group: RG1
- Tags: "tag3": "value3"

You need to identify which tags are assigned to each resource.

What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Tags assigned to RG1:

- "tag1": "value1" only
- "tag2": "value2" only
- "tag1": "value1" and "tag2": "value2"

Tags assigned to storage1:

- "tag3": "value3" only
- "tag1": "value1" and "tag3": "value3"
- "tag2": "value2" and "tag3": "value3"
- "tag1": "value1", "tag2": "value2", and "tag3": "value3"

Answer:

Tags assigned to RG1:

```
"tag1": "value1" only
"tag2": "value2" only
"tag1": "value1" and "tag2": "value2"
```

Tags assigned to storage1:

```
"tag3": "value3" only
"tag1": "value1" and "tag3": "value3"
"tag2": "value2" and "tag3": "value3"
"tag1": "value1", "tag2": "value2", and "tag3": "value3"
```

Explanation:

Box 1: "tag1": "value1" only

Box 2: "tag2": "value2" and "tag3": "value3"

Tags applied to the resource group are not inherited by the resources in that resource group.

References: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>

187. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group
VNET1	Virtual network	RG1
VM1	Virtual machine	RG1

The Not allowed resources types Azure policy is assigned to RG1 and uses the following parameters:

`Microsoft.Network/virtualNetworks`

`Microsoft.Compute/virtualMachines`

In RG1, you need to create a new virtual named VM2, and then connected VM2 to VNET1.

What should you do first?

- A. Remove Microsoft.Network/virtualNetworks from the policy.
- B. Create an Azure Resource Manager template.
- C. Remove Microsoft.Compute/virtualMachines from the policy.
- D. Add a subnet to VNET1.

Answer: C

Explanation:

The Not allowed resource types Azure policy prohibits the deployment of specified resource types.

You specify an array of the resource types to block.

Virtual Networks and Virtual Machines are prohibited.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/samples/not-allowed-resource-types>

188. You have an Azure web app named webapp1.

You have a virtual network named VNET1 and an Azure virtual machine named VM1 that hosts a MySQL database. VM1 connects to VNET1. You need to ensure that webapp1 can access the data hosted on VM1.

What should you do?

- A. Connect webapp1 to VNET1.
- B. Peer VNET1 to another virtual network.
- C. Deploy an Azure Application Gateway.
- D. Deploy an internal load balancer

Answer: C

189. Your company has three offices. The offices are located in Miami, Los Angeles, and New York.

Each office contains a datacenter.

You have an Azure subscription that contains resources in the East US and West US Azure regions. Each region contains a virtual network. The virtual networks are peered.

You need to connect the datacenters to the subscription. The solution must minimize network latency between the datacenters.

What should you create?

- A. three virtual WANs and one virtual hub
- B. three virtual hubs and one virtual WAN
- C. three On-premises data gateways and one Azure Application Gateway
- D. three Azure Application Gateways and one On-premises data gateway

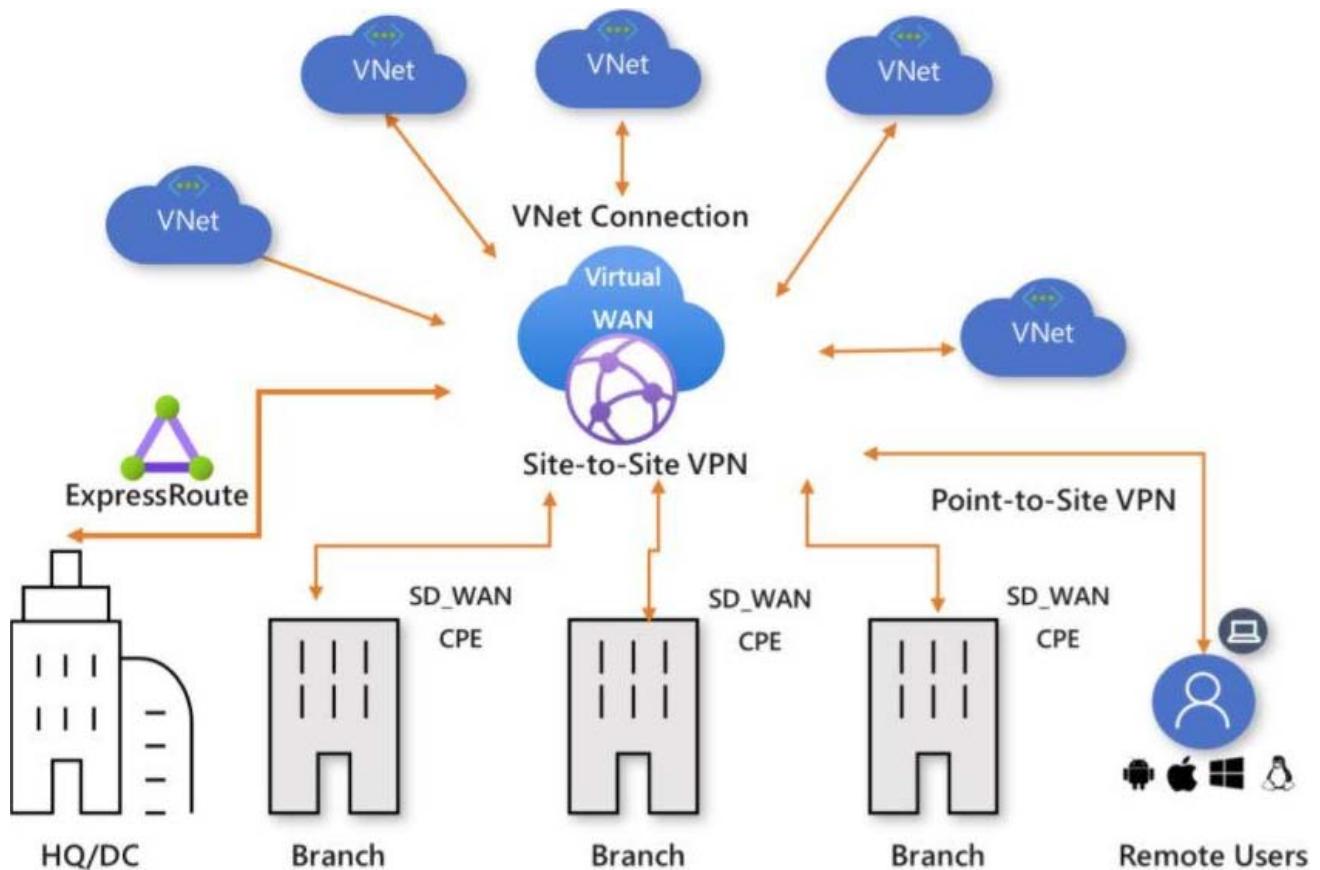
Answer: A

Explanation:

Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface.

The Virtual WAN architecture is a hub and spoke architecture with scale and performance built in for branches (VPN/SD-WAN devices), users (Azure VPN/OpenVPN/IKEv2 clients), ExpressRoute circuits, and virtual networks.

Azure regions serve as hubs that you can choose to connect to. All hubs are connected in full mesh in a Standard Virtual WAN making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) connectivity.



Virtual WAN offers the following advantages:

Integrated connectivity solutions in hub and spoke: Automate site-to-site configuration and connectivity between on-premises sites and an Azure hub.

Automated spoke setup and configuration: Connect your virtual networks and workloads to the Azure hub seamlessly.

Intuitive troubleshooting: You can see the end-to-end flow within Azure, and then use this information to take required actions.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

190. You have a Recovery Service vault that you use to test backups. The test backups contain two protected virtual machines.

You need to delete the Recovery Services vault.

What should you do first?

- From the Recovery Service vault, stop the backup of each backup item.
- From the Recovery Service vault, delete the backup data.
- Modify the disaster recovery properties of each virtual machine.
- Modify the locks of each virtual machine.

Answer: A

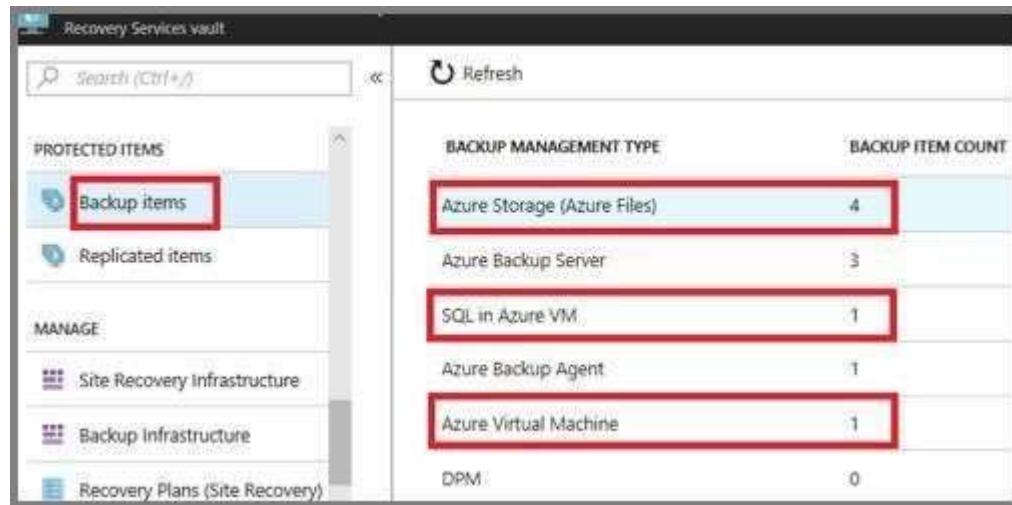
Explanation:

You can't delete a Recovery Services vault if it is registered to a server and holds backup data. If you try to delete a vault, but can't, the vault is still configured to receive backup data.

Remove vault dependencies and delete vault

In the vault dashboard menu, scroll down to the Protected Items section, and click Backup Items. In this

menu, you can stop and delete Azure File Servers, SQL Servers in Azure VM, and Azure virtual machines.



The screenshot shows the 'Recovery Services vault' interface. On the left, a sidebar lists 'PROTECTED ITEMS' with 'Backup items' selected (highlighted with a red box). Below that are 'Replicated items', 'MANAGE' with 'Site Recovery Infrastructure', 'Backup Infrastructure', and 'Recovery Plans (Site Recovery)', and a 'Search (Ctrl+Shift+F)' bar. On the right, a table titled 'BACKUP MANAGEMENT TYPE' shows the following data:

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Storage (Azure Files)	4
Azure Backup Server	3
SQL in Azure VM	1
Azure Backup Agent	1
Azure Virtual Machine	1
DPM	0

References: <https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault>

191.HOTSPOT

You have an Azure subscription named Subscription1.

In Subscription1, you create an alert rule named Alert1.

The Alert1 action group is configured as shown in the following exhibit.

```
PS Azure:\> Get-AzureRmActionGroup

ResourceGroupName: default-activitylogalerts
GroupShortName  : AG1
Enabled         : True
EmailReceivers  : {Action1_-EmailAction-}
SmsReceivers    : {Action1_-SMSAction-}
WebhookReceivers: {}
Id             : /subscriptions/a4fde29b-d56a-4f6c-8298-6c53cd0b720c/
resourceGroups/default-activitylogalerts/providers/microsoft.insights/actionGroups/ActionGroup1
Name           : ActionGroup1
Type           : Microsoft.Insights/ActionGroups
Location       : Global
Tags           : {}
```

Alert1 alert criteria is triggered every minute.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

The number of email messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

The number of SMS messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

Answer:

The number of email messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

The number of SMS messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

Explanation:

Box 1: 60

One alert per minute will trigger one email per minute.

Box 2: 12

No more than 1 SMS every 5 minutes can be send, which equals 12 per hour.

Note: Rate limiting is a suspension of notifications that occurs when too many are sent to a particular phone number, email address or device. Rate limiting ensures that alerts are manageable and actionable. The rate limit thresholds are:

SMS: No more than 1 SMS every 5 minutes.

Voice: No more than 1 Voice call every 5 minutes.

Email: No more than 100 emails in an hour.

Other actions are not rate limited.

References:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/monitoring-and-diagnostics/monitoring-overview-alerts.md>

192. You have an app named App1 that runs on an Azure web app named webapp1.

The developers at your company upload an update of App1 to a Git repository named GUI.

Webapp1 has the deployment slots shown in the following table.

Name	Function
webapp1-prod	Production
webapp1-test	Staging

You need to ensure that the App1 update is tested before the update is made available to users.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE Each correct selection is worth one point.

- A. Stop webapp1 prod.
- B. Stop webapp1-test
- C. Deploy the App1 update to webapp1-test, and then test the update.
- D. Deploy the App1 update to webapp1-prod, and then test the update.
- E. Swap the slots.

Answer: C,E

Explanation:

You can validate web app changes in a staging deployment slot before swapping it with the production slot. Deploying an app to a slot first and swapping it into production makes sure that all instances of the slot are warmed up before being swapped into production. This eliminates downtime when you deploy your app. The traffic redirection is seamless, and no requests are dropped because of swap operations. You can automate this entire workflow by configuring auto swap when pre-swap validation isn't needed.

After the swap you can deploy the App1 update to webapp1-test, and then test the update. If the changes swapped into the production slot aren't as per your expectation then you can perform the same swap immediately to get your "last known good site" back.

Reference: <https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots>

193. You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1.

You have a computer named Computer1 that runs Windows 10. Computer1 is connected to the Internet.

You add a network interface named Interface1 to VM1 as shown in the exhibit (Click the Exhibit button.)

 **Network Interface: Interface1** **Effective security rules** **Topology** 
 Virtual network/subnet: VMRD-vnet/default Public IP: IP2 Private IP: 10.0.0.6
 Accelerated networking: **Disabled**

INBOUND PORT RULES

 Network security group **VM1-nsg** (attached to network interface: **Interface1**)
 Impacts 0 subnets, 2 network interfaces

Add inbound

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINA...	ACTION	...
1000	 default-allow-...	3389	TCP	Any	Any	 Allow	
65000	AllowVnetInBound	Any	Any	VirtualN...	VirtualN...	 Allow	
65001	AllowAzureLoadB...	Any	Any	AzureLo...	Any	 Allow	
65500	AllowAllInBound	Any	Any	Any	Any	 Deny	

OUTBOUND PORT RULES

 Network security group **VM1-nsg** (attached to network interface: **Interface1**)
 Impacts 0 subnets, 2 network interfaces

Add outbound

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINA...	ACTION	...
65000	AllowVnetOutBo...	Any	Any	VirtualN...	VirtualN...	 Allow	
65001	AllowInternetOut...	Any	Any	Any	Internet	 Allow	
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny	

From Computer1, you attempt to connect to VM1 by using Remote Desktop, but the connection fails. You need to establish a Remote Desktop connection to VM1.

What should you do first?

- A. Start VM1.
- B. Attach a network interface.
- C. Delete the DenyAllOutBound outbound port rule.
- D. Delete the DenyAllInBound inbound port rule.

Answer: A

Explanation:

Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

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

194. You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template. You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. a Desired State Configuration (DSC) extension
- B. the Publish-AzVMDscConfigurationCmdlet
- C. a Microsoft Intune device configuration profile
- D. Deployment Center in Azure App Service

Answer: A

Explanation:

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.

You can use the DSC extension independently of the Automation DSC service.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

195. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group	Location
RG1	Resource group	<i>Not applicable</i>	Central US
RG2	Resource group	<i>Not applicable</i>	West US
VMSS1	Virtual machine scale set	RG2	West US
Proximity1	Proximity placement group	RG1	West US
Proximity2	Proximity placement group	RG2	Central US
Proximity3	Proximity placement group	RG1	Central US

You need to configure a proximity placement group for VMSS1

Which proximity placement groups should you use?

- A. Proximity2 only
- B. Proximity 1, Proximity2, and Proximity3
- C. Proximity 1 and Proximity3 only
- D. Proximity1 only

Answer: C

196. You have an Azure subscription named Subscription1 that has the following providers registered:

- Authorization
- Automation
- Resources
- Compute
- KeyVault
- Network
- Storage
- Billing

- Web

Subscription1 contains an Azure virtual machine named VM1 that has the following configurations:

- * Private IP address: 10.0.0.4 (dynamic)
- * Network security group (NSG): NSG1
- * Public IP address: None
- * Availability set: AVSet
- * Subnet: 10.0.0.0/24
- * Managed disks: No
- * Location: East US

You need to record all the successful and failed connection attempts to VM1.

Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Register the Microsoft.Insights resource provider
- B. Add an Azure Network Watcher connection monitor
- C. Register the Microsoft.LogAnalytics provider
- D. Enable Azure Network Watcher in the East US Azure region
- E. Create an Azure Storage account
- F. Enable Azure Network Watcher flow logs

Answer: C,D,E

Explanation:

NSG flow log data is written to an Azure Storage account. You need to create an Azure Storage account, With an Azure Storage account NSG flow logs can be enabled. Enable network watcher in the East US region.

NSG flow logging requires the Microsoft. Insights provider.

References:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal>

197. You create the following resources in an subscription:

- An Azure Container Registry instance named Registry1
- An Azure Kubernetes Service (AKS) cluster named Cluster1

You create a container image named App 1 on your administrative workstation.

You need to deploy App1 to cluster 1.

What should you do first?

- A. Create a host pool on Cluster1
- B. Run the docker push command.
- C. Run the kubectl apply command.
- D. Run the az aks create command.

Answer: B

Explanation:

An Azure container registry stores and manages private Docker container images, similar to the way Docker Hub stores public Docker images. You can use the Docker command-line interface (Docker CLI) for login, push, pull, and other operations on your container registry.

After you login to the registry you can run push command to upload the image.

Below is an sample of that command

docker push myregistry.azurecr.io/samples/nginx

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-docker-cli>

198.HOTSPOT

You have an Azure subscription.

You plan to use Azure Resource Manager templates to deploy 50 Azure virtual machines that will be part of the same availability set.

You need to ensure that as many virtual machines as possible are available if the fabric fails or during servicing.

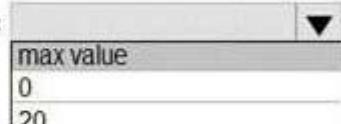
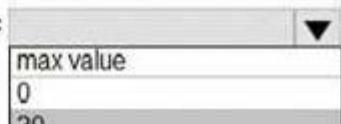
How should you configure the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/  
  deploymentTemplate.json",  
  "contentVersion": "1.0.0.0",  
  "parameters": {},  
  "resources": [  
    {  
      "type": "Microsoft.Compute/availabilitySets",  
      "name": "ha",  
      "apiVersion": "2017-12-01",  
      "location": "eastus",  
      "properties": {  
        "platformFaultDomainCount":  
          {  
            "maxValue": 0,  
            "minValue": 0,  
            "value": 20  
          },  
        "platformUpdateDomainCount":  
          {  
            "maxValue": 0,  
            "minValue": 0,  
            "value": 20  
          }  
      }  
    }  
  ]  
}
```

Answer:

```

{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/
  deploymentTemplate.json",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "resources": [
    {
      "type": "Microsoft.Compute/availabilitySets",
      "name": "ha",
      "apiVersion": "2017-12-01",
      "location": "eastus",
      "properties": {
        "platformFaultDomainCount": 
        "platformUpdateDomainCount": 
      }
    }
  ]
}

```

Explanation:

Box 1 = max value

Box 2 = 20

Explanation

Use max for platformFaultDomainCount

2 or 3 is max value, depending on which region you are in.

Use 20 for platformUpdateDomainCount

Increasing the update domain (platformUpdateDomainCount) helps with capacity and availability planning when the platform reboots nodes. A higher number for the pool (20 is max) means that fewer of their nodes in any given availability set would be rebooted at once.

References:

<https://www.itprotoday.com/microsoft-azure/check-if-azure-region-supports-2-or-3-fault-domains-manage-d-disks>

<https://github.com/Azure/acs-engine/issues/1030>

199.HOTSPOT

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

VMSS1 is set to VM (virtual machines) orchestration mode.

You need to deploy a new Azure virtual machine named VM1, and then add VM1 to VMSS1.

Which resource group and location should you use to deploy VM1? To answer, select the appropriate options in the NOTE: Each correct selection is worth one point.

Answer Area

Resource group:

RG1 only
RG2 only
RG1 or RG2 only
RG1, RG2, or RG3

Location:

West US only
Central US only
Central US or West US only
East US, Central US, or West US

Answer:

Answer Area

Resource group:

RG1 only
RG2 only
RG1 or RG2 only
RG1, RG2, or RG3

Location:

West US only
Central US only
Central US or West US only
East US, Central US, or West US

200. You have an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to configure cluster autoscaler for AKS1.

Which two tools should you use? Each correct answer presents a complete solution, NOTE: Each correct selection is worth one point

- A. the set-AzAKs cmdlet
- B. the Azure portal
- C. The azaks command
- D. the kubectl command
- E. the set Azvm cmdlet

Answer: C,D

Explanation:

With cluster auto-scaling, the actual load of your worker-nodes will be monitored actively. By adding and removing worker-nodes from the cluster, it ensures that enough resources are available to keep your application healthy and responsive. In contrast, it removes worker-nodes from the AKS cluster, to optimize resource utilization and be as cost-effective as possible

Reference:

<https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler>

<https://thorsten-hans.com/aks-cluster-auto-scaler-inside-out>

201. You have an Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address.

The virtual machines host several applications that are accessible over port 443 to user on the Internet. Your on-premises network has a site-to-site VPN connection to VNet1.

You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP)

from the Internet and from the on-premises network.

You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accessed by the Internet users.

What should you do?

- A. Modify the address space of the local network gateway.
- B. Remove the public IP addresses from the virtual machines.
- C. Modify the address space of Subnet1.
- D. Create a deny rule in a network security group (NSG) that is linked to Subnet1.

Answer: D

Explanation:

You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. 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. You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your on-premises network connect by using the RDP or SSH protocol over the site-to-site VPN connection. You don't have to allow direct RDP or SSH access over the internet. And this can be achieved by configuring a deny rule in a network security group (NSG) that is linked to Subnet1 for RDP / SSH protocol coming from internet.

Modify the address space of Subnet1: Incorrect choice

Modifying the address space of Subnet1 will have no impact on RDP traffic flow to the virtual network.

Modify the address space of the local network gateway: Incorrect choice

Modifying the address space of the local network gateway will have no impact on RDP traffic flow to the virtual network.

Remove the public IP addresses from the virtual machines: Incorrect choice

If you remove the public IP addresses from the virtual machines, none of the applications be accessible publicly by the Internet users.

Reference:

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

<https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices>

202. You have an Azure subscription named Subscription1 that contains an Azure virtual network named VNet1. VNet1 connects to your on-premises network by using Azure ExpressRoute.

You need to connect VNet1 to the on-premises network by using a site-to-site VPN. The solution must minimize cost.

Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Create a local site VPN gateway.
- B. Create a VPN gateway that uses the VpnGw1 SKU.
- C. Create a VPN gateway that uses the Basic SKU.
- D. Create a gateway subnet.
- E. Create a connection.

Answer: A,B,E

Explanation:

Create a Connection: You need to link the ExpressRoute gateway to the ExpressRoute circuit. After this

step has been completed, the connection between your on-premises network and Azure through ExpressRoute will be established. Hence this is correct option.

Create a local site VPN gateway: This will allow you to provide the local gateway settings, for example public IP and the on-premises address space, so that the Azure VPN gateway can connect to it. Hence this is correct option.

Create a VPN gateway that uses the VpnGw1 SKU: The GatewaySku is only supported for VpnGw1, VpnGw2, VpnGw3, Standard, and HighPerformance VPN gateways. ExpressRoute-VPN Gateway coexist configurations are not supported on the Basic SKU. The VpnType must be RouteBased. Hence this is correct option.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-arm>

203. You have an Azure subscription that contains a virtual network named VNET1.

VNET1 contains the subnets shown in the following table.

Name	Connected virtual machines
Subnet1	VM1, VM2
Subnet2	VM3, VM4
Subnet3	VM5, VM6

Each virtual machine uses a static IP address.

You need to create network security groups (NSGs) to meet following requirements:

- Allow web requests from the internet to VM3, VM4, VM5, and VM6.
- Allow all connections between VM1 and VM2.
- Allow Remote Desktop connections to VM1.
- Prevent all other network traffic to VNET1.

What is the minimum number of NSGs you should create?

- A. 1
- B. 3
- C. 4
- D. 12

Answer: A

Explanation:

Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).

Each network security group also contains default security rules.

References:

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

204. DRAG DROP

You have an on-premises network that you plan to connect to Azure by using a site-to-site VPN.

In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16.

VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24.

You need to create a site-to-site VPN to Azure.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

- Create an Azure Content Delivery Network (CDN) profile.
- Create a VPN connection.
- Create a custom DNS server.
- Create a local gateway.
- Create a VPN gateway.
- Create a gateway subnet.

Answer Area

Answer:

Actions

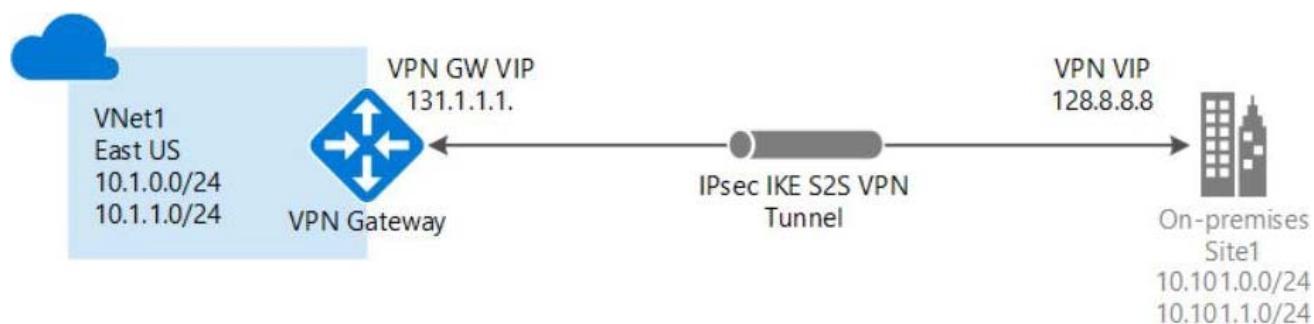
- Create an Azure Content Delivery Network (CDN) profile.
- Create a VPN connection.
- Create a custom DNS server.
- Create a local gateway.
- Create a VPN gateway.
- Create a gateway subnet.

Answer Area

Create a gateway subnet.
Create a VPN gateway.
Create a local gateway.
Create a VPN connection.

Explanation:

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it. For more information about VPN gateways, see [About VPN gateway](#).



1. Create a virtual network

You can create a VNet with the Resource Manager deployment model and the Azure portal

2. Create the gateway subnet:

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

3. Create the VPN gateway:

You create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

4. Create the local network gateway:

The local network gateway typically refers to your on-premises location. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you will create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

5. Configure your VPN device:

Site-to-Site connections to an on-premises network require a VPN device. In this step, you configure your VPN device. When configuring your VPN device, you need the following:

A shared key. This is the same shared key that you specify when creating your Site-to-Site VPN connection. In our examples, we use a basic shared key. We recommend that you generate a more complex key to use.

The Public IP address of your virtual network gateway. You can view the public IP address by using the Azure portal, PowerShell, or CLI. To find the Public IP address of your VPN gateway using the Azure portal, navigate to Virtual network gateways, then click the name of your gateway.

6. Create the VPN connection:

Create the Site-to-Site VPN connection between your virtual network gateway and your on-premises VPN device.

ference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

205.HOTSPOT

You have an Azure subscription named Subscription1 that contains the virtual networks in the following table.

Name	Subnet
VNet1	Subnet11
VNet2	Subnet12
VNet3	Subnet13

Subscription1 contains the virtual machines in the following table.

Name	IP address	Availability set
VM1	Subnet11	AS1
VM2	Subnet11	AS1
VM3	Subnet11	Not applicable
VM4	Subnet11	Not applicable
VM5	Subnet12	Not applicable
VM6	Subnet12	Not applicable

In Subscription1, you create a load balancer that has the following configurations:

- Name: LB1
- SKU: Basic
- Type: Internal
- Subnet: Subnet12

- Virtual network: VNET1

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
LB1 can balance the traffic between VM1 and VM2.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM3 and VM4.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM5 and VM6.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
LB1 can balance the traffic between VM1 and VM2.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM3 and VM4.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM5 and VM6.	<input type="radio"/>	<input type="radio"/>

Explanation:

Statement 1: Basic load balancer supports Virtual machine in a single Availability set or virtual machine scale set (VMSS) only. Hence this statement is correct.

Statement 2: Basic load balancer supports Virtual machine in a single Availability set or virtual scale set only or one standalone VM. VM3 and VM4 are not part of any availability set or VMSS .Hence this statement is incorrect.

Statement 3: Basic load balancer supports Virtual machine in a single Availability set or virtual scale set only or one standalone VM. VM5 and VM6 are not part of any availability set or VMSS .Hence this statement is incorrect.

	Standard Load Balancer	Basic Load Balancer
Backend pool size	Supports up to 1000 instances.	Supports up to 300 instances.
Backend pool endpoints	Any virtual machines or virtual machine scale sets in a single virtual network.	Virtual machines in a single availability set or virtual machine scale set.
Health probes	TCP, HTTP, HTTPS	TCP, HTTP

References: <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

206. You have a public load balancer that balances ports 80 and 443 across three virtual machines. You need to direct all the Remote Desktop Protocol (RDP) connections to VM3 only.

What should you configure?

- A. a load balancing rule
- B. a new public load balancer for VM3
- C. an inbound NAT rule
- D. a frontend IP configuration

Answer: C

Explanation: To port forward traffic to a specific port on specific VMs use an inbound network address translation (NAT) rule.

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

an inbound NAT rule:

Create a load balancer inbound network address translation (NAT) rule to forward traffic from a specific port of the front-end IP address to a specific port of a back-end VM. Hence this option is Correct
a load balancing rule: Incorrect Choice

A load balancer rule defines how traffic is distributed to the VMs. The rule defines the front-end IP configuration for incoming traffic, the back-end IP pool to receive the traffic, and the required source and destination ports.

a new public load balancer for VM3: Incorrect Choice

This option will not help you since this will route all traffic to VM3 only.

a frontend IP configuration: Incorrect Choice

When you define an Azure Load Balancer, a frontend and a backend pool configuration are connected with rules. The health probe referenced by the rule is used to determine how new flows are sent to a node in the backend pool. The frontend (aka VIP) is defined by a 3-tuple comprised of an IP address (public or internal), a transport protocol (UDP or TCP), and a port number from the load balancing rule. The backend pool is a collection of Virtual Machine IP configurations (part of the NIC resource) which reference the Load Balancer backend pool.

References:

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-port-forwarding-portal>

<https://pixelrobots.co.uk/2017/08/azure-load-balancer-for-rds/>

207. You have two subscriptions named Subscription1 and Subscription2. Each subscription is associated to a different Azure AD tenant.

Subscription1 contains a virtual network named VNet1. VNet1 contains an Azure virtual machine named VM1 and has an IP address space of 10.0.0.0/16.

Subscription2 contains a virtual network named VNet2. VNet2 contains an Azure virtual machine named VM2 and has an IP address space of 10.10.0.0/24.

You need to connect VNet1 to VNet2.

What should you do first?

- A. Move VNet1 to Subscription2.
- B. Modify the IP address space of VNet2.
- C. Provision virtual network gateways.

D. Move VM1 to Subscription2.

Answer: C

Explanation:

The virtual networks can be in the same or different regions, and from the same or different subscriptions. When connecting VNets from different subscriptions, the subscriptions do not need to be associated with the same Active Directory tenant.

Configuring a VNet-to-VNet connection is a good way to easily connect VNets. Connecting a virtual network to another virtual network using the VNet-to-VNet connection type (VNet2VNet) is similar to creating a Site-to-Site IPsec connection to an on-premises location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE, and both function the same way when communicating.

The local network gateway for each VNet treats the other VNet as a local site. This lets you specify additional address space for the local network gateway in order to route traffic.

References:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal>

208.HOTSPOT

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

Name	Connected to subnet
VM1	172.16.1.0/24
VM2	172.16.2.0/24

You add inbound security rules to a network security group (NSG) named NSG1 as shown in the following table.

Priority	Source	Destination	Protocol	Port	Action
100	172.16.1.0/24	172.16.2.0/24	TCP	Any	Allow
101	Any	172.16.2.0/24	TCP	Any	Deny

You run Azure Network Watcher as shown in the following exhibit.

Resource group *

Source type *

* Virtual machine

Destination

Select a virtual machine Specify manually

Resource group *

Virtual machine * 

Probe Settings

Protocol 

TCP ICMP

Destination port * 

Advanced settings

Check

Status

 Unreachable

Agent extension version
1.4

Source virtual machine
VM1

[Grid view](#) [Topology view](#)

Hops

NAME	IP ADDRESS	STATUS	NEXT HOP IP ADDRESS	RTT FROM SOURCE (...
VM1	172.16.1.4		172.16.2.4	-
VM2	172.16.2.4		-	-

You run Network Watcher again as shown in the following exhibit.

Source type *

* Virtual machine

Destination

 Select a virtual machine Specify manually

Resource group *

Virtual machine* 

Probe Settings

Protocol 
 TCP ICMP
Check

Status

 Reachable

Agent extension version

1.4

Source virtual machine

[VM1](#)[Grid view](#)[Topology view](#)

Hops

NAME	IP ADDRESS	STATUS	NEXT HOP IP ADDRESS	RTT FROM SOURCE (ms)
VM1	172.16.1.4		172.16.2.4	0
VM2	172.16.2.4		-	-

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**

NSG1 limits VM1 traffic

NSG1 applies to VM2

VM1 and VM2 connect to the same virtual network

Answer:

Statements	Yes	No
NSG1 limits VM1 traffic	<input type="radio"/>	<input checked="" type="radio"/>
NSG1 applies to VM2	<input checked="" type="radio"/>	<input type="radio"/>
VM1 and VM2 connect to the same virtual network	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

It limits traffic to VM2, but not VM1 traffic.

Box 2: Yes

Yes, the destination is VM2.

Box 3: No

Reference: <https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

209.HOTSPOT

You have an Azure subscription.

You create the Azure Storage account shown in the following exhibit.

The screenshot shows the Microsoft Azure 'Create storage account' wizard. At the top, there is a navigation bar with 'Microsoft Azure', a search bar, and a user profile icon. Below the navigation bar, the breadcrumb path is 'Home > Subscriptions > Subscription1 - Resources > New > Create storage account'. The main title is 'Create storage account' with a close button 'X'.

A green banner at the top indicates 'Validation passed' with a checkmark icon.

The configuration tabs are 'Basics', 'Networking', 'Advanced', 'Tags', and 'Review + create'. The 'Review + create' tab is currently selected.

Basics

Subscription	Subscription1
Resource group	RG1
Location	(Europe) North Europe
Storage account name	storage16852
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Locally-redundant storage (LRS)
Performance	Standard
Access tier (default)	Hot

Networking

Connectivity method	Private endpoint
Private Endpoint	(New) StorageEndpoint1 (blob) (privatelink.blob.core.windows.net)

Advanced

Secure transfer required	Enabled
Large file shares	Disabled
Blob soft delete	Disabled
Blob change feed	Disabled
Hierarchical namespace	Disabled
NFS v3	Disabled

At the bottom, there are buttons for 'Create' (highlighted in blue), '< Previous', and 'Next >'. Below these buttons is a link 'Download a template for automation'.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

The minimum number of copies of the storage account will be [Answer choice]

1
2
3
4

To reduce the cost of infrequently accessed data in the storage account, you must modify the [Answer choice] setting.

Access tier (default)
Performance
Account kind
Replication

Answer:

The minimum number of copies of the storage account will be [Answer choice]

1
2
3
4

To reduce the cost of infrequently accessed data in the storage account, you must modify the [Answer choice] setting.

Access tier (default)
Performance
Account kind
Replication

Explanation:

Box1: LRS will keep minimum three copies.

Box2: Changing the access tier from hot to cool will reduce the cost. In performance, standard is cheap.

In the Account kind, GPV2 is giving best price. Can be checked yourself using the pricing calculator on below link.

Reference: <https://azure.microsoft.com/en-in/pricing/calculator/?service=storage>

210.HOTSPOT

You have an Azure Active Directory (Azure AD) tenant.

You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

*** Name**

Policy1

Assignments

Users and groups

0 users and groups selected



Cloud apps

0 cloud apps selected



Conditions

0 conditions selected



Access controls

Grant
0 controls selected

Session
0 controls selected

Enables policy

On Off

Answer:

* Name

Policy1

Assignments

Users and groups
0 users and groups selected

Cloud apps
0 cloud apps selected

Conditions
0 conditions selected

Access controls



Grant
0 controls selected

Session
0 controls selected

Enables policy

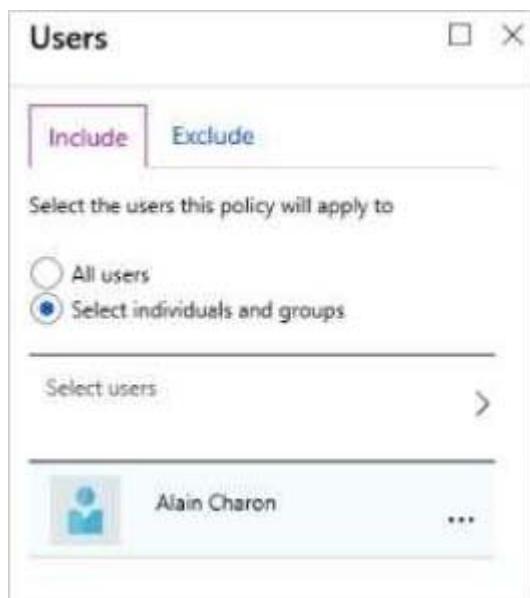
On Off

Explanation:

Box 1: Assignments, Users and Groups

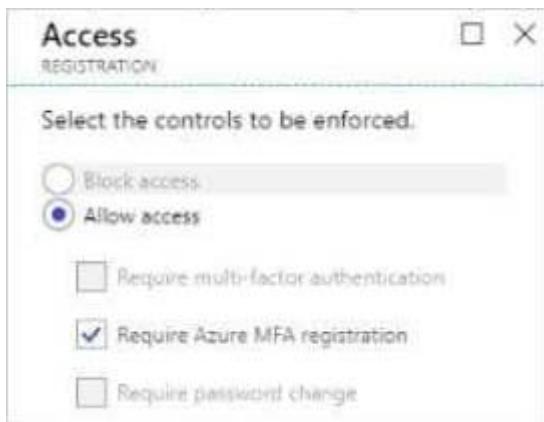
When you configure the sign-in risk policy, you need to set:

The users and groups the policy applies to: Select Individuals and Groups



Box 2:

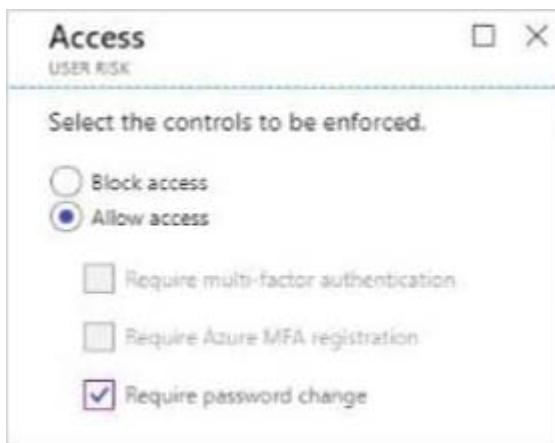
When you configure the sign-in risk policy, you need to set the type of access you want to be enforced.



Box 3:

When you configure the sign-in risk policy, you need to set:

The type of access you want to be enforced when your sign-in risk level has been met:



References:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy>

211. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From Azure Cloud Shell, you run az aks.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Installing Azure CLI doesn't mean that Azure Kubernetes client is installed. So before running kubectl client command, you have to install kubectl, the Kubernetes command-line client. First need to run az aks install-cli to install Kubernetes CLI, which is kubectl

Reference: <https://docs.microsoft.com/en-us/cli/azure/aks?view=azure-cli-latest>

212.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From the Azure CLI, you run the kubectl client.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Installing Azure CLI doesn't mean that Azure Kubernetes client is installed. So before running kubectl client command, you have install kubectl, the Kubernetes command-line client. First need to run az aks install-cli to install Kubernetes CLI, which is kubectl

Reference: <https://docs.microsoft.com/en-us/cli/azure/aks?view=azure-cli-latest>

213.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From the Azure CLI, you run azcopy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Kubectl is not installed by installing AZ CLI. As stated Azure CLI is already available but installing Azure CLI doesn't mean that Azure Kubernetes client is also installed. So before running any aks command, we have to install kubectl, the Kubernetes command-line client. az aks install-cli

Reference: <https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough#connect-to-the-cluster>

214.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2.

Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Network Interface: VM2-NIC1

Virtual network/subnet: Vnet1/Subnet11 | NIC Public IP: - | NIC Private IP: 10.240.11.5 | Accelerated networking: Disabled

Inbound port rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther443	443	Any	Any	Any	Deny
85000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
55001	AllowAzureLoadBalancerInbound	Any	Any	AcmeLoadBalancer	Any	Allow
85000	DenyAllInbound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You modify the priority of the Allow_131.107.100.50 inbound security rule.

Does this meet the goal?

A. Yes

B. No

Answer: A

215. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2.

Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Network Interface: VM2-NIC1

Virtual network/subnet: Vnet1/Subnet11 | NIC Public IP: - | NIC Private IP: 10.240.11.5 | Accelerated networking: Disabled

Inbound port rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther443	443	Any	Any	Any	Deny
85000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
55001	AllowAzureLoadBalancerInbound	Any	Any	AcmeLoadBalancer	Any	Allow
85000	DenyAllInbound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that allows any traffic from the AzureLoadBalancer source and has a cost of 150.

Does this meet the goal?

A. Yes

B. No

Answer: B

216.**Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2.

Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther443	443	Any	Any	Any	Deny
65000	AllowVmBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllVmBound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a cost of 64999.

Does this meet the goal?

A. Yes

B. No

Answer: A

217.HOTSPOT

You purchase a new Azure subscription named Subscription1.

You create a virtual machine named VM1 in Subscription1. VM1 is not protected by Azure Backup.

You need to protect VM1 by using Azure Backup. Backups must be created at 01:00 and stored for 30 days.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Location in which to store the backups:

A blob container
A file share
A Recovery Services vault
A storage account

Object to use to configure the protection for VM1:

A backup policy
A batch job
A batch schedule
A recovery plan

Answer:

Answer Area

Location in which to store the backups:

A blob container
A file share
A Recovery Services vault
A storage account

Object to use to configure the protection for VM1:

A backup policy
A batch job
A batch schedule
A recovery plan

Explanation:

Box 1: A Recovery Services vault

A Recovery Services vault is an entity that stores all the backups and recovery points you create over time.

Box 2: A backup policy

What happens when I change my backup policy?

When a new policy is applied, schedule and retention of the new policy is followed.

References:

<https://docs.microsoft.com/en-us/azure/backup/backup-configure-vault>

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-faq>

218. You have an Azure subscription that contains the resources in the following table.

Name	Type
RG1	Resource group
Store1	Azure Storage account
Sync1	Azure File Sync

Store1 contains a file share named data. Data contains 5,000 files.

You need to synchronize the files in the file share named data to an on-premises server named Server1.

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

- A. Download an automation script.
- B. Create a container instance.
- C. Create a sync group.
- D. Register Server1.
- E. Install the Azure File Sync agent on Server1.

Answer: C,D,E

Explanation:

Step 1 (E): Install the Azure File Sync agent on Server1

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share

Step 2 (D): Register Server1.

Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

Step 3 (C): Create a sync group and a cloud endpoint.

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

References: <https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

219. You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A. Azure SQL Database
- B. Azure File Storage
- C. An Azure Cosmos DB database
- D. The Azure File Sync Storage Sync Service
- E. Azure Data Factory
- F. A virtual machine

Answer: B

Explanation:

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

220. You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

A. an Azure Cosmos DB database

B. Azure File Storage

C. the Azure File Sync Storage Sync Service

D. Azure Data Factory

Answer: B

Explanation:

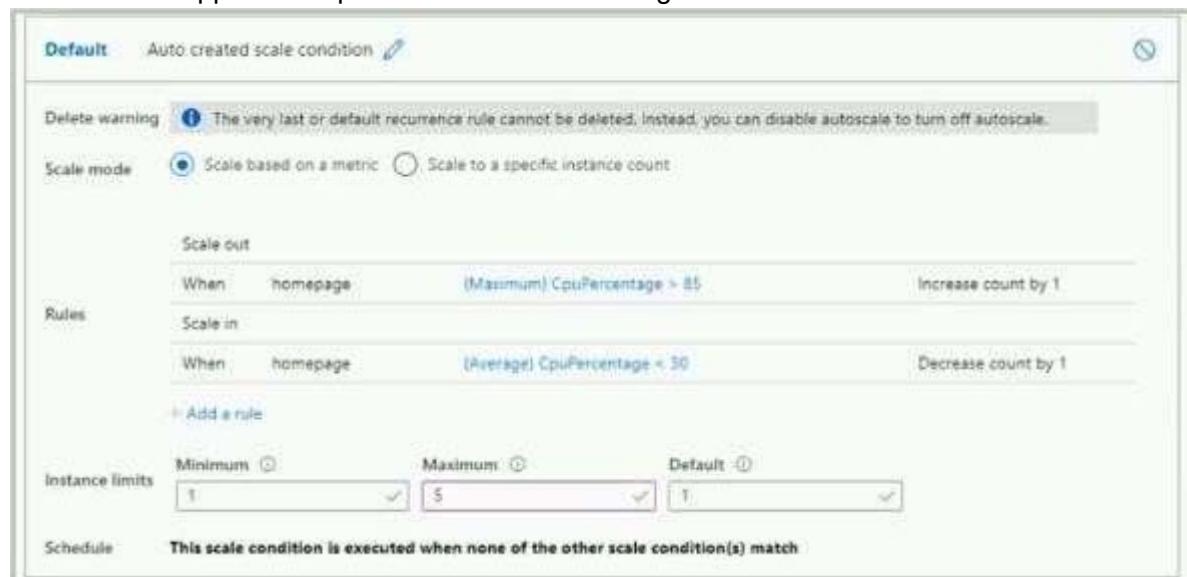
Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

The maximum size of an Azure Files Resource of a file share is 5 TB.

References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

221.HOTSPOT

You have the App Service plan shown in the following exhibit.



The screenshot shows the 'Default' scale condition configuration for an App Service plan. It includes the following settings:

- Scale mode:** Scale based on a metric (selected).
- Rules:**
 - Scale out:** When homepage, (Maximum) CpuPercentage > 85, Increase count by 1.
 - Scale in:** When homepage, (Average) CpuPercentage < 30, Decrease count by 1.
- Instance limits:** Minimum: 1, Maximum: 5, Default: 1.
- Schedule:** This scale condition is executed when none of the other scale condition(s) match.

The scale-in settings for the App Service plan are configured as shown in the following exhibit.

Operator *

Less than

Metric threshold to trigger scale action * ⓘ

30 %

Duration (in minutes) * ⓘ

5

Time grain (in mins) * ⓘ

1

Time grain statistic * ⓘ

Average

Action

Operation *

Decrease count by

Instance count *

1

Cool down (minutes) * ⓘ

5

The scale out rule is configured with the same duration and cool down time as the scale in rule. Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

If CPU usage is 70 percent for one hour and then reaches 90 percent for five minutes, the total number of instances will be [answer choice].

1
2
3
4
5

If the CPU maintains a usage of 90 percent for one hour, and then the average CPU usage is below 25 percent for nine minutes, the number of instances will be [answer choice].

1
2
3
4
5

Answer:

If CPU usage is 70 percent for one hour and then reaches 90 percent for five minutes, the total number of instances will be [answer choice].

1
2
3
4
5

If the CPU maintains a usage of 90 percent for one hour, and then the average CPU usage is below 25 percent for nine minutes, the number of instances will be [answer choice].

1
2
3
4
5

222. You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image.

You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE Each correct selection is worth one point.

- A. Modify the extension Profile section of the Azure Resource Manager template.
- B. Create a new virtual machine scale set in the Azure portal.
- C. Create an Azure policy.
- D. Create an automation account.
- E. Upload a configuration script.

Answer: A,E

Explanation:

Virtual Machine Scale Sets can be used with the Azure Desired State Configuration (DSC) extension handler. Virtual machine scale sets provide a way to deploy and manage large numbers of virtual machines, and can elastically scale in and out in response to load. DSC is used to configure the VMs as they come online so they are running the production software.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-dsc>

223. Topic 6, Misc. Questions Set C

HOTSPOT

You have an Azure subscription that contains a virtual network named VNET1 in the East US 2 region.

You have the following resources in an Azure Resource Manager template.

```
{  
  "apiVersion": "2017-03-30",  
  "type": "Microsoft.Compute/virtualMachines",  
  "name": "VM1",  
  "zones": "1",  
  "location": "EastUS2",  
  "dependsOn": [  
    "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"  
  ],  
  "properties": {  
    "hardwareProfile": {  
      "vmSize": "Standard_A2_v2"  
    },  
    "osProfile": {  
      "computerName": "VM1",  
      "adminUsername": "AzureAdmin",  
      "adminPassword": "[parameters('adminPassword')]"  
    },  
    "storageProfile": {  
      "imageReference": "[variables('image')]",  
      "osDisk": {  
        "createOption": "FromImage"  
      }  
    },  
    "networkProfile": {  
      "networkInterfaces": [  
        {  
          "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"  
        }  
      ]  
    }  
  }  
},  
{  
  "apiVersion": "2017-03-30",  
  "type": "Microsoft.Compute/virtualMachines",  
  "name": "VM2",  
  "zones": "2",  
  "location": "EastUS2",  
  "dependsOn": [  
    "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"  
  ],  
  "properties": {  
    "hardwareProfile": {  
      "vmSize": "Standard_A2_v2"  
    },  
    "osProfile": {  
      "computerName": "VM2",  
      "adminUsername": "AzureAdmin",  
      "adminPassword": "[parameters('adminPassword')]"  
    },  
    "storageProfile": {  
      "imageReference": "[variables('image')]",  
      "osDisk": {  
        "createOption": "FromImage"  
      }  
    },  
    "networkProfile": {  
      "networkInterfaces": [  
        {  
          "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"  
        }  
      ]  
    }  
  }  
}
```

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

	Yes	No
VM1 and VM2 can connect to VNET1.	<input type="radio"/>	<input type="radio"/>
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input type="radio"/>
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input type="radio"/>

Answer:

	Yes	No
VM1 and VM2 can connect to VNET1.	<input checked="" type="radio"/>	<input type="radio"/>
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	<input checked="" type="radio"/>	<input type="radio"/>
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

Box 2: Yes

VM1 is in Zone1, while VM2 is on Zone2.

Box 3: No

Reference: <https://docs.microsoft.com/en-us/azure/architecture/resiliency/recovery-loss-azure-region>

224. You have a deployment template named Template1 that is used to deploy 10 Azure web apps. You need to identify what to deploy before you deploy Template1. The solution must minimize Azure costs.

What should you identify?

- A. 10 App Service plans
- B. one Azure Traffic Manager
- C. five Azure Application Gateways
- D. one App Service plan
- E. one Azure Application Gateway

Answer: D

Explanation:

You create Azure web apps in an App Service plan.

Reference: <https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans>

225. You have an Azure subscription that contains a virtual machine named VM1. VM1 hosts a line-of-business application that is available 24 hours a day. VM1 has one network interface and one managed disk. VM1 uses the D4s v3 size.

You plan to make the following changes to VM1:

- Change the size to D8s v3.
- Add a 500-GB managed disk.
- Add the Puppet Agent extension.
- Attach an additional network interface.

Which change will cause downtime for VM1?

- A. Add a 500-GB managed disk.
- B. Attach an additional network interface.
- C. Add the Puppet Agent extension.
- D. Change the size to D8s v3.

Answer: D

Explanation:

While resizing the VM it must be in a stopped state.

References: <https://azure.microsoft.com/en-us/blog/resize-virtual-machines/>

226. You have an Azure subscription that contains 100 virtual machines.

You regularly create and delete virtual machines.

You need to identify unused disks that can be deleted.

What should you do?

- A. From Azure Advisor, modify the Advisor configuration.
- B. From Azure Cost Management view Cost Analysis.
- C. From Azure Cost Management view Advisor Recommendations.
- D. From Microsoft Azure Storage Explorer, view the Account Management properties.

Answer: D

227. You plan to create the Azure web apps shown in the following table.

Name	Runtime stack
WebApp1	.NET Core 3.0
WebApp2	ASP.NET V4.7
WebApp3	PHP 7.3
WebApp4	Ruby 2.6

What is the minimum number of App Service plans you should create for the web apps?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: D

228. You have two Azure Active Directory (Azure AD) tenants named contoso.com and fabrikam.com.

You have a Microsoft account that you use to sign in to both tenants.

You need to configure the default sign-in tenant for the Azure portal.

What should you do?

- A. From the Azure portal, configure the portal settings.
- B. From the Azure portal, change the directory.
- C. From Azure Cloud Shell, run Set-AzureRmContext.
- D. From Azure Cloud Shell, run Set-AzureRmSubscription.

Answer: B

Explanation:

The Set-AzureRmContext cmdlet sets authentication information for cmdlets that you run in the current session. The context includes tenant, subscription, and environment information.

References: <https://docs.microsoft.com/en-us/powershell/module/azurerm.profile/set-azurermcontext>

229. You have two Azure Active Directory (Azure AD) tenants named contoso.com and fabrikam.com.

You have a Microsoft account that you use to sign in to both tenants.

You need to configure the default sign-in tenant for the Azure portal.

What should you do?

- A. From the Azure portal, change the directory.
- B. From Azure Cloud Shell, run Set-AzContext.
- C. From the Azure portal, configure the portal settings.
- D. From Azure Cloud Shell, run Select- AzSubscription.

Answer: B

230. You have an Azure subscription named Subscription1 that contains an Azure virtual network named VM1. VM1 is in a resource group named RG1.

VM1 runs services that will be used to deploy resources to RG1.

You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1.

What should you do first?

- A. From the Azure portal modify the Access control (IAM) settings of VM1.
- B. From the Azure portal, modify the Policies settings of RG1.
- C. From the Azure portal, modify the value of the Managed Service Identity option for VM1.
- D. From the Azure portal, modify the Access control (IAM) settings of RG1.

Answer: C

Explanation:

A managed identity from Azure Active Directory allows your app to easily access other AAD-protected resources such as Azure Key Vault. The identity is managed by the Azure platform and does not require you to provision or rotate any secrets.

User assigned managed identities can be used on Virtual Machines and Virtual Machine Scale Sets.

References: <https://docs.microsoft.com/en-us/azure/app-service/app-service-managed-service-identity>

231.HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains three global administrators named Admin1, Admin2, and Admin3.

The tenant is associated to an Azure subscription.

Access control for the subscription is configured as shown in the Access control exhibit. (Click the Exhibit tab.)

+ Add **Remove** **Roles** **Refresh** **?** Help

Name **Type** **Role**

Scope **Group by**

5 items (4 Users, 1 Service Principals)

<input type="checkbox"/>	NAME	TYPE	ROLE	SCOPE
OWNER				
	Admin3 Admin3@contoso...	User	Owner <small>Service administrator</small>	This resource
...				

You sign in to the Azure portal as Admin1 and configure the tenant as shown in the Tenant exhibit. (Click the Exhibit tab.)

Save **Discard**

*** Name**

Country or region
United States

Location
United States datacenters

Notification language

Global admin can manage Azure Subscriptions and Management Groups

Directory ID
a8ccb916-31f3-4582-b9b7-854f413d7177 

Technical contact

Global privacy contact

Privacy statement URL

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
Admin1 can add Admin2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin3 can add Admin2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can add Admin2 as an owner of the subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can add Admin2 as an owner of the subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

They are all Global admins so they can all modify user permission. i.e add self as owner etc. You can be GA in one of the subscription, it doesn't mean that you can create the resources in all subscription. As a Global Administrator in Azure Active Directory (Azure AD), you might not have access to all subscriptions and management groups in your directory. Azure AD and Azure resources are secured independently from one another. That is, Azure AD role assignments do not grant access to Azure resources, and Azure role assignments do not grant access to Azure AD.

However, if you are a Global Administrator in Azure AD, you can assign yourself access to all Azure subscriptions and management groups in your directory

Reference:

<https://docs.microsoft.com/en-gb/azure/role-based-access-control/elevate-access-global-admin>

232.HOTSPOT

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

Name	Operating system	Subnet	Virtual network
VM1	Windows Server 2019	Subnet1	VNET1
VM2	Windows Server 2019	Subnet2	VNET1
VM3	Red Hat Enterprise Linux 7.7	Subnet3	VNET1

You configure the network interfaces of the virtual machines to use the settings shown in the following table

Name	DNS server
VM1	None
VM2	192.168.10.15
VM3	192.168.10.15

From the settings of VNET1, you configure the DNS servers shown in the following exhibit.



The virtual machines can successfully connect to the DNS server that has an IP address of 192.168.10.15 and the DNS server that has an IP address of 193.77.134.10.

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

	Yes	No
VM1 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input type="radio"/>
VM2 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input type="radio"/>
VM3 connects to 192.168.10.15 for DNS queries.	<input type="radio"/>	<input type="radio"/>

Answer:

	Yes	No
VM1 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input checked="" type="radio"/>
VM2 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 connects to 192.168.10.15 for DNS queries.	<input checked="" type="radio"/>	<input type="radio"/>

233. You have an Azure virtual machine named VM1.

The network interface for VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

Network interface: vm1175 Effective security rules Topology

Virtual network/subnet: RG5-vnet/default Public IP: 40.127.109.108 Private IP: 172.16.1.4 Accelerated networking: Disabled

APPLICATION SECURITY GROUPS

Configure the application security groups

INBOUND PORT RULES

Network security group VM1-nsg (attached to network interface: vm1175) Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
300	⚠️ RDP	3389	TCP	Any	Any	Allow	...
400	⚠️ Rule1	80	TCP	Any	Any	Deny	...
500	Rule2	80,443	TCP	Any	Any	Deny	...
1000	Rule4	50-100,400-500	UDP	Any	Any	Allow	...
2000	Rule5	50-5000	Any	Any	VirtualNetwork	Deny	...
3000	Rule6	150-300	Any	Any	Any	Allow	...
4000	Rule3	60-500	Any	Any	VirtualNetwork	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBal...	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the internet.

What should you do?

- Create a new inbound rule that allows TCP protocol 443 and configure the protocol to have a priority of 501.
- For Rule5, change the Action to Allow and change the priority to 401.
- Delete Rule1.
- Modify the protocol of Rule4.

Answer: B

Explanation:

Rule 2 is blocking HTTPS access (port 443) and has a priority of 500.

Changing Rule 5 (ports 50-5000) and giving it a lower priority number will allow access on port 443.

Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops.

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

234.HOTSPOT

You plan to use Azure Network Watcher to perform the following tasks:

- Task1: Identify a security rule that prevents a network packet from reaching an Azure virtual machine
- Task2: Validate outbound connectivity from an Azure virtual machine to an external host

Which feature should you use for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Task1:

IP flow verify
Next hop
Packet capture
Security group view
Traffic Analytics

Task2:

Connection troubleshoot
IP flow verify
Next hop
NSG flow logs
Traffic Analytics

Answer:

Task1:

IP flow verify
Next hop
Packet capture
Security group view
Traffic Analytics

Task2:

Connection troubleshoot
IP flow verify
Next hop
NSG flow logs
Traffic Analytics

Explanation:

Task 1: IP flow verify

The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which security rule allowed or denied the communication, so that you can resolve the problem.

Task 2: Connection troubleshoot

The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the

connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>
<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>
<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-connectivity-overview>

235. You have the Azure virtual networks shown in the following table.

Name	Address space	Subnet	Resource group Azure region
VNet1	10.11.0.0/16	10.11.0.0/17	West US
VNet2	10.11.0.0/17	10.11.0.0/25	West US
VNet3	10.10.0.0/22	10.10.1.0/24	East US
VNet4	192.168.16.0/22	192.168.16.0/24	North Europe

To which virtual networks can you establish a peering connection from VNet1?

- A. VNet2 and VNet3 only
- B. VNet2 only
- C. VNet3 and VNet4 only
- D. VNet2, VNet3, and VNet4

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal>

You can connect virtual networks to each other with virtual network peering. These virtual networks can be in the same region or different regions (also known as Global VNet peering). Once virtual networks are peered, resources in both virtual networks are able to communicate with each other, with the same latency and bandwidth as if the resources were in the same virtual network.

Global VNet Peering is now generally available in all Azure public regions, excluding the China, Germany, and Azure Government regions.

The address space is the most critical configuration for a VNet in Azure. This is the IP range for the entire network that will be divided into subnets. The address space can almost be any IP range that you wish (public or private). You can add multiple address spaces to a VNet. To ensure this VNet can be connected to other networks, the address space should never overlap with any other networks in your environment. If a VNet has an address space that overlaps with another Azure VNet or on-premises network, the networks cannot be connected, as the routing of traffic will not work properly.

<https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal>

<https://azure.microsoft.com/en-in/updates/general-availability-global-vnet-peering/#:~:text=Global%20VNet%20Peering%20is%20now,transit%20over%20the%20public%20internet.>

<https://www.microsoftpressstore.com/articles/article.aspx?p=2873369>

236. HOTSPOT

You have an Azure virtual machine named VM1 that connects to a virtual network named VNet1.

VM1 has the following configurations:

- Subnet: 10.0.0.0/24
- Availability set: AVSet
- Network security group (NSG): None
- Private IP address: 10.0.0.4 (dynamic)
- Public IP address: 40.90.219.6 (dynamic)

You deploy a standard, Internet-facing load balancer named slb1.

You need to configure slb1 to allow connectivity to VM1.

Which changes should you apply to VM1 as you configure slb1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Before you create a backend pool on slb1, you must:

Create and assign an NSG to VM1
Remove the public IP address from VM1
Change the private IP address of VM1 to static

Before you can connect to VM1 from slb1, you must:

Create and configure an NSG
Remove the public IP address from VM1
Change the private IP address of VM1 to static

Answer:

Before you create a backend pool on slb1, you must:

Create and assign an NSG to VM1
Remove the public IP address from VM1
Change the private IP address of VM1 to static

Before you can connect to VM1 from slb1, you must:

Create and configure an NSG
Remove the public IP address from VM1
Change the private IP address of VM1 to static

Explanation:

Box 1: Remove the public IP address from VM1

If the Public IP on VM1 is set to Dynamic, that means it is a Public IP with Basic SKU because Public IPs with Standard SKU have Static assignments by default, that cannot be changed. We cannot associate Basic SKUs IPs with Standard SKUs LBs. One cannot create a backend SLB pool if the VM to be associated has a Public IP. For Private IP it doesn't matter whether it is dynamic or static, still we can add the such VM into the SLB backend pool.

Box 2: Create and configure an NSG

Standard Load Balancer is built on the zero trust network security model at its core. Standard Load Balancer is secure by default and is part of your virtual network. The virtual network is a private and isolated network. This means Standard Load Balancers and Standard Public IP addresses are closed to inbound flows unless opened by Network Security Groups. NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource. To learn more about NSGs and how to apply them for your scenario, see Network Security Groups. Basic Load Balancer is open to the internet by default.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>
<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

237. You have an Azure subscription that contains the following storage account:

Name	Kind	Replication	Access tier	Advanced threat protection	Lock
storage1	StorageV2	Read access geo-redundant storage (RA-GRS)	Cool	On	Delete

You need to create a request to Microsoft Support to perform a live migration of storage1 to Zone Redundant Storage (ZRS) replication.

How should you modify storage1 before the live migration?

- A. Set the replication to Locally-redundant storage (IRS)
- B. Disable Advanced threat protection
- C. Remove the lock
- D. Set the access tier to Hot

Answer: A

238. You have an Azure Active Directory (Azure AD) tenant that syncs to on-premises Active Directory and contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Azure AD
User3	Member	Windows Server Active Directory
User4	Guest	Microsoft account

You create a group named Group1 and add User1 to the group. You need to configure the ownership of Group 1.

Which users can you add as owners of Group1?

- A. East US, West Europe, and North Europe
- B. East US and West Europe only
- C. East US only
- D. East US and North Europe only

Answer: C

239. HOTSPOT

You have an Azure subscription that contains the resources in the following table.

Name	Type
VM1	Virtual machine
VM2	Virtual machine
LB1	Load balancer (Basic SKU)

You install the Web Server server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1.

Statements**Yes** **No**

VM1 is in the same availability set as VM2.

If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.

If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.

Answer:**Statements****Yes** **No**

VM1 is in the same availability set as VM2.

If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.

If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.

240.HOTSPOT

VM1 is running and connects to NIC1 and Disk1. NIC1 connects to VNET1.

RG2 contains a public IP address named IP2 that is in the East US location. IP2 is not assigned to a virtual machine.

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**

You can move storage1 to RG2.

You can move NIC1 to RG2.

If you move IP2 to RG1, the location of IP2 will change.

Answer:

Answer Area

Statements	Yes	No
You can move storage1 to RG2.	<input checked="" type="radio"/>	<input type="radio"/>
You can move NIC1 to RG2.	<input type="radio"/>	<input checked="" type="radio"/>
If you move IP2 to RG1, the location of IP2 will change.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources>

<https://docs.microsoft.com/en-us/azure/virtual-network/move-across-regions-publicip-powershell>

241. You have an Azure subscription that contains a user account named User1.

You need to ensure that User1 can assign a policy to the tenant root management group.

What should you do?

- A. Assign the Global administrator role to User1, and then instruct User1 to configure access management for Azure resources.
- B. Assign the Global administrator role to User1, and then modify the default conditional access policies.
- C. Assign the Owner role to User1. and then modify the default conditional access policies.
- D. Assign the Owner role to User1. and then instruct User1 to configure access management for Azure resources.

Answer: B

242. You have an Azure subscription named Subscription1 that contains the storage accounts shown in the following table.

Name	Account kind	Azure service that contains data
storage1	Storage	File
storage2	StorageV2 (general purpose v2)	File, Table
storage3	StorageV2 (general purpose v2)	Queue
storage4	BlobStorage	Blob

You plan to use the Azure Import/Export service to export data from Subscription1.

- A. storage1
- B. storage2
- C. storage3
- D. storage4

Answer: D

Explanation:

Azure Import/Export service supports the following of storage accounts:

Azure Import/Export service supports the following storage types

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements>

243.HOTSPOT

You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit.

Policy1

Associated items

Backup schedule

* Frequency * Time * Timezone

Retention range

Retention of daily backup point

* At For
 Day(s)

Retention of weekly backup point

* On * At For
 Week(s)

Retention of monthly backup point

* On * At For
 Month(s)

Retention of yearly backup point

* In * On * At For
 Year(s)

Duplicate of Questions 35 and incomplete here..

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

Answer:

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

244. You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You join Computer2 to Azure Active Directory (Azure AD).

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

A client computer that connects to a VNet using Point-to-Site must have a client certificate installed.

References: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

245. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You delete VM1. You recreate VM1, and then you create a new network interface for VM1 and connect it to VNET2.

Does this meet the goal?

A. Yes

B. No

Answer: B

246. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You turn off VM1, and then you add a new network interface to VM1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview>

247. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You create a new network interface, and then you add the network interface to VM1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview>

248. You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1.

You have a computer named Computer1 that runs Windows 10. Computer1 is connected to the Internet.

You add a network interface named VM1173 to VM1 as shown in the exhibit. (Click the Exhibit tab.)

From Computer1, you attempt to connect to VM1 by using Remote Desktop, but the connection fails.

A. Change the priority of the RDP rule.

B. Delete the DenyAllInBound rule.

C. Start VM1.

D. Attach a network interface.

Answer: C

Explanation:

Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

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

249. You create the following resources in an Azure subscription:

- An Azure Container Registry instance named Registry1.
- An Azure Kubernetes Service (AKS) cluster named Cluster1.

You create a container image named App1 on your administrative workstation. You need to deploy App1

to Cluster1.

What should you do first?

- A. Create a host pool on Cluster1.
- B. Run the az acr build command.
- C. Run the docker build command.
- D. Run the docker push command.

Answer: B

Explanation:

Run the az acr build command: Correct Choice

az acr build command queues a quick build, providing streaming logs for an Azure Container Registry

az acr build --registry

[--agent-pool]
[--auth-mode {Default, None}]
[--build-arg]
[--file]
[--image]
[--no-format]
[--no-logs]
[--no-push]
[--no-wait]
[--platform]
[--resource-group]
[--secret-build-arg]
[--subscription]
[--target]
[--timeout]
[<SOURCE_LOCATION>]

Create a host pool on Cluster1: Incorrect Choice

Host pools are a collection of one or more identical virtual machines (VMs) within Windows Virtual Desktop environments. It won't deploy the app to the cluster. Run the docker push command : Incorrect Choice

Use docker push to share your images to the Docker Hub registry or to a self-hosted one. It won't deploy the app to the cluster.

Run the docker build command: Incorrect Choice

This command will build an image from a Dockerfile. But in the question it has been said that image file is already built and need to deploy. This command will not deploy the image.

Reference:

<https://docs.microsoft.com/en-us/cli/azure/acr?view=azure-cli-latest#az-acr-build>

<https://docs.docker.com/engine/reference/commandline/push/>

<https://docs.microsoft.com/en-us/azure/virtual-desktop/create-host-pools-azure-marketplace>

<https://docs.docker.com/engine/reference/commandline/build/>

250.DRAG DROP

You have an Azure subscription that contains a storage account.

You have an on-premises server named Server1 that runs Windows Server 2016. Server1 has 2 TB of data.

You need to transfer the data to the storage account by using the Azure Import/Export service.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order. NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions	Answer Area
Detach the external disks from Server1 and ship the disks to an Azure data center.	
From the Azure portal, update the import job.	
Attach an external disk to Server1 and then run <code>waimportexport.exe</code> .	
From the Azure portal, create an import job.	

Answer:

Actions	Answer Area
Detach the external disks from Server1 and ship the disks to an Azure data center.	Attach an external disk to Server1 and then run <code>waimportexport.exe</code> .
From the Azure portal, update the import job.	From the Azure portal, update the import job.
Attach an external disk to Server1 and then run <code>waimportexport.exe</code> .	Detach the external disks from Server1 and ship the disks to an Azure data center.
From the Azure portal, create an import job.	From the Azure portal, create an import job.

Explanation:

At a high level, an import job involves the following steps:

Step 1: Attach an external disk to Server1 and then run `waimportexport.exe`

Determine data to be imported, number of drives you need, destination blob location for your data in Azure storage.

Use the WAImportExport tool to copy data to disk drives. Encrypt the disk drives with BitLocker.

Step 2: From the Azure portal, create an import job.

Create an import job in your target storage account in Azure portal. Upload the drive journal files.

Step 3: Detach the external disks from Server1 and ship the disks to an Azure data center.

Provide the return address and carrier account number for shipping the drives back to you.

Ship the disk drives to the shipping address provided during job creation.

Step 4: From the Azure portal, update the import job

Update the delivery tracking number in the import job details and submit the import job.

The drives are received and processed at the Azure data center.

The drives are shipped using your carrier account to the return address provided in the import job.

References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

251. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.

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

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You delete VM1. You recreate VM1, and then you create a new network interface for VM1.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview>

252. You have an Azure DNS zone named adatum.com. You need to delegate a subdomain named research.adatum.com to a different DNS server in Azure.

What should you do?

A. Create an PTR record named research in the adatum.com zone.

B. Create an NS record named research in the adatum.com zone.

C. Modify the SOA record of adatum.com.

D. Create an A record named ".research" in the adatum.com zone.

Answer: B

Explanation:

You need to create a name server (NS) record for the zone.

References: <https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain>

253. Your company has a main office in London that contains 100 client computers.

Three years ago, you migrated to Azure Active Directory (Azure AD).

The company's security policy states that all personal devices and corporate-owned devices must be

registered or joined to Azure AD.

A remote user named User1 is unable to join a personal device to Azure AD from a home network.

You verify that other users can join their devices to Azure AD.

You need to ensure that User1 can join the device to Azure AD.

What should you do?

- A. From the Device settings blade, modify the Users may join devices to Azure AD setting.
- B. From the Device settings blade, modify the Maximum number of devices per user setting.
- C. Create a point-to-site VPN from the home network of User1 to Azure.
- D. Assign the User administrator role to User1.

Answer: B

Explanation:

The Maximum number of devices setting enables you to select the maximum number of devices that a user can have in Azure AD. If a user reaches this quota, they will not be able to add additional devices until one or more of the existing devices are removed.

254.CORRECT TEXT

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

You need to modify the JobTitle and UsageLocation attributes for the users.

For which users can you modify the- attributes from Azure AD? To answer, select the appropriate options in the answer area.

Answer Area

JobTitle:

UsageLocation:

Answer: see the solution below:

Explanation:

See below answer

Answer Area

JobTitle: User1 only

UsageLocation: User1 only

255.You have an Azure subscription that contains a user named User1.

You need to ensure that User1 can deploy virtual machines and manage virtual networks. The solution must use the principle of least privilege.

Which role-based access control (RBAC) role should you assign to User1?

- A. Owner

- B. Virtual Machine Administrator Login
- C. Contributor
- D. Virtual Machine Contributor

Answer: C

256. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

You need to deploy Application1 to Cluster1.

Which command should you run?

- A. az acr build
- B. az ales create
- C. kubectl apply
- D. docker build

Answer: B

257. HOTSPOT

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

RG1 contains the resources shown in the following table.

Name	Type	Location
storage1	Storage account	West US
VNET1	Virtual network	West US

Answer Area

Statements	Yes	No
You can move storage1 to RG2.	<input type="radio"/>	<input type="radio"/>
You can move NIC1 to RG2.	<input type="radio"/>	<input type="radio"/>
If you move IP2 to RG1, the location of IP2 will change.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can move storage1 to RG2.	<input checked="" type="radio"/>	<input type="radio"/>
You can move NIC1 to RG2.	<input type="radio"/>	<input checked="" type="radio"/>
If you move IP2 to RG1, the location of IP2 will change.	<input type="radio"/>	<input checked="" type="radio"/>

258. You have an Azure Active Directory (Azure AD) tenant named contosocloud.onmicrosoft.com.

Your company has a public DNS zone for contoso.com.

You add contoso.com as a custom domain name to Azure AD.

You need to ensure that Azure can verify the domain name.

Which type of DNS record should you create?

- A. NSEC
- B. PTR
- C. DNSKEY
- D. TXT

Answer: D

Explanation:

TXT: Correct Choice

You need to go to your hosting domain registrar and add in a TXT record.

Home > Fabrikam - Custom domain names > contoso.com

contoso.com X
Custom domain name

Delete

Info To use contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE TXT MX

ALIAS OR HOST NAME Save

DESTINATION OR POINTS TO ADDRESS Save

TTL Save

[Share these settings via email](#)

Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.

Verify

NSEC3: Incorrect Choice

This is Part of DNSSEC. This is used for explicit denial-of-existence of a DNS record. It is used to prove a name does not exist.

RRSIG: Incorrect Choice

This contains a cryptographic signature.

DNSKEY: Incorrect Choice

This will verify that the records are originating from an authorized sender.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#verify-your-custom-domain-name>

[https://www.cloudflare.com/dns/dnssec/how-dnssec-works/#:~:text=DNSKEY%20%2D%20Contains%20a%20public%20signing,s\)%20in%20the%20parent%20zone.](https://www.cloudflare.com/dns/dnssec/how-dnssec-works/#:~:text=DNSKEY%20%2D%20Contains%20a%20public%20signing,s)%20in%20the%20parent%20zone.)

259. You have an Azure subscription that contains a resource group named RG26.

RG26 is set to the West Europe location and is used to create temporary resources for a project.

RG26 contains the resources shown in the following table.

Name	Type	Location
VM1	Virtual machine	North Europe
RGV1	Recovery Services vault	North Europe
SQLDB01	Azure SQL database	North Europe
AZSQL01	Azure SQL database server	North Europe
sa001	Storage account	West Europe

SQLD01 is backed up to RGV1.

When the project is complete, you attempt to delete RG26 from the Azure portal. The deletion fails.

You need to delete RG26.

What should you do first?

- A. Stop the backup of SQLDB01.
- B. Delete sa001.
- C. Delete VM1.
- D. StopVM1.

Answer: A

Explanation:

You can't delete a vault that contains backup data. So in this case at first you have to delete the backup of 'SQLD01' before you attempt to delete the vault.

Reference: <https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault>

260. You have an Azure subscription named Subscription1 that contains a virtual network named VNet1.

VNet1 is in a resource group named RG1.

Subscription1 has a user named User1.

User1 has the following roles;

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Assign User1 the Contributor role for VNet1.
- B. Remove User from the Security Reader and Reader roles tot Subscription1.
- C. Assign User1 the Network Contributor role for VNet1.
- D. Assign User1 the User Access Administrator role for VNet1

Answer: D

Explanation:

The User Access Administrator role allows you to manage user access to Azure resources.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>

261. You deploy an Azure Kubernetes Service (AKS) cluster named Cluster1 that uses the IP addresses shown in the following table.

IP address	Assigned to
131.107.2.1	Load balancer front end
192.168.10.2	Kubernetes DNS service
172.17.7.1	Docker bridge address
10.0.10.11	Kubernetes cluster node

You need to provide internet users with access to the applications that run in Cluster1.

Which IP address should you include in the DNS record for Ousted?

- A. 172.17.7.1
- B. 131.107.2.1
- C. 192.168.10.2
- D. 10.0.10.11

Answer: B

Explanation:

When any internet user will try to access the cluster which is behind a load balancer, traffic will first hit to load balancer front end IP. So in the DNS configuration you have to provide the IP address of the load balancer.

Reference: <https://stackoverflow.com/questions/43660490/giving-a-dns-name-to-azure-load-balancer>

262. You need to deploy an Azure virtual machine scale set that contains five instances as quickly as possible.

What should you do?

- A. Deploy five virtual machines. Modify the Size setting for each virtual machine.
- B. Deploy live virtual machines. Modify the Availability Zones setting for each virtual machine.
- C. Deploy one virtual machine scale set that is set to ScaleSetVM orchestration mode.
- D. Deploy one virtual machine scale set that is set to VM (virtual machines) orchestration mode.

Answer: B

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/orchestration-modes>

263. HOTSPOT

You have an Azure subscription named Subscription1 that contains the quotas shown in the following table.

Quota	Location	Usage
Standard B5 Family vCPUs	West US	0 of 20
Standard D Family vCPUs	West US	0 of 20
Total Regional vCPUs	West US	0 of 20

You deploy virtual machines to Subscription1 as shown in the following table.

Name	Size	vCPUs	Location	Status
VM1	Standard_B2ms	2	West US	Running

Answer Area

Statements	Yes	No
You can deploy VM3 to West US.	<input type="radio"/>	<input type="radio"/>
You can deploy VM4 to West US.	<input type="radio"/>	<input type="radio"/>
You can deploy VM5 to West US.	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area**

Statements	Yes	No
You can deploy VM3 to West US.	<input type="radio"/>	<input checked="" type="radio"/>
You can deploy VM4 to West US.	<input type="radio"/>	<input checked="" type="radio"/>
You can deploy VM5 to West US.	<input type="radio"/>	<input checked="" type="radio"/>

264. You have an Azure subscription that contains the resources in the following table.

Name	Type	Azure region	Resource group
VNet1	Virtual network	West US	RG2
VNet2	Virtual network	West US	RG1
VNet3	Virtual network	East US	RG1
NSG1	Network security group (NSG)	East US	RG2

To which subnets can you apply NSG1?

- A. the subnets on VNet1 only
- B. the subnets on VNet2 only
- C. the subnets on VNet3 only
- D. the subnets on VNet2, VNet2, and VNet3
- E. the subnets on VNet2 and VNet3 only

Answer: C**Explanation:**

All Azure resources are created in an Azure region and subscription. A resource can only be created in a virtual network that exists in the same region and subscription as the resource.

References: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm>

265. HOTSPOT

You have an Azure subscription.

The subscription contains virtual machines that run Windows Server 2016 and are configured as shown in the following table.

Name	Virtual network	DNS suffix configured in Windows Server
VM1	VNET2	Contoso.com
VM2	VNET2	None
VM3	VNET2	Adatum.com

Answer Area

- | Statements | Yes | No |
|---|-----------------------|-----------------------|
| When VM1 starts, a record for VM1 is added to the contoso.com DNS zone. | <input type="radio"/> | <input type="radio"/> |
| When VM2 starts, a record for VM2 is added to the contoso.com DNS zone. | <input type="radio"/> | <input type="radio"/> |
| When VM3 starts, a record for VM3 is added to the adatum.com DNS zone. | <input type="radio"/> | <input type="radio"/> |

Answer:**Answer Area**

- | Statements | Yes | No |
|---|-------------------------------------|-------------------------------------|
| When VM1 starts, a record for VM1 is added to the contoso.com DNS zone. | <input checked="" type="checkbox"/> | <input type="radio"/> |
| When VM2 starts, a record for VM2 is added to the contoso.com DNS zone. | <input type="radio"/> | <input checked="" type="checkbox"/> |
| When VM3 starts, a record for VM3 is added to the adatum.com DNS zone. | <input checked="" type="checkbox"/> | <input type="radio"/> |

266.HOTSPOT

You have an on-premises data center and an Azure subscription. The data center contains two VPN devices. The subscription contains an Azure virtual network named VNet1. VNet1 contains a gateway subnet.

You need to create a site-to-site VPN. The solution must ensure that if a single instance of an Azure VPN gateway fails, or a single on-premises VPN device fails, the failure will not cause an interruption that is longer than two minutes.

What is the minimum number of public IP addresses, virtual network gateways, and local network gateways required in Azure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Public IP addresses:

1
2
3
4

Virtual network gateways:

1
2
3
4

Local network gateways:

1
2
3
4

Answer:

Public IP addresses:

1
2
3
4

Virtual network gateways:

1
2
3
4

Local network gateways:

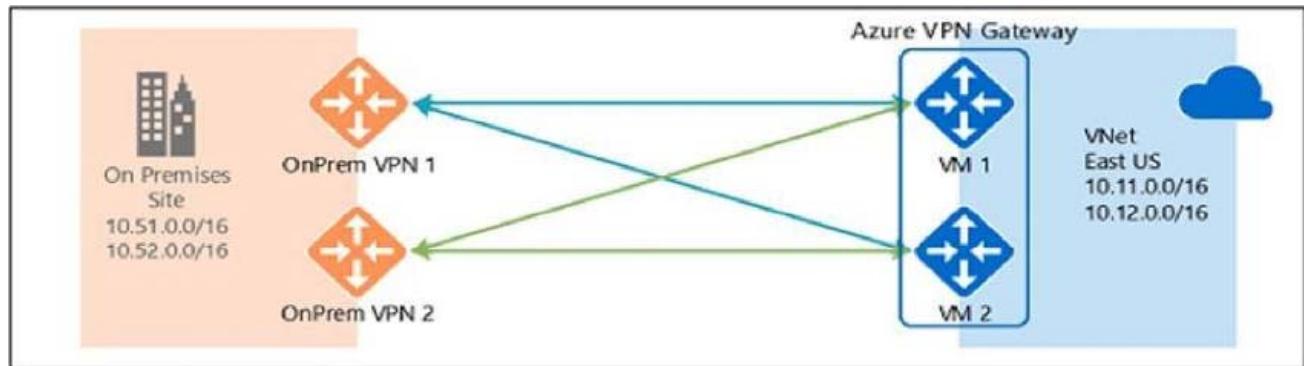
1
2
3
4

Explanation:

Box 1: 4

Two public IP addresses in the on-premises data center, and two public IP addresses in the VNET.

The most reliable option is to combine the active-active gateways on both your network and Azure, as shown in the diagram below.



Box 2: 2

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the S2S VPN or VNet-to-VNet connections.

Box 3: 2

Dual-redundancy: active-active VPN gateways for both Azure and on-premises networks

Reference: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable>

267. You have an Azure subscription named Subscription 1 that contains two Azure virtual networks named VNet1 and VNet2. VNet1 contains a VPN gateway named VPNGW1 that uses static routing.

There is a site-to-site VPN connection between your on-premises network and VNet1.

On a computer named Client1 that runs Windows 10, you configure a point to site VPN connection to VNet1.

You configure virtual network peering between VNet1 and VNet2. You verify that you can connect to VNet2 from the on-premises network. Client1 is unable to connect to VNet2.

You need to ensure that you can connect Client1 to VNet2.

What should you do?

- A. Select Allow gateway transit on VNet2.
- B. Select Allow gateway transit on VNet1.
- C. Download and re-install the VPN client configuration package on Client1.
- D. Enable BGP on VPNGW1

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

268. You have an Azure subscription named Subscription1.

Subscription1 contains the resource groups in the following table.

Name	Azure region	Policy
RG1	West Europe	Policy1
RG2	North Europe	Policy2
RG3	France Central	Policy3

RG1 has a web app named WebApp1. WebApp1 is located in West Europe.

You move WebApp1 to RG2.

What is the effect of the move?

- A. The App Service plan to WebApp1 moves to North Europe. Policy2 applies to WebApp1.
- B. The App Service plan to WebApp1 moves to North Europe. Policy1 applies to WebApp1.
- C. The App Service plan to WebApp1 remains to West Europe. Policy2 applies to WebApp1.
- D. The App Service plan to WebApp1 remains to West Europe. Policy1 applies to WebApp1.

Answer: C

Explanation:

You can move an app to another App Service plan, as long as the source plan and the target plan are in the same resource group and geographical region.

The region in which your app runs is the region of the App Service plan it's in. However, you cannot change an App Service plan's region.

References: <https://docs.microsoft.com/en-us/azure/app-service/app-service-plan-manage>

269. You have an Azure subscription that contains a resource group named RG1. RG1 contains 100 virtual machines.

Your company has three cost centers named Manufacturing, Sales, and Finance.

You need to associate each virtual machine to a specific cost center.

What should you do?

- A. Add an extension to the virtual machines.
- B. Modify the inventory settings of the virtual machine.
- C. Assign tags to the virtual machines.
- D. Configure locks for the virtual machine.

Answer: C

Explanation:

You apply tags to your Azure resources, resource groups, and subscriptions to logically organize them into a taxonomy. Each tag consists of a name and a value pair. For example, you can apply the name "Environment" and the value "Production" to all the resources in production

References:

<https://docs.microsoft.com/en-us/azure/billing/billing-getting-started>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>

270. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the Subscriptions blade, you select the subscription, and then click Resource providers.

Does this meet the goal?

- A. Yes

B. No

Answer: B

Explanation:

Through activity logs, you can determine:

§ what operations were taken on the resources in your subscription

§ who started the operation

§ when the operation occurred

§ the status of the operation

§ the values of other properties that might help you research the operation

1. On the Azure portal menu, select Monitor, or search for and select Monitor from any page

2. Select Activity Log.

3. You see a summary of recent operations. A default set of filters is applied to the operations. Notice the information on the summary includes who started the action and when it happened.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
▶ List Storage Account Keys	Succeeded	3 h ago	Tue Jan 22 2...	Third Internal Consumption	example@microsoft.com
▶ AuditIfNotExists	Succeeded	3 h ago	Tue Jan 22 2...	Third Internal Consumption	Microsoft Azure Policy Insig...
▶ AuditIfNotExists	Succeeded	3 h ago	Tue Jan 22 2...	Third Internal Consumption	Microsoft Azure Policy Insig...

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs>

271.HOTSPOT

You have an Azure subscription named Subscription1 that has a subscription ID of c276fc76-9cd4-44c9-99a7-4fd71546436e.

You need to create a custom RBAC role named CR1 that meets the following requirements:

- Can be assigned only to the resource groups in Subscription1
- Prevents the management of the access permissions for the resource groups
- Allows the viewing, creating, modifying, and deleting of resource within the resource groups

What should you specify in the assignable scopes and the permission elements of the definition of CR1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```
assigneesScopes : [
```

```
"/"
```

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"
```

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups"
```

```
],
```

```
"permissions": [
```

```
{
```

```
  "actions": [
```

```
  "*/"
```

```
  ],
```

```
  "additionalProperties" : {},
```

```
  "dataActions": [],
```

```
  "notActions" : [
```

```
  "Microsoft.Authorization/*"
```

```
  "Microsoft.Resources/*"
```

```
  "Microsoft.Security/*"
```

```
  ],
```

```
  "notDataActions": []
```

```
}
```

```
1
```

Answer:

```

"assignableScopes": [
  "/",
  "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e",
  "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups"
],
"permissions": [
  {
    "actions": [
      "*"
    ],
    "additionalProperties" : {},
    "dataActions": [],
    "notActions" : [
      "Microsoft.Authorization/*"
    ],
    "notDataActions": []
  }
]

```

Explanation:

Box 1: "/subscription/c276fc76-9cd4-44c9-99a7-4fd71546436e"

Box 2: "Microsoft.Authorization/*"

Box 1: "/subscription/c276fc76-9cd4-44c9-99a7-4fd71546436e"

In the assignableScopes you need to mention the subscription ID where you want to implement the RBAC

Box 2: "Microsoft.Authorization/*" Microsoft.Authorization/* is used to Manage authorization

References:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsof> tresources

272.HOTSPOT

You have an Azure subscription named Subscription1.

You plan to deploy an Ubuntu Server virtual machine named VM1 to Subscription1.

You need to perform a custom deployment of the virtual machine. A specific trusted root certification authority (CA) must be added during the deployment.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

File to create:

Answer.ini
Autounattend.conf
Cloud-init.txt
Unattend.xml

Tool to use to deploy the virtual machine:

The az vm create command
The Azure portal
The New-AzureRmVM cmdlet

Answer:

Answer Area

File to create:

Answer.ini
Autounattend.conf
Cloud-init.txt
Unattend.xml

Tool to use to deploy the virtual machine:

The az vm create command
The Azure portal
The New-AzureRmVM cmdlet

Explanation:

Box 1: Cloud-init.txt

Cloud-init.txt is used to customize a Linux VM on first boot up. It can be used to install packages and write files, or to configure users and security. No additional steps or agents are required to apply your configuration.

Box 2: The az vm create command

Once Cloud-init.txt has been created, you can deploy the VM with az vm create cmdlet, sing the --customdata parameter to provide the full path to the cloud-init.txt file.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-automate-vm-deployment>

273.DRAG DROP

You have an Azure subscription that is used by four departments in your company. The subscription contains 10 resource groups. Each department uses resources in several resource groups.

You need to send a report to the finance department. The report must detail the costs for each

department.

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

- Assign a tag to each resource group.
- Open the **Resource costs** blade of each resource group.
- Download the usage report.
- Assign a tag to each resource.
- From the Cost analysis blade, filter the view by tag.

Answer Area

Answer:

Actions

- Assign a tag to each resource group.
- Open the **Resource costs** blade of each resource group.
- Download the usage report.
- Assign a tag to each resource.
- From the Cost analysis blade, filter the view by tag.

Answer Area

Assign a tag to each resource.	
From the Cost analysis blade, filter the view by tag.	
Download the usage report.	

Explanation:

Box 1: Assign a tag to each resource.

You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy. After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Each resource or resource group can have a maximum of 15 tag name/value pairs. Tags applied to the resource group are not inherited by the resources in that resource group.

Box 2: From the Cost analysis blade, filter the view by tag

After you get your services running, regularly check how much they're costing you. You can see the current spend and burn rate in Azure portal.

Box 3: Download the usage report

References:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>

<https://docs.microsoft.com/en-us/azure/billing/billing-getting-started>

274. You have a resource group named RG1. RG1 contains an Azure Storage account named storageaccount1 and a virtual machine named VM1 that runs Windows Server 2016. Storageaccount1 contains the disk files for VM1. You apply a **ReadOnly** lock to RG1.

What can you do from the Azure portal?

- A. Generate an automation script for RG1.
- B. View the keys of storageaccount1.
- C. Upload a blob to storageaccount1.
- D. Start VM1.

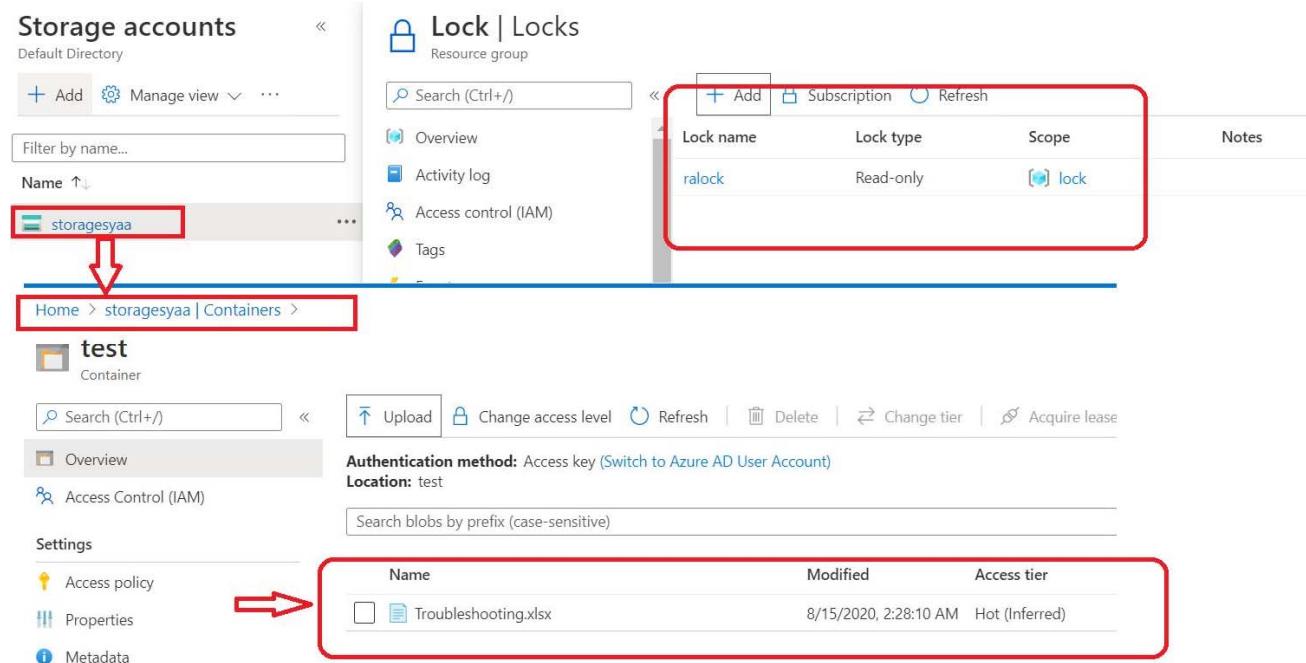
Answer: C

Explanation:

Applying locks can lead to unexpected results because some operations that don't seem to modify the resource actually require actions that are blocked by the lock. Locks are inherited to all of its resources if it applies on resource group level.

Upload a blob to storageaccount1 is possible if we have readonly lock on RG1 since we are trying to modify the data not resource properties.

When a R/O lock is put on a resource, you lock its properties not the resource. So while a read only lock is present on a storage account(inherited from a resource group), a file can still be uploaded to the already existing container of a storage account.



The screenshot shows the Azure portal interface with the following sections:

- Storage accounts:** A list of storage accounts, with "storagesyaa" selected. A red box highlights "storagesyaa" and an arrow points to the "Containers" link in the breadcrumb navigation.
- Lock | Locks:** A table showing a lock named "ralock" with a "Read-only" type and a scope of "lock". A red box highlights this table.
- Containers:** A list of blobs in the "test" container. A red box highlights the table, and an arrow points to the "Troubleshooting.xlsx" blob.

275. You have an Azure subscription.

You have 100 Azure virtual machines.

You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.

Which blade should you use?

- A. Metrics
- B. Customer insights
- C. Monitor
- D. Advisor

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations>

<https://docs.microsoft.com/bs-latn-ba/azure/cost-management/tutorial-acm-opt-recommendations>

Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.

276. HOTSPOT

You have an Azure subscription.

You need to implement a custom policy that meet the following requirements:

- * Ensures that each new resource group in the subscription has a tag named organization set to a value of Contoso.

- * Ensures that resource group can be created from the Azure portal.

- * Ensures that compliance reports in the Azure portal are accurate.

How should you complete the policy? To answer, select the appropriate options in the answers area.

```
{
  "policyRule": {
    "if": {
      "allOf": [
        {
          "field": "type",
          "equals": "
```

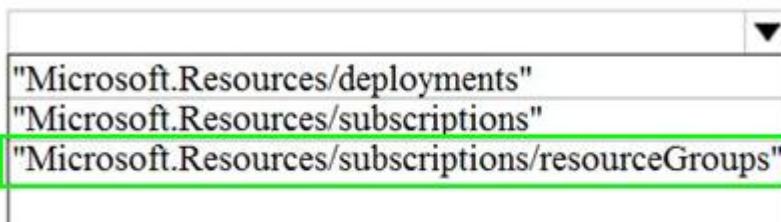
"Microsoft.Resources/deployments"	▼
"Microsoft.Resources/subscriptions"	▼
"Microsoft.Resources/subscriptions/resourceGroups"	▼

```
},
{
  "not": {
    "field": "tags['organization']",
    "equals": "Contoso"
  }
}
]
```

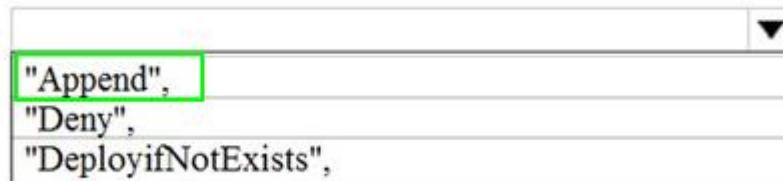
```
},
  "then": {
    "effect": "Append",
    "details": [
      "Deny",
      "DeployifNotExists",
      "field": "tags['organization']",
      "value": "Contoso"
    ]
  }
}
```

Answer:

```
{
  "policyRule": {
    "if": {
      "allOf": [
        {
          "field": "type",
          "equals": "
```



```
},
  {
    "not": {
      "field": "tags['organization']",
      "equals": "Contoso"
    }
  }
],
},
"then": {
  "effect": "Append",
  "details": [
    "Deny",
    "DeployIfExists",
    "field": "tags['organization']",
    "value": "Contoso"
  ]
}
}
}
```



Explanation:

Box 1: "Microsoft.Resources/subscriptions/resourceGroups"

To create a new resource group in a subscription, account have at least the this permission.

Box 2: "Append"

Append adds fields to the resource when the if condition of the policy rule is met. If the append effect would override a value in the original request with a different value, then it acts as a deny effect and rejects the request. To append a new value to an existing array, use the [*] version of the alias

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

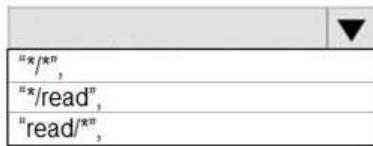
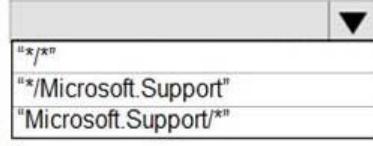
<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

277.HOTSPOT

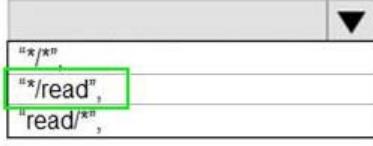
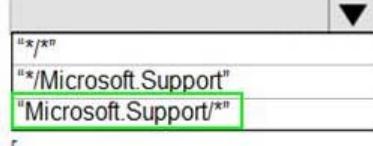
You plan to create a new Azure Active Directory (Azure AD) role.

You need to ensure that the new role can view all the resources in the Azure subscription and issue support requests to Microsoft. The solution must use the principle of least privilege.

How should you complete the JSON definition? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Subscription reader and support request and support request creator.",
  "Actions": [
    
    
  ],
  "NotActions": [
  ],
  "AssignableScopes": [
    "/subscriptions/11111111-1111-1111-1111-111111111111"
  ]
}
```

Answer:

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Subscription reader and support request and support request creator.",
  "Actions": [
    
    
  ],
  "NotActions": [
  ],
  "AssignableScopes": [
    "/subscriptions/11111111-1111-1111-1111-111111111111"
  ]
}
```

Explanation:

Box 1: `/*/read`,

`/*/read` lets you view everything, but not make any changes.

Box 2: `Microsoft.Support/*`

The action `Microsoft.Support/*` enables creating and management of support tickets.

References:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell>
<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

278.HOTSPOT

You plan to deploy 20 Azure virtual machines by using an Azure Resource Manager template. The virtual machines will run the latest version of Windows Server 2016 Datacenter by using an Azure Marketplace image.

You need to complete the storageProfile section of the template.

How should you complete the storageProfile section? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```
"storageProfile": {
    "imageReference": {
        "publisher": "MicrosoftWindowsServer",
        "offer": [
            "2016-Datacenter",
            "WindowsClient",
            "Windows-Hub",
            "WindowsServer",
            "WindowsServerEssentials",
            "WindowsServerSemiAnnual",
        ],
        "sku": [
            "2016-Datacenter",
            "WindowsClient",
            "Windows-Hub",
            "WindowsServer",
            "WindowsServerEssentials",
            "WindowsServerSemiAnnual",
        ],
        "version": "latest"
    }
}
```

Answer:

```

"storageProfile": {
    "imageReference": {
        "publisher": "MicrosoftWindowsServer",
        "offer": [
            "2016-Datacenter",
            "WindowsClient",
            "Windows-Hub",
            "WindowsServer", WindowsServer,
            "WindowsServerEssentials",
            "WindowsServerSemiAnnual",
        ],
        "sku": [
            "2016-Datacenter", 2016-Datacenter,
            "WindowsClient",
            "Windows-Hub",
            "WindowsServer",
            "WindowsServerEssentials",
            "WindowsServerSemiAnnual",
        ],
        "version": "latest"
    }
}
...

```

Explanation:

```

...
"storageProfile": {
    "imageReference": {
        "publisher": "MicrosoftWindowsServer",
        "offer": "WindowsServer",
        "sku": "2016-Datacenter",
        "version": "latest"
    },
...

```

References: <https://docs.microsoft.com/en-us/rest/api/compute/virtualmachines/createorupdate>

279.HOTSPOT

You need to deploy two Azure web apps named WebApp1 and WebApp2.

The web apps have the following requirements:

- WebApp1 must be able to use staging slots
- WebApp2 must be able to access the resources located on an Azure virtual network

What is the least costly plan that you can use to deploy each web app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

WebApp1:	
	D1–Dev/Test F1–Dev/Test I1– Production P3 – Production S1 – Production

WebApp2:	
	D1–Dev/Test F1–Dev/Test I1– Production P3 – Production S1 – Production

Answer:

WebApp1:	
	D1–Dev/Test F1–Dev/Test I1– Production P3 – Production S1 – Production

WebApp2:	
	D1–Dev/Test F1–Dev/Test I1– Production P3 – Production S1 – Production

Explanation:

References:

<https://azure.microsoft.com/en-au/pricing/details/app-service/windows/>

<https://azure.microsoft.com/en-gb/pricing/details/app-service/plans/>

280.HOTSPOT

You have an Azure subscription named Subscription1.

You have a virtualization environment that contains the virtualization server in the following table.

Name	Hypervisor	Run virtual machine
Server1	Hyper-V	VM1, VM2, VM3
Server2	VMWare	VMA, VMB, VMC

The virtual machines are configured as shown on the following table.

Name	Generation	Memory	Operating System (OS) disk	Data disk	OS
VM1	1	4 GB	200 GB	800 GB	Windows Server 2012 R2
VM2	1	12 GB	12 GB	200 GB	Red Hat Enterprise Linux 7.2
VM3	2	32 GB	100 GB	1 TB	Windows Server 2016
VMA	<i>Not applicable</i>	8 GB	100 GB	2 TB	Windows Server 2012 R2
VMB	<i>Not applicable</i>	16 GB	150 GB	1 TB	Red Hat Enterprise Linux 7.2
VMC	<i>Not applicable</i>	24 GB	500 GB	6 TB	Windows Server 2016

All the virtual machines use basic disks. VM1 is protected by using BitLocker Drive Encryption (BitLocker). You plan to use Azure Site Recovery to migrate the virtual machines to Azure.

Which virtual machines can you migrate? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Virtual machines that can be migrated from Server1.

VM1 only
VM2 only
VM3 only
VM1 and VM2 only
VM1 and VM3 only
VM1, VM2, and VM3

Virtual machines that can be migrated from Server2.

VMA only
VMB only
VMC only
VMA and VMB only
VMA and VMC only
VMA, VMB, and VMC

Answer:

Virtual machines that can be migrated from Server1.

VM1 only
VM2 only
VM3 only
VM1 and VM2 only
VM1 and VM3 only
VM1, VM2, and VM3

Virtual machines that can be migrated from Server2.

VMA only
VMB only
VMC only
VMA and VMB only
VMA and VMC only
VMA, VMB, and VMC

Explanation:

Not VM1 because it has BitLocker enabled.

Not VM2 because the OS disk is larger than 2TB.

Not VMC because the Data disk is larger than 4TB.

References:

<https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix#azure-vm-requirements>

281.HOTSPOT

You have an Azure web app named WebApp1 that runs in an Azure App Service plan named ASP1.

ASP1 is based on the D1 pricing tier.

You need to ensure that WebApp1 can be accessed only from computers on your on-premises network.

The solution must minimize costs.

What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Pricing tier for ASP1:

B1
P1v2
S1

Settings for WebApp1:

Cross-origin resource sharing(CORS)
Networking
SSL

Answer:

Pricing tier for ASP1:

B1
P1v2
S1

Settings for WebApp1:

Cross-origin resource sharing(CORS)
Networking
SSL

Explanation:

Box 1: B1

B1 (Basic) would minimize cost compared P1v2 (premium) and S1 (standard).

Box 2: Cross Origin Resource Sharing (CORS)

Once you set the CORS rules for the service, then a properly authenticated request made against the service from a different domain will be evaluated to determine whether it is allowed according to the rules you have specified.

Note: CORS (Cross Origin Resource Sharing) is an HTTP feature that enables a web application running under one domain to access resources in another domain. In order to reduce the possibility of cross-site scripting attacks, all modern web browsers implement a security restriction known as same-origin policy. This prevents a web page from calling APIs in a different domain. CORS provides a secure way to allow one origin (the origin domain) to call APIs in another origin.

References:

<https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

<https://docs.microsoft.com/en-us/azure/cdn/cdn-cors>

282.DRAG DROP

You have an on-premises network that includes a Microsoft SQL Server instance named SQL1.

You create an Azure Logic App named App1.

You need to ensure that App1 can query a database on SQL1.

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
From the Azure portal, create an on-premises data gateway.	
From an on-premises computer, install an on-premises data gateway.	
Create an Azure virtual machine that runs Windows Server 2016.	
From an Azure virtual machine, install an on-premises data gateway.	
From the Logic Apps Designer in the Azure portal, add a connector.	

Answer:

Actions	Answer Area
From the Azure portal, create an on-premises data gateway.	From an on-premises computer, install an on-premises data gateway.
From an on-premises computer, install an on-premises data gateway.	From the Azure portal, create an on-premises data gateway.
Create an Azure virtual machine that runs Windows Server 2016.	From the Logic Apps Designer in the Azure portal, add a connector.
From an Azure virtual machine, install an on-premises data gateway.	
From the Logic Apps Designer in the Azure portal, add a connector.	

Explanation:

To access data sources on premises from your logic apps, you can create a data gateway resource in Azure so that your logic apps can use the on-premises connectors.

Box 1: From an on-premises computer, install an on-premises data gateway.

Before you can connect to on-premises data sources from Azure Logic Apps, download and install the on-premises data gateway on a local computer.

Box 2: From the Azure portal, create an on-premises data gateway Create Azure resource for gateway
After you install the gateway on a local computer, you can then create an Azure resource for your gateway. This step also associates your gateway resource with your Azure subscription.

Box 3: From the Logic Apps Designer in the Azure portal, add a connector

After you create your gateway resource and associate your Azure subscription with this resource, you can now create a connection between your logic app and your on-premises data source by using the gateway. References: <https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-connection>

283. You are the global administrator for an Azure Active Directory (Azure AD) tenant named adatum.com.

You need to enable two-step verification for Azure users.

What should you do?

- A. Create a sign-in risk policy in Azure AD Identity Protection
- B. Enable Azure AD Privileged Identity Management.
- C. Create and configure the Identity Hub.
- D. Configure a security policy in Azure Security Center.

Answer: A

Explanation:

Identity Protection analyzes signals from each sign-in, both real-time and offline, and calculates a risk score based on the probability that the sign-in wasn't performed by the user. Administrators can make a decision based on this risk score signal to enforce organizational requirements.

Administrators can choose to block access, allow access, or allow access but require multi-factor authentication.

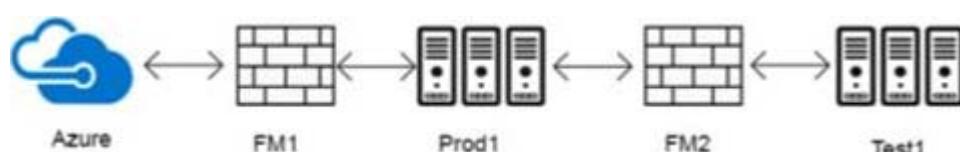
If risk is detected, users can perform multi-factor authentication to self-remediate and close the risky sign-in event to prevent unnecessary noise for administrators.

With Azure Active Directory Identity Protection, you can:

References: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/flows>

284. DRAG DROP

Your network is configured as shown in the following exhibit.



The firewalls are configured as shown in the following table.

Allowed port name	Inbound (TCP)	Outbound (TCP)
FW1	993, 3389	80, 993
FM2	443, 995, 3389	80, 995

Prod1 contains a vCenter server.

You install an Azure Migrate Collector on Test1.

You need to discover the virtual machines.

Which TCP port should be allowed on each firewall? To answer, drag the appropriate ports to the correct firewalls. Each port 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.

TCP Ports**Answer Area**

Inbound 80

FW1:

Inbound 995

FW2:

Outbound 3389

Outbound 443

Answer:

TCP Ports**Answer Area**

Inbound 80

FW1: Outbound 443

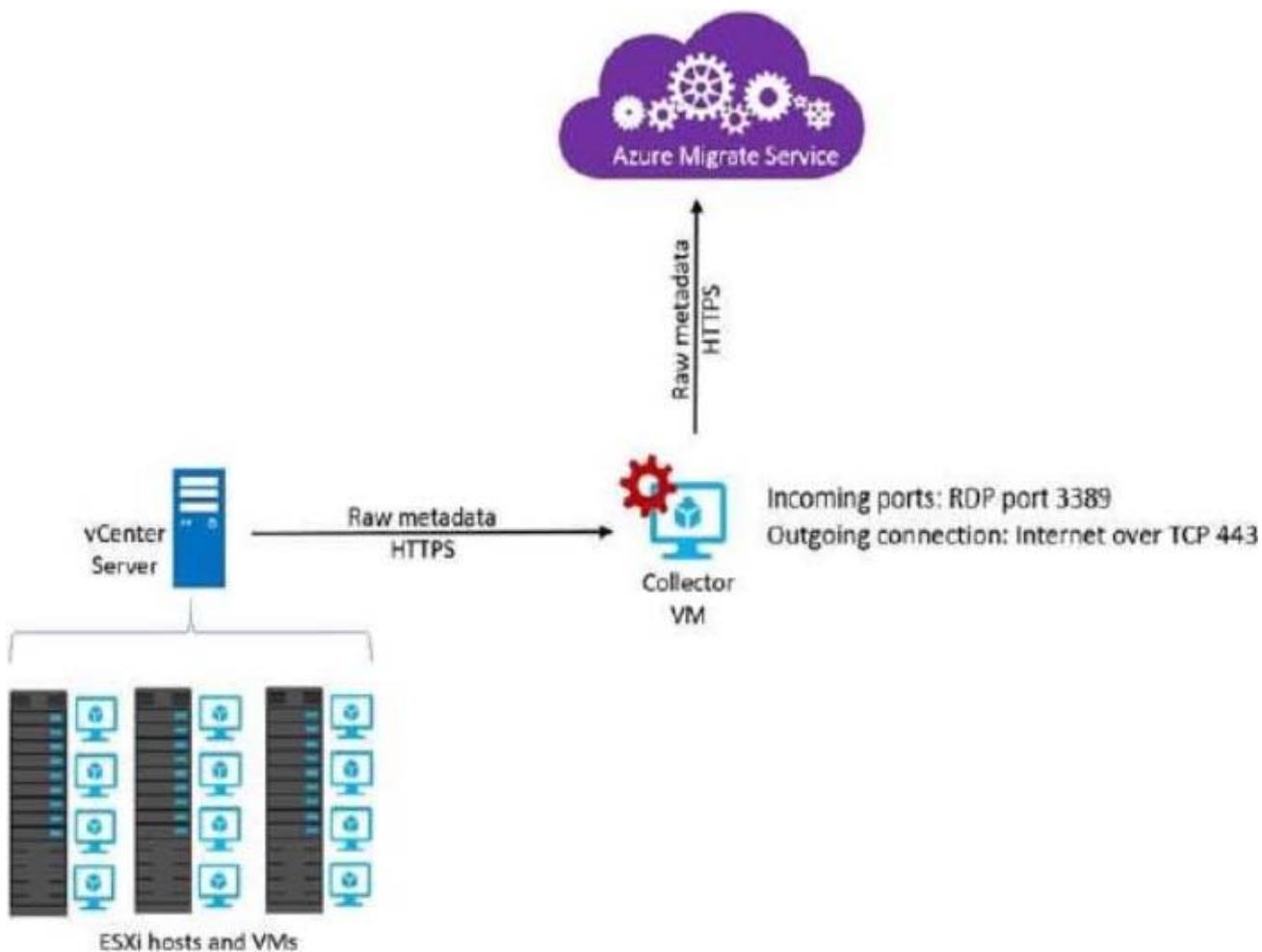
Inbound 995

FW2: Outbound 443

Outbound 3389

Outbound 443

Explanation:



References:

<https://docs.microsoft.com/en-us/azure/migrate/concepts-collector>

<https://docs.microsoft.com/en-us/azure/migrate/migrate-appliance>

285. You plan to move services from your on-premises network to Azure.

You identify several virtual machines that you believe can be hosted in Azure.

The virtual machines are shown in the following table.

Name	Role	Operating system (OS)	Environment
Sea-DC01	Domain controller	Windows Server 2016	Hyper-V on Windows Server 2016
NYC-FS01	File server	Windows Server 2012 R2	VMware vCenter Server 5.1
BOS-DB01	Microsoft SQL server	Windows Server 2016	VMware vCenter Server 6
Sea-CA01	Certification authority (CA)	Windows Server 2012 R2	Hyper-V on Windows Server 2016
Hou-NW01	DHCP/DNS	Windows Server 2008 R2	VMware vCenter Server 5.5

Which two virtual machines can you access by using Azure migrate? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Sea-CA01
- B. Hou-NW01
- C. NYC-FS01
- D. Sea-DC01
- E. BOS-DB01

Answer: C,E

Explanation:

Azure Migrate provides a centralized hub to assess and migrate to Azure on-premises servers, infrastructure, applications, and data. It provides the following:

Unified migration platform: A single portal to start, run, and track your migration to Azure.

Range of tools: A range of tools for assessment and migration. Azure Migrate tools include Server

Assessment and Azure Migrate: Server Migration. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings. Assessment and migration: In the Azure Migrate hub, you can assess and migrate:

Servers: Assess on-premises servers and migrate them to Azure virtual machines or Azure VMware Solution (AVS) (Preview).

Databases: Assess on-premises databases and migrate them to Azure SQL Database or to SQL Managed Instance.

Web applications: Assess on-premises web applications and migrate them to Azure App Service by using the Azure App Service Migration Assistant.

Virtual desktops: Assess your on-premises virtual desktop infrastructure (VDI) and migrate it to Windows Virtual Desktop in Azure.

Data: Migrate large amounts of data to Azure quickly and cost-effectively using Azure Data Box products.

Based on this information let's analyze each option:

NYC-FS01: Its role "Server" fall under above categories. Hence it can be accessed by using Azure migrate.

BOS-DB01: Its role "server" fall under above categories. Hence it can be accessed by using Azure migrate.

Sea-CA01: Its role "CA" does not fall under above categories. Hence it can not be accessed by using Azure migrate.

Hou-NW01: Its role "DNS" does not fall under above categories. Hence it can not be accessed by using Azure migrate.

Sea-DC01: Its role "DC" does not fall under above categories. Hence it can not be accessed by using Azure migrate.

Reference: <https://docs.microsoft.com/en-us/azure/migrate/migrate-services-overview>

286. You have a Basic App Service plan named ASP1 that hosts an Azure App Service named App1.

You need to configure a custom domain and enable backups for App1.

What should you do first?

- A. Configure a WebJob for App1.
- B. Scale up ASP1.
- C. Scale out ASP1.
- D. Configure the application settings for App1.

Answer: B

Explanation:

Scale up ASP1 : Correct

Basic App service plan does not support backup/restore.

	FREE	SHARED	BASIC	STANDARD	PREMIUM	ISOLATED	APP SERVICE LINUX
Authorization							
Backup/Restore				✓	✓		✓
Custom Domains		✓	✓	✓	✓	✓	✓

The Backup and Restore feature requires the App Service plan to be in the Standard, Premium or Isolated tier. Since in question it is mentioned as a Basic service plan app so at first you need to do it to Scale up the service plan so that backup can be enabled on App1.

Scale up: Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more. You scale up by changing the pricing tier of the App Service plan that your app belongs to.

Configure a WebJob for App1: Incorrect

WebJobs is a feature of Azure App Service that enables you to run a program or script in the same instance as a web app, API app, or mobile app. There is no additional cost to use WebJobs

Scale out ASP1: Incorrect

Scale out: Increase the number of VM instances that run your app. You can scale out to as many as 30 instances, depending on your pricing tier.

Configure the application settings for App1: Incorrect

This is the 2nd step you need to perform once azure service plan upgraded to standard.

Most folks don't realize how easy it is to configure a backup copy of your Azure App Service to ensure you have restorable archive copies of your app and database. In order to take advantage of this, you'll need to log into your Azure account and go to your App Service that you created and look under Settings then you will see Backup

 Configure  Refresh  Reset

 **Backup**

Configure backup to create restorable archive copies of your apps content, configuration and database. [Learn more](#)

 Backup is not configured. Click here to configure backup for your app.

Reference: <https://azure.microsoft.com/en-in/pricing/details/app-service/windows/>
<https://docs.microsoft.com/en-us/azure/app-service/manage-scale-up>
<https://docs.microsoft.com/en-us/azure/app-service/webjobs-create>
<https://microsoft.github.io/AzureTipsAndTricks/blog/tip28.html>

287.DRAG DROP

You are developing an Azure web app named WebApp1. WebApp1 uses an Azure App Service plan named Plan1 that uses the B1 pricing tier.

You need to configure WebApp1 to add additional instances of the app when CPU usage exceeds 70 percent for 10 minutes.

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

Set the Scale mode to **Scale based on a metric**, add rule, and set the instance limits.

From the Deployment Resource settings blade of WebApp1, add a slot.

Set the Scale mode to **Scale to a specific instance count**, and set the instance count.

From the Tags settings blade of WebApp1, add a tag named **SScale** that has a value of **Auto**.

From the Scale up (App Service Plan) settings blade, change the pricing tier.

From the Scale out (App Service Plan) settings blade, enable autoscale.

Answer:**Actions****Answer Area**

Set the Scale mode to **Scale based on a metric**, add rule, and set the instance limits.

From the Scale up (App Service Plan) settings blade, change the pricing tier.

From the Deployment Resource settings blade of WebApp1, add a slot.

From the Scale out (App Service Plan) settings blade, enable autoscale.

Set the Scale mode to **Scale to a specific instance count**, and set the instance count.

Set the Scale mode to **Scale based on a metric**, add rule, and set the instance limits.

From the Tags settings blade of WebApp1, add a tag named **SScale** that has a value of **Auto**.

From the Scale up (App Service Plan) settings blade, change the pricing tier.

From the Scale out (App Service Plan) settings blade, enable autoscale.

Explanation:

Box 1: From the Scale up (App Service Plan) settings blade, change the pricing tier. The B1 pricing tier only allows for 1 core. We must choose another pricing tier.

Box 2: From the Scale out (App Service Plan) settings blade, enable autoscale

1. Log in to the Azure portal at <http://portal.azure.com>
2. Navigate to the App Service you would like to autoscale.
3. Select Scale out (App Service plan) from the menu
4. Click on Enable autoscale. This activates the editor for scaling rules.

Default Auto created scale condition Edit

Scale mode Scale based on a metric Scale to a specific instance count

Rules Scale out and scale in your instances based on metric. For example, add a rule that increases instance count by 1 when CPU percentage is above 70%

Add a rule

Instance limits Minimum Maximum Default

Schedule This scale condition is executed when none of the other scale condition(s) match

Add a scale condition

Box 3: From the Scale mode to Scale based on metric, add a rule, and set the instance limits.

Click on Add a rule. This shows a form where you can create a rule and specify details of the scaling.

References:

<https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

<https://blogs.msdn.microsoft.com/hsirli/2017/07/03/autoscaling-azure-web-apps/>

288.HOTSPOT

You have an Azure Storage accounts as shown in the following exhibit.

Storage accounts								
Contoso								
Add		Edit columns		Refresh	Assign Tags		Delete	
Subscriptions: All 2 selected - Don't see a subscription? Switch directories								
<input type="button" value="Filter by name..."/>	<input type="button" value="All subscriptions"/>	<input type="button" value="All resource groups"/>	<input type="button" value="All types"/>	<input type="button" value="All locations"/>	<input type="button" value="No grouping"/>			
3 items								
<input type="checkbox"/>	NAME	TYPE	KIND	RESOURCE	LOCATION	SUBSCRIPTI...	ACCESS T...	REPLICAT....
<input type="checkbox"/>	storageaccount1	Storage account	Storage	ContosoRG1	EastUS	Subscription 1	-	Read-access ge...
<input type="checkbox"/>	storageaccount2	Storage account	StorageV2	ContosoRG1	CentralUS	Subscription 1	Host	Geo-redundant...
<input type="checkbox"/>	storageaccount3	Storage account	BlobStorage	ContosoRG1	EastUS	Subscription 1	Host	Locally-redundant...

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

You can use [answer choice] for Azure Table Storage.

<input type="checkbox"/>
storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

<input type="checkbox"/>
storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Answer:

Answer Area

You can use [answer choice]
for Azure Table Storage.

storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice]
for Azure Blob storage.

storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Explanation:

Box 1: storageaccount1 and storageaccount2 only

Box 2: All the storage accounts

Note: The three different storage account options are: General-purpose v2 (GPv2) accounts, General-purpose v1 (GPv1) accounts, and Blob storage accounts.

References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-account-options>

289. You create an Azure Storage account named Contoso storage.

You plan to create a file share named data.

Users need to map a drive to the data file share from home computers that run Windows 10.

Which port should be open between the home computers and the data file share?

- A. 80
- B. 443
- C. 445
- D. 3389

Answer: C

Explanation:

Ensure port 445 is open: The SMB protocol requires TCP port 445 to be open; connections will fail if port 445 is blocked.

References: <https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

290. DRAG DROP

You have two Azure virtual machines named VM1 and VM2. VM1 has a single data disk named Disk1.

You need to attach Disk1 to VM2. The solution must minimize downtime for both virtual machines.

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

Actions	Answer Area
Start VM2.	
Stop VM1.	
Start VM1.	
Detach Disk1 from VM1.	
Attach Disk1 to VM2.	
Stop VM2.	

Answer:

Actions	Answer Area
Start VM2.	Stop VM1.
Stop VM1.	Detach Disk1 from VM1.
Start VM1.	Start VM1.
Detach Disk1 from VM1.	Attach Disk1 to VM2.
Attach Disk1 to VM2.	
Stop VM2.	

Explanation:

Step 1: Stop VM1.

Step 2: Detach Disk1 from VM1.

Step 3: Start VM1.

Detach a data disk using the portal

Step 4: Attach Disk1 to VM2

Attach an existing disk

Follow these steps to reattach an existing available data disk to a running VM.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/detach-disk>

<https://docs.microsoft.com/en-us/azure/lab-services/devtest-lab-attach-detach-data-disk>

291.HOTSPOT

You have an Azure subscription named Subscription1.

Subscription1 contains the resources in the following table.

Name	Type
RG1	Resource group
RG2	Resource group
VNet1	Virtual network
VNet2	Virtual network

VNet1 is in RG1. VNet2 is in RG2. There is no connectivity between VNet1 and VNet2.

An administrator named Admin1 creates an Azure virtual machine named VM1 in RG1. VM1 uses a disk named Disk1 and connects to VNet1. Admin1 then installs a custom application in VM1.

You need to move the custom application to VNet2. The solution must minimize administrative effort.

Which two actions should you perform? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First action:

- ▼
- Create a network interface in RG2.
- Detach a network interface.
- Delete VM1.
- Move a network interface to RG2.

Second action:

- ▼
- Attach a network interface.
- Create a network interface in RG2.
- Create a new virtual machine.
- Move VM1 to RG2.

Answer:

Answer Area

First action:

- ▼
- Create a network interface in RG2.
- Detach a network interface.
- Delete VM1.
- Move a network interface to RG2.

Second action:

- ▼
- Attach a network interface.
- Create a network interface in RG2.
- Create a new virtual machine.
- Move VM1 to RG2.

Explanation:

We cannot just move a virtual machine between networks.

What we need to do is identify the disk used by the VM, delete the VM itself while retaining the disk, and recreate the VM in the target virtual network and then attach the original disk to it. First action: Delete VM1

Second action: Create a new virtual machine

Reference:

<https://docs.microsoft.com/en-us/archive/blogs/canitpro/step-by-step-move-a-vm-to-a-different-vnet-on-azure>

<https://4sysops.com/archives/move-an-azure-vm-to-another-virtual-network-vnet/#migrate-an-azure-vm-between-vnets>

292. You have an Azure virtual machine named VM1 that you use for testing. VM1 is protected by Azure Backup.

You delete VM1.

You need to remove the backup data stored for VM1.

What should you do first?

- A. Modify the backup policy.
- B. Delete the Recovery Services vault.
- C. Stop the backup.
- D. Delete the storage account.

Answer: C

Explanation:

Azure Backup provides backup for virtual machines — created through both the classic deployment model and the Azure Resource Manager deployment model — by using custom-defined backup policies in a Recovery Services vault.

With the release of backup policy management, customers can manage backup policies and model them to meet their changing requirements from a single window. Customers can edit a policy, associate more virtual machines to a policy, and delete unnecessary policies to meet their compliance requirements.

293. You have an Azure subscription that contains 100 virtual machines.

You regularly create and delete virtual machines.

You need to identify unattached disks that can be deleted.

What should you do?

- A. From Microsoft Azure Storage Explorer, view the Account Management properties.
- B. From Azure Cost Management, create a Cost Management report.
- C. From the Azure portal, configure the Advisor recommendations.

Answer: A

Explanation:

Explanation

You can find unused disks in the Azure Storage Explorer console. Once you drill down to the Blob containers under a storage account, you can see the lease state of the residing VHD (the lease state determines if the VHD is being used by any resource) and the VM to which it is leased out. If you find that the lease state and the VM fields are blank, it means that the VHD in question is unused. The screenshot below shows two active VHDs being used by VMs as data and OS disks. The name of the VM and lease

state are shown in the "VM Name" and "Lease State" columns, respectively.

Name	Last Modified	Blob Type	Content Type	Size	Lease State	Disk Name	VM Name	Disk Type
netappinst5-20170418-102205.vhd	Tue, 18 Apr 2017 00:24:25 GMT	Page Blob	application/octet-stream	350.0 GB	Leased	netappinst5-20170418-102205	netappinst5	DataDisk
netappinst520170418001901.vhd	Tue, 18 Apr 2017 00:43:46 GMT	Page Blob	application/octet-stream	127.0 GB	Leased	netappinst5	netappinst5	OSDisk

Reference: <https://cloud.netapp.com/blog/reduce-azure-storage-costs>

294.DRAG DROP

You have an availability set named AS1 that contains three virtual machines named VM1, VM2, and VM3. You attempt to reconfigure VM1 to use a larger size. The operation fails and you receive an allocation failure message.

You need to ensure that the resize operation succeeds.

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

Start VM1, VM2, and VM3.

Stop VM1, VM2, and VM3.

Start VM2 and VM3.

Resize VM1.

Stop VM2 and VM3.

Start VM1.

Answer:

Actions	Answer Area
Start VM1, VM2, and VM3.	Stop VM1, VM2, and VM3.
Stop VM1, VM2, and VM3.	Resize VM1.
Start VM2 and VM3.	Start VM1, VM2, and VM3.
Resize VM1.	
Stop VM2 and VM3.	
Start VM1.	

Explanation:

Action 1: Stop VM1, VM2 and VM3

If the VM you wish to resize is part of an availability set, then you must stop all VMs in the availability set before changing the size of any VM in the availability set. The reason all VMs in the availability set must be stopped before performing the resize operation to a size that requires different hardware is that all running VMs in the availability set must be using the same physical hardware cluster. Therefore, if a change of physical hardware cluster is required to change the VM size then all VMs must be first stopped and then restarted one-by-one to a different physical hardware clusters.

Action 2: Resize VM1

Action 3: Start VM1, VM2, and VM3

References: <https://azure.microsoft.com/es-es/blog/resize-virtual-machines/>

295. You have an Azure tenant that contains two subscriptions named Subscription1 and Subscription2.

In Subscription1, you deploy a virtual machine named Server1 that runs Windows Server 2016. Server1 uses managed disks.

You need to move Server1 to Subscription2. The solution must minimize administration effort.

What should you do first?

- A. In Subscription2, create a copy of the virtual disk.
- B. From Azure PowerShell, run the Move-AzureRmResource cmdlet.
- C. Create a snapshot of the virtual disk.
- D. Create a new virtual machine in Subscription2.

Answer: B

Explanation:

To move existing resources to another resource group or subscription, use the Move-AzureRmResource cmdlet.

References:

<https://docs.microsoft.com/en-in/azure/azure-resource-manager/resource-group-move-resources#mover>

esources

296. You have an Azure Active Directory (Azure AD) tenant named Tenant1 and an Azure subscription named Subscription1. You enable Azure AD Privileged Identity Management.

You need to secure the members of the Lab Creator role. The solution must ensure that the lab creators request access when they create labs.

What should you do first?

- A. From Azure AD Privileged Identity Management, edit the role settings for Lab Creator.
- B. From Subscription1 edit the members of the Lab Creator role.
- C. From Azure AD Identity Protection, creates a user risk policy.
- D. From Azure AD Privileged Identity Management, discover the Azure resources of Conscription.

Answer: A

Explanation:

As a Privileged Role Administrator you can:

References: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

297. DRAG DROP

You create an Azure Migrate project named TestMig in a resource group named test-migration.

You need to discover which on-premises virtual machines to assess for migration.

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

Answer Area

Configure the collector and start discovery

Create a migration group in the project

Create a collector virtual machine

Create an assessment in the project

Download the OVA file for the collector appliance

Answer:

Answer Area

Configure the collector and start discovery	Download the OVA file for the collector appliance
Create a migration group in the project	Create a migration group in the project
Create a collector virtual machine	Create an assessment in the project
Create an assessment in the project	
Download the OVA file for the collector appliance	

Explanation:

Step 1: Download the OVA file for the collection appliance

Azure Migrate uses an on-premises VM called the collector appliance, to discover information about your on-premises machines. To create the appliance, you download a setup file in Open Virtualization Appliance (.ova) format, and import it as a VM on your on-premises vCenter Server.

Step 2: Create a migration group in the project

For the purposes of assessment, you gather the discovered VMs into groups. For example, you might group VMs that run the same application. For more precise grouping, you can use dependency visualization to view dependencies of a specific machine, or for all machines in a group and refine the group.

Step 3: Create an assessment in the project

After a group is defined, you create an assessment for it.

References: <https://docs.microsoft.com/en-us/azure/migrate/migrate-overview>

298. You plan to migrate an on-premises Hyper-V environment to Azure by using Azure Site Recovery. The Hyper-V environment is managed by using Microsoft System Center Virtual Machine Manager (VMM).

The Hyper-V environment contains the virtual machines in the following table.

Name	Operating system (OS)	OS disk size	BitLocker Drive Encryption (BitLocker) enabled on OS disks	Generation
DC1	Windows Server 2016	500 GB	No	2
FS1	Ubuntu 16.04 LTS	200 GB	No	2
CA1	Windows Server 2012 R2	1 TB	Yes	1
SQL1	Windows Server 2016	200 GB	No	2

Which virtual machine can be migrated by using Azure Site Recovery?

- A. DC1
- B. FS1
- C. CA1
- D. SQL1

Answer: D

Explanation:

DC1: Not supported as it is Gen2 and OS disk size is greater than 300 GB

FS1: Not supported as it is Gen2 and Linux VM. Linux Generation 2 VMs aren't supported.

CA1: Not supported as bitlocker is enabled. BitLocker must be disabled before you enable replication for a VM.

SQL1: Supported

Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix#azure-vm-requirements>

299. You have an Azure Active Directory (Azure AD) tenant that has Azure AD Privileged Identity Management configured.

You have 10 users who are assigned the Security Administrator role for the tenant.

You need the users to verify whether they still require the Security Administrator role.

What should you do?

- A. From Azure AD Identity Protection, configure a user risk policy.
- B. From Azure AD Privileged Identity Management, create an access review.
- C. From Azure AD Identity Protection, configure the Weekly Digest.
- D. From Azure AD Privileged Identity Management, create a conditional access policy.

Answer: B

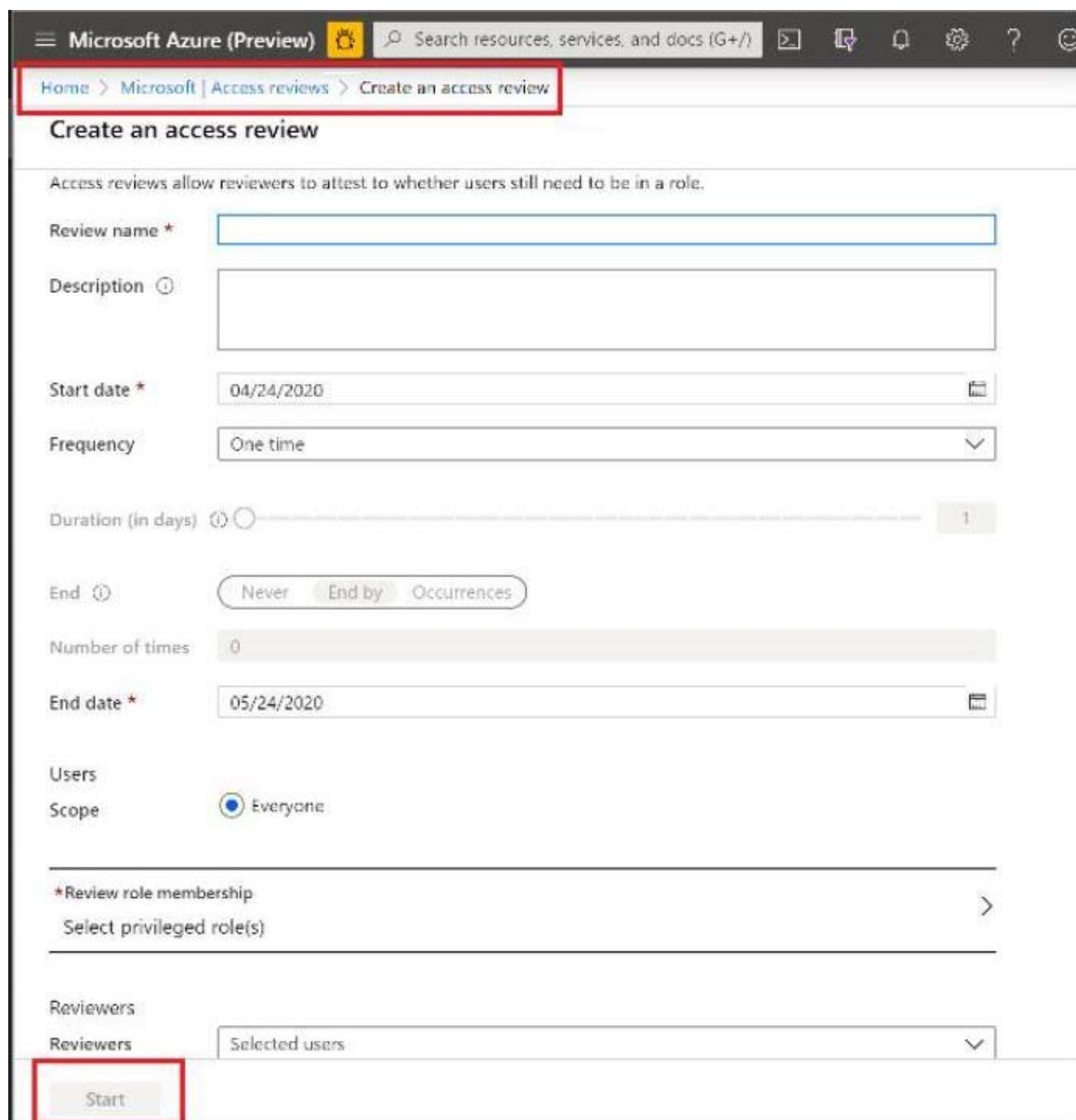
Explanation:

To reduce the risk associated with stale role assignments, you should regularly review access.

You can use Azure AD Privileged Identity Management (PIM) to create access reviews for privileged Azure AD roles. You can also configure recurring access reviews that occur automatically.

Steps:

1. Sign in to Azure portal with a user that is a member of the Privileged role administrator role.
2. Open Azure AD Privileged Identity Management.
3. Select Azure AD roles.
4. Under Manage, select Access reviews, and then select New.



Microsoft Azure (Preview) Search resources, services, and docs (G+/-) Home > Microsoft | Access reviews > Create an access review

Create an access review

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

Review name *

Description

Start date * Calendar icon

Frequency Down arrow

Duration (in days) End date

End Never End by Occurrences

Number of times

End date * Calendar icon

Users

Scope Everyone

***Review role membership** >

Select privileged role(s)

Reviewers

Reviewers Down arrow

Start

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

300. You have an Azure App Service plan that hosts an Azure App Service named App1.

You configure one production slot and four staging slots for App1.

You need to allocate 10 percent of the traffic to each staging slot and 60 percent of the traffic to the production slot.

What should you add to App1?

A. slots to the Testing in production blade

B. a performance test

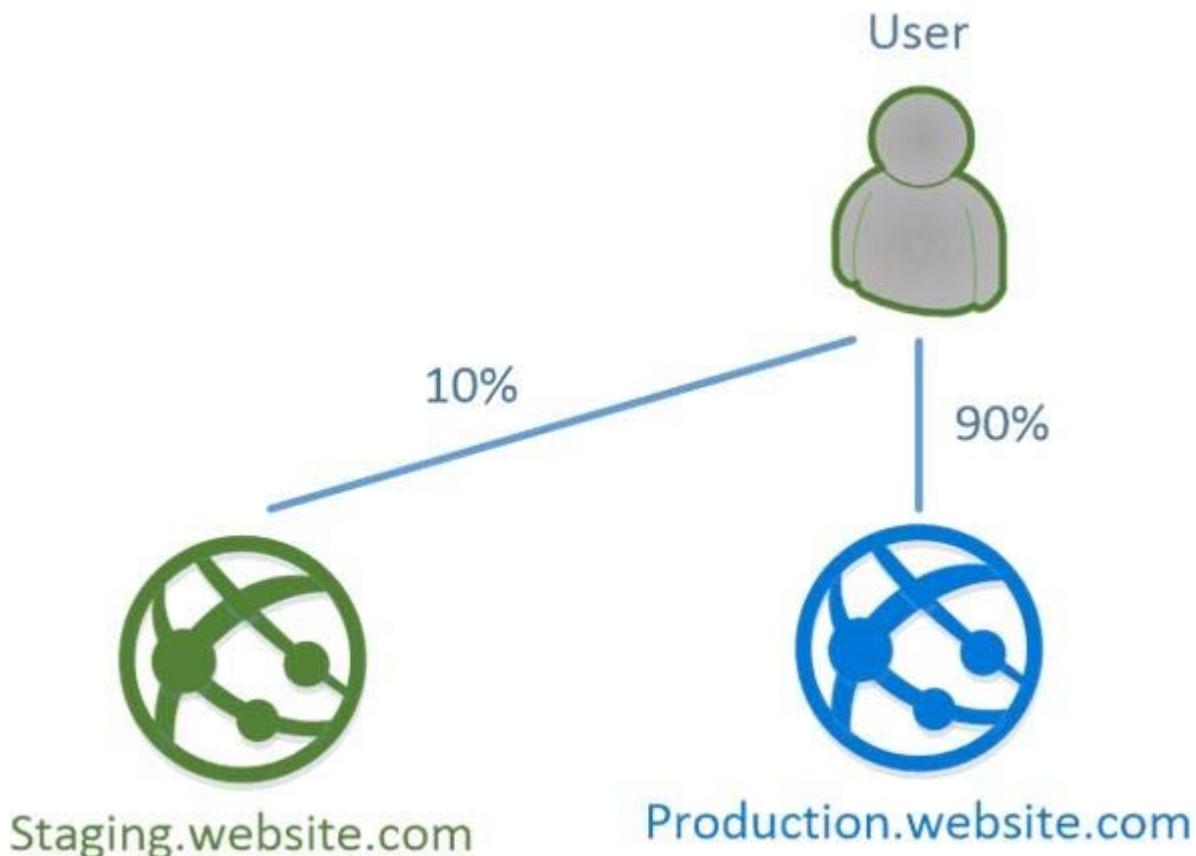
- C. a WebJob
- D. templates to the Automation script blade

Answer: A

Explanation:

Besides swapping, deployment slots offer another killer feature: testing in production. Just like the name suggests, using this, you can actually test in production. This means that you can route a specific percentage of user traffic to one or more of your deployment slots.

Example:



References: <https://stackify.com/azure-deployment-slots/>

301. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has 100 users located in an office in Paris.

The on-premises network contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2012 R2	Microsoft Exchange Server 2016
Server2	Windows Server 2016	Microsoft SQL Server 2016
Server3	Windows Server 2016	Domain controller
Server4	Red Hat Enterprise Linux 7.5	File server

You create a new subscription. You need to move all the servers to Azure.

Solution: You use Azure Site Recovery.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads online, when planned and unplanned outages occur. Azure Recovery Services contributes to your BCDR strategy:

- Site Recovery service: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

- Backup service: The Azure Backup service keeps your data safe and recoverable.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs, and physical servers.

Reference: <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview>

302. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has 100 users located in an office in Paris.

The on-premises network contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2012 R2	Microsoft Exchange Server 2016
Server2	Windows Server 2016	Microsoft SQL Server 2016
Server3	Windows Server 2016	Domain controller
Server4	Red Hat Enterprise Linux 7.5	File server

You create a new subscription. You need to move all the servers to Azure.

Solution: You run azcopy.exe.

Does this meet the goal?

A. Yes

B. No

Answer: B

303. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has 100 users located in an office in Paris.

The on-premises network contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2012 R2	Microsoft Exchange Server 2016
Server2	Windows Server 2016	Microsoft SQL Server 2016
Server3	Windows Server 2016	Domain controller
Server4	Red Hat Enterprise Linux 7.5	File server

You create a new subscription. You need to move all the servers to Azure.

Solution: You use the Data Migration Assistant tool.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The Data Migration Assistant tool is used to assess on-premises SQL Server instance(s) migrating to Azure SQL database(s).

Reference: <https://docs.microsoft.com/en-us/sql/dma/dma-overview?view=sql-server-ver15>

304. You create an Azure subscription that is associated to a basic Azure Active Directory (Azure AD) tenant. You need to receive an email notification when any user activates an administrative role.

What should you do?

- A. Purchase Azure AD Premium P2 and configure Azure AD Privileged Identity Management,
- B. Purchase Enterprise Mobility + Security E3 and configure conditional access policies.
- C. Purchase Enterprise Mobility + Security E5 and create a custom alert rule in Azure Security Center.
- D. Purchase Azure AD Premium P1 and enable Azure AD Identity Protection.

Answer: A

Explanation:

When key events occur in Azure AD Privileged Identity Management (PIM), email notifications are sent.

For example, PIM sends emails for the following events:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications>

305. You have an Azure subscription that contains 10 virtual machines.

You need to ensure that you receive an email message when any virtual machines are powered off, restarted, or deallocated.

What is the minimum number of rules and action groups that you require?

- A. three rules and three action groups
- B. one rule and one action group
- C. three rules and one action group
- D. one rule and three action groups

Answer: C

Explanation:

An action group is a collection of notification preferences defined by the user. Azure Monitor and Service Health alerts are configured to use a specific action group when the alert is triggered. Various alerts may use the same action group or different action groups depending on the user's requirements.

References:

<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-action-groups>

306. You have an Azure subscription that contains two resource groups named RG1 and RG2. RG2 does not contain any resources.

RG1 contains the resources in the following table.

Name	Type	Description	Lock
VNet1	Virtual network	A virtual network	ReadOnly
VNet3	Virtual network	A classic virtual network	None
W10	Virtual machine	A virtual machine that runs Windows 10 and is stopped and attached only to VNet1	Delete
W10_OsDisk	Disk	A managed SSD disk that is attached to W10	None

Which resource can you move to RG2?

- A. W10_OsDisk
- B. VNet1
- C. VNet3
- D. W10

Answer: B

Explanation:

When moving a virtual network, you must also move its dependent resources. For example, you must move gateways with the virtual network. VM W10, which is in Vnet1, is not a dependent resource.

307. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the Redeploy blade, you click Redeploy.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

When you redeploy a VM, it moves the VM to a new node within the Azure infrastructure and then powers it back on, retaining all your configuration options and associated resources.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

308.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the Overview blade, you move the virtual machine to a different resource group.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You should redeploy the VM.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

309.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: Solution: From the Overview blade, you move the virtual machine to a different subscription.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You would need to Redeploy the VM.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

310.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the Update management blade, you click enable.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You would need to Redeploy the VM.

References: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

311.Note This question is part of a series of questions that present the same scenario. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Performance Monitor, you create a Data Collector Set (DCS)

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation: Network performance monitor allows you to monitor connectivity and latencies across hybrid network architectures, Expressroute circuits, and service/application endpoints. With an data collector set we can count specified network traffic, but we cannot inspect it. For this we would need a network watcher Packet Capture.

References:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/network-performance-monitor>

312.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals.

Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to these questions will not appear in the review screen.

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a packet capture.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.

Capture packets to and from a VM

Advanced filtering options and fine-tuned controls, such as the ability to set time and size limitations, provide versatility. The capture can be stored in Azure Storage, on the VM's disk, or both. You can then analyze the capture file using several standard network capture analysis tools.

Network Watcher variable packet capture allows you to create packet capture sessions to track traffic to and from a virtual machine. Packet capture helps to diagnose network anomalies both reactively and proactively.

References:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

313. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a connection monitor.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Network Watcher Connection Monitor enables you to configure and track connection reachability, latency, and network topology changes. It helps reduce the amount of time to detect connectivity problems. The returned results can provide insights into whether a connectivity problem is due to a platform or a user configuration problem. This is not used in cases where we need to inspect for all the network traffic from one vm to another vm.

On the other hand Network Watcher packet capture allows you to create capture sessions to track traffic to and from a virtual machine. So in this scenario we need to use Network Watcher packet capture

References:

[https://azure.microsoft.com/en-in/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-](https://azure.microsoft.com/en-in/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/#:~:text=Network%20Watcher%20Connection%20Monitor%20helps,or%20a%20user%20configuration%20problem)

[regions/#:~:text=Network%20Watcher%20Connection%20Monitor%20helps,or%20a%20user%20configuration%20problem">https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal](https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal)

314. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a packet capture.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

<https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/>

315. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Monitor, you create a metric on Network In and Network Out.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You should use Azure Network Watcher.

References:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

316. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Performance Monitor, you create a Data Collector Set (DCS).

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You should use Azure Network Watcher.

References:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

317. HOTSPOT

You have an Azure Subscription named Subscription1. has

Subscription1 contains the virtual machines in the following table.

Name	IP address
VM1	10.0.1.4
VM2	10.0.2.4
VM3	10.0.3.4

Subscription1 contains the virtual machines in the following table.

Name	Address space	Connected virtual machine
Subnet1	10.0.1.0/24	VM1
Subnet2	10.0.2.0/24	VM2
Subnet3	10.0.3.0/24	VM3

VM3 has multiple network, including a network adapter named NIC3, IP forwarding is enabled on NIC3.

Routing is enabled on VM3.

You create a route table named RT1 that contains the routes in the following table.

Address prefix	Next hop type	Next hop address
10.0.1.0/24	Virtual appliance	10.0.3.4
10.0.2.0/24	Virtual appliance	10.0.3.4

You apply RT1 to subnet1 and Subnet2.

For each of the following statements, select Yes if the statements is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM3 can establish a network connection to VM1.	<input type="radio"/>	<input type="radio"/>
If VM3 is turned off, VM2 can establish a network connection to VM1.	<input type="radio"/>	<input type="radio"/>
VM1 can establish a network connection to VM2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM3 can establish a network connection to VM1.	<input checked="" type="radio"/>	<input type="radio"/>
If VM3 is turned off, VM2 can establish a network connection to VM1.	<input type="radio"/>	<input checked="" type="radio"/>
VM1 can establish a network connection to VM2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

IP forwarding enables the virtual machine a network interface is attached to:

The setting must be enabled for every network interface that is attached to the virtual machine that receives traffic that the virtual machine needs to forward. A virtual machine can forward traffic whether it has multiple network interfaces or a single network interface attached to it. Box 1: Yes

The routing table allows connections from VM3 to VM1 and VM2. And as IP forwarding is enabled on VM3, VM3 can connect to VM1.

Box 2: No

VM3, which has IP forwarding, must be turned on, in order for VM2 to connect to VM1. Box 3: Yes

The routing table allows connections from VM1 and VM2 to VM3. IP forwarding on VM3 allows VM1 to connect to VM2 via VM3.

References:

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

<https://www.quora.com/What-is-IP-forwarding>

318.HOTSPOT

Your company has offices in New York and Los Angeles.

You have an Azure subscription that contains an Azure virtual network named VNet1. Each office has a site-to-site VPN connection to VNet1.

Each network uses the address spaces shown in the following table.

Location	IP address space
VNet1	192.168.0.0/20
New York	10.0.0.0/16
Los Angeles	10.10.0.0/16

You need to ensure that all Internet-bound traffic from VNet1 is routed through the New York office.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

In Azure, run:

New-AzureRmLocalNetworkGateway
New-AzureRmVirtualNetworkGatewayConnection
Set-AzureRmVirtualNetworkGatewayDefaultSite

On a VPN device in the New York office, set the traffic selectors to:

0.0.0.0/0
10.0.0.0/16
192.168.0.0/20

Answer:

In Azure, run:

New-AzureRmLocalNetworkGateway
New-AzureRmVirtualNetworkGatewayConnection
Set-AzureRmVirtualNetworkGatewayDefaultSite

On a VPN device in the New York office, set the traffic selectors to:

0.0.0.0/0
10.0.0.0/16
192.168.0.0/20

Explanation:

Box 1: Set-AzureRmVirtualNetworkGatewayDefaultSite

The Set-AzureRmVirtualNetworkGatewayDefaultSite cmdlet assigns a forced tunneling default site to a virtual network gateway. Forced tunneling provides a way for you to redirect Internet-bound traffic from Azure virtual machines to your on-premises network; this enables you to inspect and audit traffic before releasing it. Forced tunneling is carried out by using a virtual private network (VPN) tunnel; this tunnel requires a default site, a local gateway where all the Azure Internet-bound traffic is redirected. Set-AzureRmVirtualNetworkGatewayDefaultSite provides a way to change the default site assigned to a gateway.

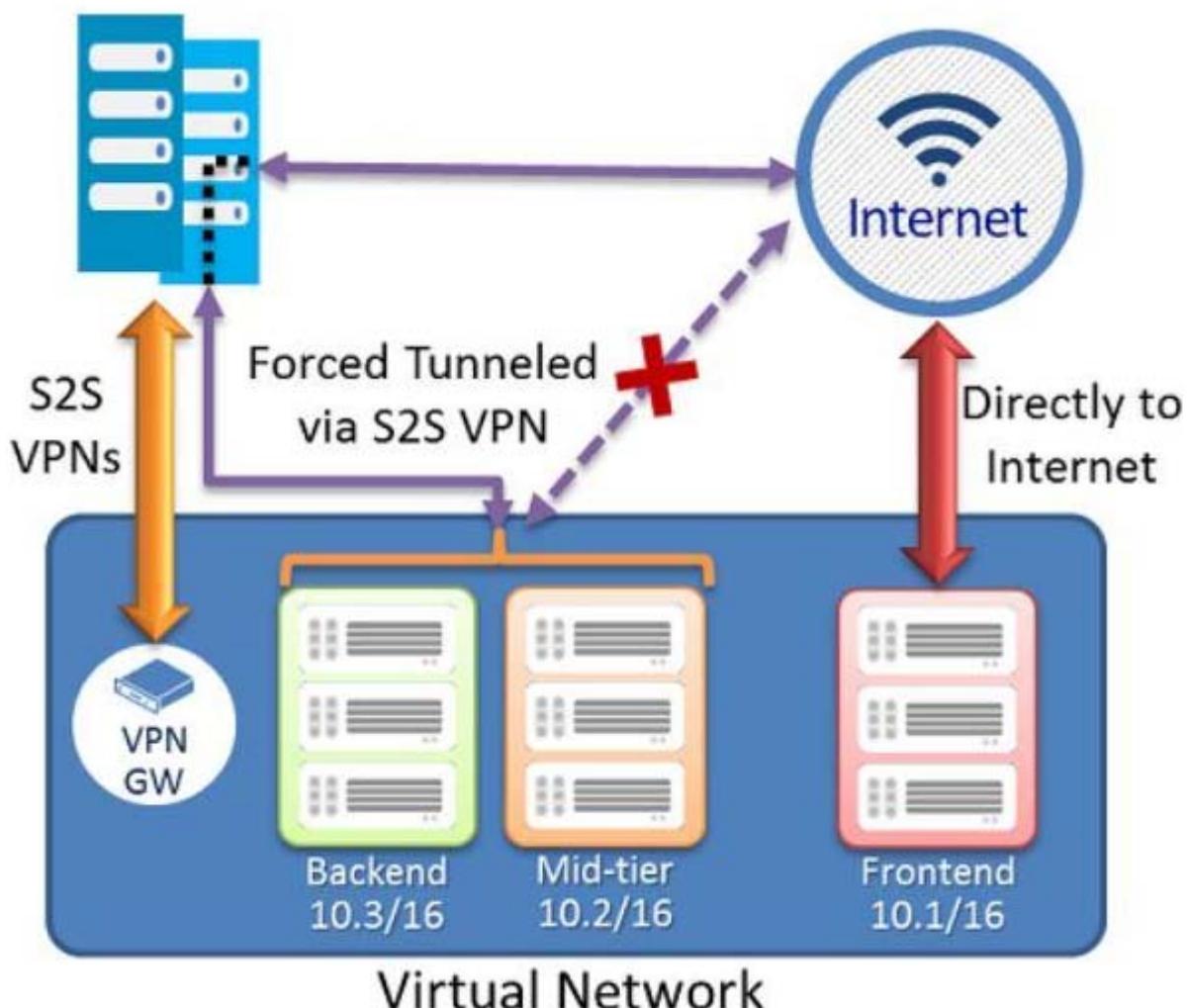
Box 2: 0.0.0.0/0

Forced tunneling must be associated with a VNet that has a route-based VPN gateway. You need to set a "default site" among the cross-premises local sites connected to the virtual network. Also, the on-premises VPN device must be configured using 0.0.0.0/0 as traffic selectors.

Forced Tunneling:

The following diagram illustrates how forced tunneling works

On Premises



Virtual Network

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.network/set-azurermvirtualnetworkgatewaydefaultsite?view=azurermps-6.13.0>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm>

319. You have an Azure subscription that contains the resources shown in the following table.

Resource group (change)
Production

Address space
10.2.0.0/16

Location
West US

DNS servers
Azure provided DNS service

Subscription (change)
Production subscription

Subscription ID
14d26092-8e42-4ea7-b770-9dcef70fb1ea

Tags (change)
Click here to add tags

Connected devices

DEVICE TYPE IP ADDRESS SUBNET

No results.

The Not allowed resource types Azure policy is assigned to RG1 and uses the following parameters:

- § Microsoft.Network/virtualNetwork
- § Microsoft.Compute/virtualMachines

In RG1, you need to create a new virtual machine named VM2, and then connect VM2 to VNET1.

What should you do first?

- A. Remove Microsoft.Network/virtualNetworks from the policy
- B. Create an Azure Resource Manager template
- C. Remove Microsoft.Compute/virtualMachines from the policy
- D. Add a subnet to VNET1

Answer: C

Explanation: The Not allowed resource types Azure policy prohibits the deployment of specified resource types. You specify an array of the resource types to block.

Virtual Networks and Virtual Machines are prohibited.

Reference: <https://docs.microsoft.com/en-us/azure/governance/policy/samples/>

320.HOTSPOT

You are creating an Azure load balancer.

You need to add an IPv6 load balancing rule to the load balancer.

How should you complete the Azure PowerShell script? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```

$rule1 = 

|                                             |
|---------------------------------------------|
| Add-AzureRmLoadBalancerRuleConfig           |
| New-AzureRmLoadBalancerInboundNatRuleConfig |
| New-AzureRmLoadBalancerRuleConfig           |
| Set-AzureRmLoadBalancerRuleConfig           |

 -Name "HTTPv6" -FrontendIpConfiguration $FEConfigv6
      -BackendAddressPool $backendpoolipv6 -Probe $Probe -Protocol Tcp -FrontendPort 80 -Backendport 8080
      New-AzureRmLoadBalancer -ResourceGroupName AdatumR0 -Name 'AdatumIPv6LB' -Location 'East US' -
      FrontendIpConfiguration $FEConfigv6
      -BackendAddressPool $backendpoolipv6 -Probe $Probe 

|                    |
|--------------------|
| \$rule1            |
| -InboundNatPool    |
| -InboundNatRule    |
| -LoadBalancingRule |


```

Answer:

```

$rule1 = 

|                                             |
|---------------------------------------------|
| Add-AzureRmLoadBalancerRuleConfig           |
| New-AzureRmLoadBalancerInboundNatRuleConfig |
| New-AzureRmLoadBalancerRuleConfig           |
| Set-AzureRmLoadBalancerRuleConfig           |

 -Name "HTTPv6" -FrontendIpConfiguration $FEConfigv6
      -BackendAddressPool $backendpoolipv6 -Probe $Probe -Protocol Tcp -FrontendPort 80 -Backendport 8080
      New-AzureRmLoadBalancer -ResourceGroupName AdatumR0 -Name 'AdatumIPv6LB' -Location 'East US' -
      FrontendIpConfiguration $FEConfigv6
      -BackendAddressPool $backendpoolipv6 -Probe $Probe 

|                    |
|--------------------|
| \$rule1            |
| -InboundNatPool    |
| -InboundNatRule    |
| -LoadBalancingRule |


```

Explanation:

Powershell command to create a load balancer rule (AzureRm module new version is AZ as given in below command):

```

$rule1v6 = New-AzLoadBalancerRuleConfig
- Name "HTTPv6"
- FrontendIpConfiguration $FEIPConfigv6
- BackendAddressPool $backendpoolipv6
- Probe $healthProbe
- Protocol Tcp
- FrontendPort 80
- BackendPort 8080

```

Powershell command to create the load balancer using the previously created objects :

```

New-AzLoadBalancer
- ResourceGroupName NRP-RG
- Name 'myNrpIPv6LB'
- Location 'West US'
- FrontendIpConfiguration $FEIPConfigv6
- InboundNatRule $inboundNATRule1v6
- BackendAddressPool $backendpoolipv6
- Probe $healthProbe
- LoadBalancingRule $rule1v6

```

References: <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-ipv6-internet-ps>

321. Note: This question is part of a series of questions that present the same scenario. Each question in

the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company registers a domain name of contoso.com.

You create an Azure DNS zone named contoso.com, and then you add an A record to the zone for a host named www that has an IP address of 131.107.1.10.

You discover that Internet hosts are unable to resolve www.contoso.com to the 131.107.1.10 IP address.

You need to resolve the name resolution issue.

Solution: You create a PTR record for www in the contoso.com zone.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Modify the Name Server (NS) record.

A NS record would be created automatically and you cannot modify it (but you can add to it to support co-hosting domains). You can add additional name servers to this NS record set, to support co-hosting domains with more than one DNS provider. You can also modify the TTL and metadata for this record set. However, you cannot remove or modify the pre-populated Azure DNS name servers.

References: <https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

322. You have an Azure subscription that contains three virtual networks named VNet1, VNet2, VNet3.

VNet2 contains a virtual appliance named VM2 that operates as a router.

You are configuring the virtual networks in a hub and spoke topology that uses VNet2 as the hub network.

You plan to configure peering between VNet1 and VNet2 and between VNet2 and VNet3.

You need to provide connectivity between VNet1 and VNet3 through VNet2.

Which two configurations should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. On the peering connections, allow forwarded traffic.
- B. On the peering connections, allow gateway transit.
- C. Create route tables and assign the table to subnets.
- D. Create a route filter.
- E. On the peering connections, use remote gateways.

Answer: A,C

Explanation:

Allow gateway transit: Check this box if you have a virtual network gateway attached to this virtual network and want to allow traffic from the peered virtual network to flow through the gateway. The peered virtual network must have the Use remote gateways checkbox checked when setting up the peering from the other virtual network to this virtual network.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints>

323.HOTSPOT

You have an Azure subscription named Subscription1.

In Subscription1, you create an Azure web app named WebApp1. WebApp1 will access an external service that requires certificate authentication.

You plan to require the use of HTTPS to access WebApp1.

You need to upload certificates to WebApp1.

In which formats should you upload the certificate? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Certificate format for HTTPS access:

<input type="checkbox"/>

Certificate format for external service access:

<input type="checkbox"/>

Answer:

Certificate format for HTTPS access:

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input checked="" type="checkbox"/>

Certificate format for external service access:

<input checked="" type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

Explanation:

A PFX file contains the public key file (SSL Certificate) and its unique private key file. This is required for HTTPS access. The web app will distribute the public key (in a CER file) to clients that connect to the web app.

The CER file is an SSL Certificate which has the public key of the external service. The external service will have the private key associated with the public key contained in the CER file.

324. You are the global administrator for an Azure Active Directory (Azure AD) tenant named adatum.com. You need to enable two-step verification for Azure users.

What should you do?

- A. Configure a playbook in Azure AD conditional access policy.
- B. Create an Azure AD conditional access policy.
- C. Create and configure the Identify Hub.
- D. Install and configure Azure AD Connect.

Answer: B

Explanation:

Conditional Access policies enforce registration, requiring unregistered users to complete registration at first sign-in, an important security consideration.

References: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>

325. Note: This question is part of a series of questions that present the same scenario goals. Some question sets might have more than one correct solution, while others

ion in the series contains a unique solution that might meet the stated not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure web app named App1. App1 runs in an Azure App Service plan named Plan1. Plan1 is associated to the Free pricing tier.

You discover that App1 stops each day after running continuously for 60 minutes.

You need to ensure that App1 can run continuously for the entire day.

Solution: You add a triggered WebJob to App1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to change to Basic pricing Tier.

Note: The Free Tier provides 60 CPU minutes / day. This explains why App1 is stops. The Basic tier has no such cap.

References: <https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

326. You have an Azure Service Bus.

You need to implement a Service Bus queue that guarantees first in first-out (FIFO) delivery of messages.

What should you do?

- A. Set the Lock Duration setting to 10 seconds.
- B. Enable duplicate detection.
- C. Set the Max Size setting of the queue to 5 GB.
- D. Enable partitioning.
- E. Enable sessions.

Answer: E

Explanation:

Through the use of messaging sessions you can guarantee ordering of messages, that is first-in-first-out (FIFO) delivery of messages.

References:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-azure-and-service-bus-queues-compared-contrasted>

327. You have an Azure subscription.

You activate Enterprise Mobility + Security E5 licenses for all users.

You need the users to request approval before they can create virtual machines.

What should you configure first?

- A. Azure Active Directory (Azure AD) conditional access policies
- B. Azure Active Directory (Azure AD) Authentication methods
- C. Azure Active Directory (Azure AD) Privileged Identity Management for the Azure resource roles
- D. Azure Active Directory (Azure AD) Privileged Identity Management for the Azure AD directory roles

Answer: C

Explanation:

Explanation

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

328. Your company registers a domain name of contoso.com.

You create an Azure DNS named contoso.com and then you add an A record to the zone for a host named www that has an IP address of 131.107.1.10.

You discover that Internet hosts are unable to resolve www.contoso.com to the 131.107.1.10 IP address.

You need to resolve the name resolution issue.

Solution: You modify the name server at the domain registrar.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

References: <https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

329. You have an on-premises network that contains a Hyper-V host named Host1. Host1 runs Windows Server 2016 and hosts 10 virtual machines that run Windows Server 2016.

You plan to replicate the virtual machines to Azure by using Azure Site Recovery.

You create a Recovery Services vault named ASR1 and a Hyper-V site named Site1.

You need to add Host1 to ASR1.

What should you do?

A. Download the installation file for the Azure Site Recovery Provider.

Download the vault registration key.

Install the Azure Site Recovery Provider on Host1 and register the server.

B. Download the installation file for the Azure Site Recovery Provider.

Download the storage account key.

Install the Azure Site Recovery Provider on Host1 and register the server.

C. Download the installation file for the Azure Site Recovery Provider.

Download the vault registration key.

Install the Azure Site Recovery Provider on each virtual machine and register the virtual machines.

D. Download the installation file for the Azure Site Recovery Provider.

Download the storage account key.

Install the Azure Site Recovery Provider on each virtual machine and register the virtual machines.

Answer: A

Explanation:

Below are the steps you need to perform in this scenario. Refer the link mentioned in the reference section.

Download the installation file for the Azure Site Recovery Provider

To set up the source environment, you create a Hyper-V site and add to that site the Hyper-V hosts containing VMs that you want to replicate. Then, you download and install the Azure Site Recovery Provider and the Azure Recovery Services agent on each host, and register the Hyper-V site in the vault.

The screenshot shows the Azure Site Recovery setup wizard. On the left, a vertical list of steps is shown:

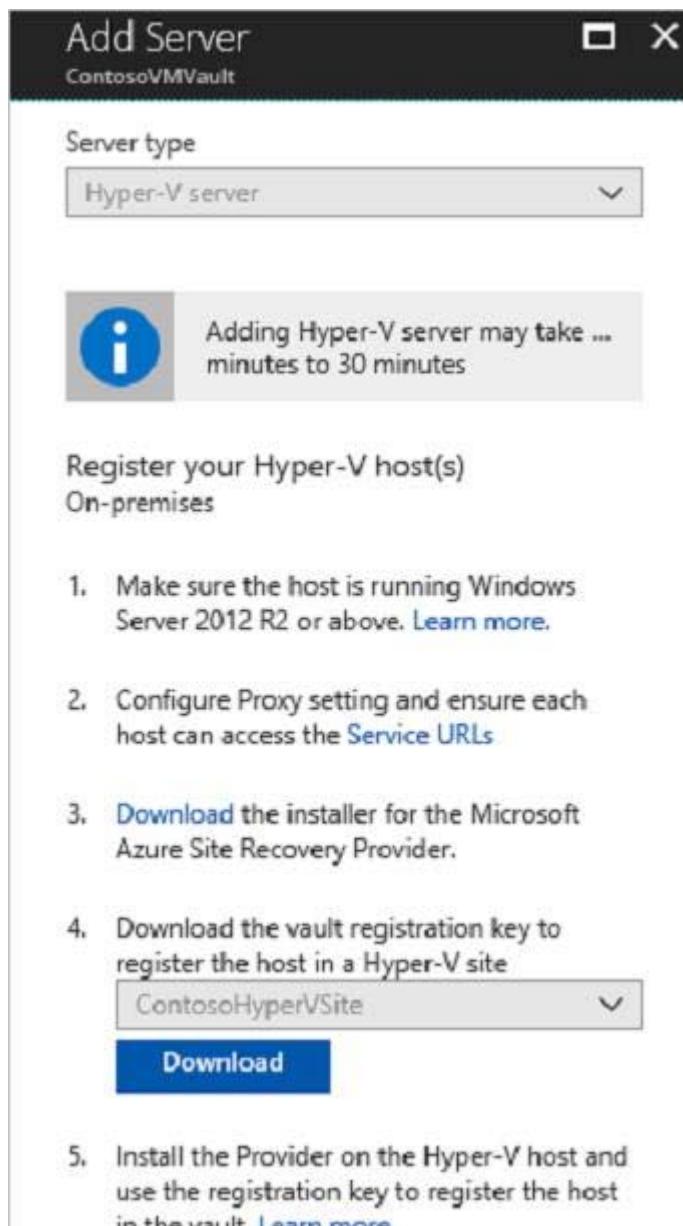
- 1 Protection goal: Hyper-V VMs to Azure (Completed)
- 2 Deployment planning: I will do it later (Completed)
- 3 Source: Prepare (In Progress)
- 4 Target: Prepare (In Progress)
- 5 Replication settings: Prepare (In Progress)

On the right, the configuration interface for a Hyper-V site is displayed. The top bar has two buttons: '+ Hyper-V Site' (highlighted with a dashed blue border) and '+ Hyper-V Server' (highlighted with a red border). The main area shows the following steps:

- ✓ Step 1: Select Hyper-V site**
 - * Hyper-V Site: ContosoHyperVSite
- Step 2: Ensure Hyper-V servers are added**
 - 0 Found... Click on +Hyper-V server in top command bar to add a Hyper-V server to the site. This may take approximately 15 min to 30 min.

Download the vault registration key

Download the Vault registration key. You need this when you install the Provider. The key is valid for five days after you generate it.



Install the Azure Site Recovery Provider on Host1.

Install the downloaded setup file (AzureSiteRecoveryProvider.exe) on each Hyper-V host that you want to add to the Hyper-V site. Setup installs the Azure Site Recovery Provider and Recovery Services agent on each Hyper-V host.

Register the server

In Registration, after the server is registered in the vault, select Finish.

References: <https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-tutorial>

330.HOTSPOT

From Azure Active Directory (AD) Privileged Identity Management, you configure the Role settings for the Owner role of an Azure subscription as shown in the following exhibit.

Role Settings

Assignment

Allow permanent eligible assignment

Expire eligible assignments after

3 months



Allow permanent active assignment

Expire eligible assignments after

1 Month



- Require Multi-Factor Authentication on active assignment
 Require justification on active assignment

Activation

Activation maximum duration (hours)



- Require Multi-Factor Authentication on activation
 Require justification on activation
 Require approval to activate

From Azure AD Privileged Identity Management, you assign the Owner role for the subscription to a user named User1, and you set the Assignment type to Active and Permanently eligible.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

User1 will be able to use the Owner role

for eight hours
for one month
for three months
indefinitely

After User1 activates the role for the first time, User1 will

need to activate the role in eight hours
need to activate the role in one month
need to activate the role in three months
never need to activate the role again

Answer:

User1 will be able to use the Owner role

for eight hours
for one month
for three months
indefinitely

After User1 activates the role for the first time, User1 will

need to activate the role in eight hours
need to activate the role in one month
need to activate the role in three months
never need to activate the role again

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=new>

331. You have an Azure subscription that contains two virtual networks named VNET1 and VNET2 and the users shown in the following table:

[Larger image](#)

Name	Subscription role	Azure Active Directory (Azure AD) role
User1	Owner	<i>None</i>
User2	Network Contributor	<i>None</i>
User3	<i>None</i>	Global administrator

You need to identify which users can configure peering between VNET1 and VNET2.

Which users should you identify?

- A. User1 only
- B. User3 only
- C. User1 and User2 only
- D. User1 and User3 only
- E. User1, User2 and User3

Answer: E

Explanation:

Owner: An owner can configure peering.

A Global administrator can configure peering. Network Contributor:

The accounts you use to work with virtual network peering must be assigned to the following roles:

§ Network Contributor: For a virtual network deployed through Resource Manager.

§ Classic Network Contributor: For a virtual network deployed through the classic deployment model.

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/resource-consistency/governance-multiple-teams>

332.HOTSPOT

You have an Azure subscription named Subscription1.

Subscription1 contains the virtual networks in the following table.

Name	Address space	Subnet name	Subnet address range
VNet1	10.1.0.0/16	Subnet1	10.1.0.0/24
VNet2	10.10.0.0/16	Subnet2	10.10.1.0/24
VNet3	172.16.0.0/16	Subnet3	172.16.1.0/24

Subscription1 contains the virtual machines in the following table:

Name	Network	Subnet	IP address
VM1	VNet1	Subnet1	10.1.1.4
VM2	VNet2	Subnet2	10.10.1.4
VM3	VNet3	Subnet3	172.16.1.4

The firewalls on all the virtual machines are configured to allow all ICMP traffic.

You add the peerings in the following table.

Virtual network	Peering network
VNet1	VNet3
VNet2	VNet3
VNet3	VNet1

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 |
|-------------------|-----------------------|-----------------------|
| VM1 can ping VM3. | <input type="radio"/> | <input type="radio"/> |
| VM2 can ping VM3. | <input type="radio"/> | <input type="radio"/> |
| VM2 can ping VM1. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

- | Statements | Yes | No |
|-------------------|----------------------------------|----------------------------------|
| VM1 can ping VM3. | <input checked="" type="radio"/> | <input type="radio"/> |
| VM2 can ping VM3. | <input type="radio"/> | <input checked="" type="radio"/> |
| VM2 can ping VM1. | <input type="radio"/> | <input checked="" type="radio"/> |

Explanation:

Statement 1: Yes

Vnet1 and Vnet3 are peers.

Statement 2: No

Statement 3: No

Peering connections are non-transitive.

References:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>

333. You have an Azure virtual machine named VM1

The network interface for VM1 is configured as shown in the exhibit (Click the Exhibit tab.)

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	RDP	3389	TCP	Any	Any	Allow
400	Rule1	80	TCP	Any	Any	Deny
500	Rule2	80,443	TCP	Any	Any	Deny
1000	Rule4	50-100,400-500	UDP	Any	Any	Allow
2000	Rule5	50-5000	Any	Any	VirtualNetwork	Deny
3000	Rule6	150-300	Any	Any	Any	Allow
4000	Rule3	60-500	Any	Any	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBal...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the internet.

What should you do?

- For Rule4, change the protocol from UDP to Any
- Modify the protocol of Rule4.
- Modify the action of Rule1.
- Change the priority of Rule3 to 450

Answer: D

Explanation:

Rule 2 is blocking HTTPS access (port 443) and has a priority of 500.

Changing Rule 3 (ports 60-500) and giving it a lower priority number will allow access on port 443.

Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops.

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

334. You have an Azure subscription that contains the resources in the following table.

Name	Type
ASG1	Application security group
NSG1	Network security group (NSG)
Subnet1	Subnet
VNet1	Virtual network
NIC1	Network interface
VM1	Virtual machine

Subnet1 is associated to VNet1. NIC1 attaches VM1 to Subnet1.

You need to apply ASG1 to VM1.

What should you do?

- A. Modify the properties of NSG1.
- B. Modify the properties of ASG1.
- C. Associate NIC1 to ASG1.

Answer: C

Explanation:

Application Security Group can be associated with NICs.

References:

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

335. You have an Azure virtual machine named VM1.

The network interface for VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

Network Interface: vm1175 **Effective security rules** **Topology** **Virtual network/subnet: RG5-vnet/default** **Public IP: 40.127.109.108** **Private IP: 172.16.1.4** **Accelerated networking: Disabled**

APPLICATION SECURITY GROUPS

INBOUND PORT RULES

Network security group VM1-nsg (attached to network interface: vm1175) **Add inbound port rule**

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	▲ RDP	3389	TCP	Any	Any	Allow
400	▲ Rule1	80	TCP	Any	Any	Deny
500	Rule2	80,443	TCP	Any	Any	Deny
1000	Rule4	50-100,400-500	UDP	Any	Any	Allow
2000	Rule5	50-5000	Any	Any	VirtualNetwork	Deny
3000	Rule6	150-300	Any	Any	Any	Allow
4000	Rule3	60-500	Any	Any	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBal...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the internet.

What should you do?

- A. Create a new inbound rule that allows TCP protocol 443 and configure the protocol to have a priority of 501.
- B. For Rule5, change the Action to Allow and change the priority to 401.
- C. Delete Rule1.
- D. Modify the protocol of Rule4.

Answer: B

Explanation:

Rule 2 is blocking HTTPS access (port 443) and has a priority of 500.

Changing Rule 5 (ports 50-5000) and giving it a lower priority number will allow access on port 443.

Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops.

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

336.HOTSPOT

You have an Azure subscription named Subscription1 that contains the quotas shown in the following table.

Quota	Location	Usage
Standard BS Family vCPUs	West US	0 of 20
Standard D Family vCPUs	West US	0 of 20
Total Regional vCPUs	West US	0 of 20

You deploy virtual machine to Subscription1 as shown in the following table.

Name	Size	vCPUs	Location	Status
VM1	Standard_B2ms	2	West US	Running
VM20	Standard_B16ms	16	West US	Stopped (Deallocated)

You plan to deploy the virtual machines shown in the following table.

Name	Size	vCPUs
VM3	Standard_B2ms	1
VM4	Standard_D4s_v3	4
VM5	Standard_B16ms	16

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

Statements	Yes	No
You can deploy VM3 to West US.	<input type="radio"/>	<input type="radio"/>
You can deploy VM4 to West US.	<input type="radio"/>	<input type="radio"/>
You can deploy VM5 to West US.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can deploy VM3 to West US.	<input checked="" type="radio"/>	<input type="radio"/>
You can deploy VM4 to West US.	<input type="radio"/>	<input checked="" type="radio"/>
You can deploy VM5 to West US.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

The total regional vCPUs is 20 so that means a maximum total of 20 vCPUs across all the different VM sizes.

The deallocated VM with 16 vCPUs counts towards the total. VM20 and VM1 are using 18 of the maximum 20 vCPUs leaving only two vCPUs available.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quotas>

337.Your VMware vSphere on-premises infrastructure hosts 600 virtual machines (VMs).

Your company is planning to move all of these VMs to Azure. You are asked to provide information about the resources that will be needed in Azure to host all of the VMs.

All VMs hosted in your on-premise infrastructure are based on Windows Server 2012 R2 or newer and RedHat Enterprise Linux 7.0 or newer.

You conduct the initial migration assessment and get a message that some virtual machines are conditionally ready for Azure.

You need to find the cause of this message.

What are two reasons why you might get this message on some VMs? (Choose two) Each correct answer presents part of the solution.

- A. The vCenter user does not have enough permissions on affected VMs.
- B. The operating system is configured as Windows Server 2003 in vCenter Server.
- C. The operating system is configured as Others in vCenter Server.
- D. The VMs are configured with the BIOS boot type.
- E. The VMs are configured with the UEFI boot type.

Answer: BE

Explanation:

To prepare for VMware VM assessment, you need to:

Verify VMware settings. Make sure that the vCenter Server and VMs you want to migrate meet requirements.

Set up permissions for assessment. Azure Migrate uses a vCenter account to access the vCenter Server, to discover and assess VMs.

Verify appliance requirements. Verify deployment requirements for the Azure Migrate appliance, before you deploy it in the next tutorial.

Reference: <https://docs.microsoft.com/en-us/azure/migrate/tutorial-prepare-vmware>

338.HOTSPOT

You enable password reset for contoso.onmicrosoft.com as shown in the Password Reset exhibit (Click the Password Reset tab.)

Name	Member of	Role assigned
User1	Group1	None
User2	Group2	None
User3	Group1, Group2	User administrator

You configure the authentication methods for password reset as shown in the Authentication Methods exhibit. (Click the Authentication Methods tab.)

Self-service password reset enabled 

Select group

Group2

Number of methods required to reset 

Methods available to users

- Mobile app notification (preview)
- Mobile app code (preview)
- Email
- Mobile phone
- Office phone
- Security questions

Number of questions required to register 

Number of questions required to reset 

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
After User2 answers three security questions, he can reset his password immediately.	<input type="radio"/>	<input type="radio"/>
If User1 forgets her password, she can reset the password by using the mobile phone app.	<input type="radio"/>	<input type="radio"/>
User3 can add security questions to the password reset process.	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area**

Statements	Yes	No
After User2 answers three security questions, he can reset his password immediately.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 forgets her password, she can reset the password by using the mobile phone app.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add security questions to the password reset process.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

Two methods are required.

Box 2: No

Self-service password reset is only enabled for Group2, and User1 is not a member of Group2.

Box 3: Yes

As a User Administrator User3 can add security questions to the reset process.

References: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr>
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/active-directory-passwords-faq>

339. You have an Azure Active Directory (Azure AD) tenant.

All administrators must enter a verification code to access the Azure portal.

You need to ensure that the administrators can access the Azure portal only from your on-premises network.

What should you configure?

- A. an Azure AD Identity Protection user risk policy.
- B. the multi-factor authentication service settings.
- C. the default for all the roles in Azure AD Privileged Identity Management
- D. an Azure AD Identity Protection sign-in risk policy

Answer: B**Explanation:**

the multi-factor authentication service settings - Correct choice There are two criterias mentioned in the question.

1. MFA required
2. Access from only a specific geographic region/IP range.

To satisfy both the requirements you need MFA with location conditional access. Please note to achieve this configuration you need to have AD Premium account for Conditional Access policy. Navigate to Active Directory --> Security --> Conditional Access --> Named Location. Here you can create a policy with location (on-premise IP range) and enable MFA. This will satisfy the requirements.

an Azure AD Identity Protection user risk policy - Incorrect choice

In the Identity Protection, there are three (3) protection policies- User Risk, Sign-In Risk & MFA

Registration. None of those in which you can enable a location (on-prem IP Range) requirement in any blade.

the default for all the roles in Azure AD Privileged Identity Management - Incorrect choice This option will not help you to restrict the users to access only from on-prem. an Azure AD Identity Protection sign-in risk policy - Incorrect choice

In the Identity Protection, there are three (3) protection policies- User Risk, Sign-In Risk & MFA Registration. None of those in which you can enable a location (on-prem IP Range) requirement in any blade.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

340. You have an Azure subscription.

You enable multi-factor authentication for all users.

Some users report that the email applications on their mobile device cannot connect to their Microsoft Exchange Online mailbox. The users can access Exchange Online by using a web browser and from Microsoft Outlook 2016 on their computer.

You need to ensure that the users can use the email applications on their mobile device.

What should you instruct the users to do?

- A. Create an app password
- B. Reset the Azure Active Directory (Azure AD) password
- C. Enable self-service password reset
- D. Reinstall the Microsoft Authenticator app

Answer: A

Explanation:

If you're enabled for multi-factor authentication, make sure that you have set up app passwords. Note: During your initial two-factor verification registration process, you're provided with a single app password. If you require more than one, you'll have to create them yourself. Go to the Additional security verification page.

References:

<https://docs.microsoft.com/en-us/office365/troubleshoot/sign-in/sign-in-to-office-365-azure-intune>

<https://docs.microsoft.com/sv-se/azure/active-directory/user-help/multi-factor-authentication-end-user-app-passwords>

341. You have an Azure Active Directory (Azure AD) tenant named Contoso.com that is synced to an Active Directory domain.

The tenant contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account
User4	Member	Windows Server Active Directory

The user have the attributes shown in the following table.

Name	Office phone	Mobile phone
User1	222-555-1234	222-555-2345
User2	null	null
User3	222-555-1234	222-555-2346
User4	222-555-1234	null

You need to ensure that you can enable Azure Multi-Factor Authentication (MFA) for all four users.

Solution: You create a new user account in Azure AD for User3.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

User3 requires a user account in Azure AD.

Note: Your Azure AD password is considered an authentication method. It is the one method that cannot be disabled.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

342. You are deploying a containerized web application in Azure.

When deploying the web app, which of the following are valid container image sources?

- A. Virtual machine

- B. Docker hub
- C. ACR
- D. On-premises

Answer: B,C

Explanation:

When you create a web app from a Docker image, you configure the following properties:

-The registry that contains the image. The registry can be Docker Hub, Azure Container Registry (ACR), or some other private registry.

- The image: This item is the name of the repository.
- The tag: This item indicates which version of the image to use from the repository. By convention, the most recent version is given the tag latest when it's built.
- Startup File: This item is the name of an executable file or a command to be run when the image is loaded. It's equivalent to the command that you can supply to Docker when running an image from the command line by using docker run. If you're deploying a ready-to-run, containerized app that already has the ENTRYPOINT and/or COMMAND values configured, you don't need to fill this in.

Reference:

<https://docs.microsoft.com/en-us/learn/modules/deploy-run-container-app-service/4-deploy-web-app>

343. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure web app named App1. App1 runs in an Azure App Service plan named Plan1.

Plan1 is associated to the Free pricing tier.

You discover that App1 stops each day after running continuously for 60 minutes.

You need to ensure that App1 can run continuously for the entire day.

Solution: You add a continuous WebJob to App1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

A web app can time out after 20 minutes of inactivity. Only requests to the actual web app reset the timer. Viewing the app's configuration in the Azure portal or making requests to the advanced tools site (https://<app_name>.scm.azurewebsites.net) don't reset the timer. If your app runs continuous or scheduled (Timer trigger) WebJobs, enable Always On to ensure that the WebJobs run reliably. This feature is available only in the Basic, Standard, and Premium pricing tiers.

The app service plan mentioned in the question is associated to the free tier , so addition of a continuous WebJob to App1 is not possible. So the proposed solution won't meet the goal.

Reference: <https://docs.microsoft.com/en-us/azure/app-service/webjobs-create>

344.HOTSPOT

Your network contains an Active Directory domain. The domain contains a user named User1.

The domain is synced to Azure Active Directory (Azure AD) as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

User1 can change his password from [answer choice].

- the My Apps portal
- a computer joined to the Active Directory domain
- a computer joined to Azure AD

When User1 changes his password, the password will be [answer choice].

- stored in Azure AD only
- stored in the Active Directory domain only
- stored in both Azure AD and the Active Directory domain

Answer:

User1 can change his password from [answer choice].

- the My Apps portal
- a computer joined to the Active Directory domain
- a computer joined to Azure AD

When User1 changes his password, the password will be [answer choice].

- stored in Azure AD only
- stored in the Active Directory domain only
- stored in both Azure AD and the Active Directory domain

Explanation:

Box 1: a computer joined in the Active Directory domain

The Active Directory domain service stores passwords in the form of a hash value representation, of the actual user password.

Box 2: Stored in both Azure AD and in the Active Director domain

The Active Directory domain service stores passwords in the form of a hash value representation, of the actual user password.

To synchronize your password, Azure AD Connect sync extracts your password hash from the

on-premises Active Directory instance.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization>

345. You have an Active Directory forest named contoso.com.

You install and configure Azure AD Connect to use password hash synchronization as the single sign-on (SSO) method. Staging mode is enabled.

You review the synchronization results and discover that the Synchronization Service Manager does not display any sync jobs.

You need to ensure that the synchronization completes successfully.

What should you do?

- A. From Synchronization Service Manager, run a full import.
- B. Run Azure AD Connect and set the SSO method to Pass-through Authentication.
- C. From Azure PowerShell, run Start-AdSyncSyncCycle -PolicyType Initial.
- D. Run Azure AD Connect and disable staging mode.

Answer: D

Explanation:

Staging mode must be disabled. If the Azure AD Connect server is in staging mode, password hash synchronization is temporarily disabled.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-troubleshoot-password-hash-synchronization#no-passwords-are-synchronized-troubleshoot-by-using-the-troubleshooting-task>

346. You sign up for Azure Active Directory (Azure AD) Premium.

You need to add a user named admin1@contoso.com as an administrator on all the computers that will be joined to the Azure AD domain.

What should you configure in Azure AD?

- A. Device settings from the Devices blade.
- B. General settings from the Groups blade.
- C. User settings from the Users blade.
- D. Providers from the MFA Server blade.

Answer: A

Explanation:

When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principles to the local administrators group on the device:

- The Azure AD global administrator role
- The Azure AD device administrator role
- The user performing the Azure AD join

In the Azure portal, you can manage the device administrator role on the Devices page.

To open the Devices page:

1. Sign in to your Azure portal as a global administrator or device administrator.
2. On the left navbar, click Azure Active Directory.

3. In the Manage section, click Devices.
4. On the Devices page, click Device settings.
5. To modify the device administrator role, configure Additional local administrators on Azure AD joined devices.

References: <https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin>

347.HOTSPOT

Your network contains an Active Directory domain named adatum.com and an Azure Active Directory (Azure AD) tenant named adatum.onmicrosoft.com.

Adatum.com contains the user accounts in the following table.

Name	Member of
User1	Domain Admins
User2	Schema Admins
User3	Incoming Forest Trust Builders
User4	Replicator
User5	Enterprise Admins

Adatum.onmicrosoft.com contains the user accounts in the following table.

Name	Role
UserA	Global administrator
UserB	User administrator
UserC	Security administrator
UserD	Service administrator

You need to implement Azure AD Connect. The solution must follow the principle of least privilege. Which user accounts should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Adatum.com:

▼

User1

User2

User3

User4

User5

Adatum.onmicrosoft.com:

▼

UserA

UserB

UserC

UserD

Answer:

Answer Area

Adatum.com:

User1
User2
User3
User4
User5

Adatum.onmicrosoft.com:

UserA
UserB
UserC
UserD

Explanation:

Box 1: User5

In Express settings, the installation wizard asks for the following:

AD DS Enterprise Administrator credentials

Azure AD Global Administrator credentials

The AD DS Enterprise Admin account is used to configure your on-premises Active Directory. These credentials are only used during the installation and are not used after the installation has completed. The Enterprise Admin, not the Domain Admin should make sure the permissions in Active Directory can be set in all domains.

Box 2: UserA

Azure AD Global Admin credentials credentials are only used during the installation and are not used after the installation has completed. It is used to create the Azure AD Connector account used for synchronizing changes to Azure AD. The account also enables sync as a feature in Azure AD.

References:

[https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-pe](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions)
missions

348. You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You hire a temporary vendor. The vendor uses a Microsoft account that has a sign-in of user1@outlook.com.

You need to ensure that the vendor can authenticate to the tenant by using user1@outlook.com.

What should you do?

- From Windows PowerShell, run the New-AzureADUser cmdlet and specify the –UserPrincipalName user1@outlook.com parameter.
- From the Azure portal, add a custom domain name, create a new Azure AD user, and then specify user1@outlook.com as the username.
- From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the –UserPrincipalName user1@outlook.com parameter.
- From the Azure portal, add a new guest user, and then specify user1@outlook.com as the email

address.

Answer: D

Explanation:

UserPrincipalName - contains the UserPrincipalName (UPN) of this user. The UPN is what the user will use when they sign in into Azure AD. The common structure is @, so for Abby Brown in Contoso.com, the UPN would be AbbyB@contoso.com Example:

To create the user, call the New-AzureADUser cmdlet with the parameter values: powershell

```
New-AzureADUser -AccountEnabled $True -DisplayName "Abby Brown" -
```

```
PasswordProfile$PasswordProfile -MailNickname "AbbyB" -UserPrincipalName "AbbyB@contoso.com"
```

References:

<https://docs.microsoft.com/bs-cyrl-ba/powershell/azure/active-directory/new-user-sample?view=azuread-ps-2.0>

349.DRAG DROP

You have an Azure Active Directory (Azure AD) tenant that has the initial domain name.

You have a domain name of contoso.com registered at a third-party registrar.

You need to ensure that you can create Azure AD users that have names containing a suffix of @contoso.com.

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

Actions

Answer Area

Configure company branding.

Add an Azure AD tenant.

Verify the domain.

Create an Azure DNS zone.

Add a custom domain name.

Add a record to the public contoso.com DNS zone.

Answer:

Actions	Answer Area
Configure company branding.	Add a custom domain name.
Add an Azure AD tenant.	Add a record to the public contoso.com DNS zone.
Verify the domain.	Verify the domain.
Create an Azure DNS zone.	
Add a custom domain name.	
Add a record to the public contoso.com DNS zone.	

Explanation:

The process is simple:

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

350. You have an Azure resource manager template that will be used to deploy 10 Azure Web Apps.

You have to ensure to deploy the pre-requisites before the deployment of the template.

You have to minimize the costs associated with the implementation.

Which of the following would you deploy as pre-requisites?

- A. An Azure Load Balancer
- B. An Application Gateway
- C. 10 Azure App Service Plans
- D. One App Service Plan

Answer: D

Explanation:

In App Service (Web Apps, API Apps, or Mobile Apps), an app always runs in an App Service plan. An App Service plan defines a set of compute resources for a web app to run. One App Service Plan: Correct Choice

For an Azure Web App, you need to have an Azure App Service Plan in place. You can associate multiple Azure Web Apps with the same App Service Plan. Hence to save on costs, you can just have one Azure App Service Plan in place.

An Azure Load Balancer: Incorrect Choice

An Azure load balancer is a Layer-4 (TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs. A load balancer health probe monitors a given port on each VM and only distributes traffic to an operational VM

An Application Gateway: Incorrect Choice

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

10 Azure App Service Plans: Incorrect Choice

For an Azure Web App, you need to have an Azure App Service Plan in place. You can associate multiple Azure Web Apps with the same App Service Plan. Hence to save on costs, you can just have one Azure

App Service Plan in place. So there is no need for 10 App Service Plans.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-load-balancer>

<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

351. You configure Azure AD Connect for Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) for an on-premises network. Users report that when they attempt to access myapps.microsoft.com, they are prompted multiple times to sign in and are forced to use an account name that ends with onmicrosoft.com.

You discover that there is a UPN mismatch between Azure AD and the on-premises Active Directory. You need to ensure that the users can use single-sign on (SSO) to access Azure resources.

What should you do first?

- A. From the on-premises network, deploy Active Directory Federation Services (AD FS).
- B. From Azure AD, add and verify a custom domain name.
- C. From the on-premises network, request a new certificate that contains the Active Directory domain name.
- D. From the server that runs Azure AD Connect, modify the filtering options.

Answer: B

Explanation:

Azure AD Connect lists the UPN suffixes that are defined for the domains and tries to match them with a custom domain in Azure AD. Then it helps you with the appropriate action that needs to be taken. The Azure AD sign-in page lists the UPN suffixes that are defined for on-premises Active Directory and displays the corresponding status against each suffix. The status values can be one of the following:

State: Verified Azure AD Connect found a matching verified domain in Azure AD. All users for this domain can sign in by using their on-premises credentials.

State: Not verified

Azure AD Connect found a matching custom domain in Azure AD, but it isn't verified. The UPN suffix of the users of this domain will be changed to the default .onmicrosoft.com suffix after synchronization if the domain isn't verified.

Action Required: Verify the custom domain in Azure AD.

References: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-user-signin>

352. You have an Azure subscription that contains the following storage account:

Name	Kind	Replication	Access tier	Advanced threat protection	Lock
storage1	StorageV2	Read access geo-redundant storage (RA-GRS)	Cool	On	Delete

You need to create a request to Microsoft Support to perform a live migration of storage1 to Zone Redundant Storage (ZRS) replication.

How should you modify storage1 before the Live migration?

- A. Set the replication to Locally-redundant storage (IRS)
- B. Disable Advanced threat protection

- C. Remove the lock
 D. Set the access tier to Hot

Answer: A

Explanation:

If you want to live migration from RA-GRS to ZRS, at first you have to Switch the storage tier to LRS and then only you can request a live migration.

Switching	...to LRS	...to GRS/RA-GRS	...to ZRS	...to GZRS/RA-GZRS
...from LRS	N/A	Use Azure portal, PowerShell, or CLI to change the replication setting ¹	Perform a manual migration Request a live migration	Perform a manual migration OR Switch to GRS/RA-GRS first and then request a live migration ¹
...from GRS/RA-GRS	Use Azure portal, PowerShell, or CLI to change the replication setting	N/A	Perform a manual migration OR Switch to LRS first and then request a live migration	Perform a manual migration Request a live migration

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/redundancy-migration?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&tabs=portal>

353. You have an Azure Kubernetes cluster in place.

You have to deploy an application using an Azure Container registry image.

Which of the following command can be used for this requirement?

- A. az kubernetes deploy
 B. kubectl apply
 C. New-AzKubernetes set
 D. docker run

Answer: B

Explanation:

kubectl apply: Correct Choice

The kubectl command can be used to deploy applications to a Kubernetes cluster.

az kubernetes deploy : Incorrect Choice

This command is used to manage Azure Kubernetes Services. This is not used to deploy applications to a Kubernetes cluster.

New-AzKubernetes set : Incorrect Choice

This command is used to create a new managed Kubernetes cluster. This is not used to deploy applications to a Kubernetes cluster.

docker run: Incorrect Choice

This is run command in a new container. This is not used to deploy applications to a Kubernetes cluster.

Reference:

<https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply>

<https://docs.microsoft.com/en-us/cli/azure/aks?view=azure-cli-latest>

<https://docs.microsoft.com/en-us/powershell/module/az.aks/New-AzAks?view=azps-3.8.0&viewFallbackFrom=azps-4.3.0>

<https://docs.docker.com/engine/reference/commandline/run/>

354.HOTSPOT

You have an Azure Storage account named storage1.

You have an Azure App Service app named app1 and an app named App2 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App1 and App2 can read blobs from storage1 for the next 30 days.

What should you configure in storage1 for each app?

App1: Access keys
 Advanced security
 Access control (IAM)
 Shared access signatures (SAS)

App2: Access keys
 Advanced security
 Access control (IAM)
 Shared access signatures (SAS)

Answer:

App1: Access keys
 Advanced security
 Access control (IAM)
 Shared access signatures (SAS)

App2: Access keys
 Advanced security
 Access control (IAM)
 Shared access signatures (SAS)

Explanation:

With Shared access signature you can limit the resources for access and at the same time can control the duration of the access.

A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data. You can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>

355. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Traffic Manager Contributor role at the subscription level to Admin1.

A. Yes

B. No

Answer: A

Explanation:

Explanation

With Traffic Manager Contributor role you can manage Traffic Manager profiles, do traffic analysis but does not let you control who has access to them.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

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

356. You have a service deployed to a Kubernetes cluster.

Another application needs to access the service via the private IP address of the pod.

Which of the following would you define as the networking type for the cluster to meet this requirement?

A. Kubenet

B. Azure container networking plugin

C. Service Endpoints

D. Network security groups

Answer: B

Explanation:

Azure container networking plugin: Correct Choice

With the Azure container networking plugin, every pod gets an IP address allocated.

With Azure CNI, every pod gets an IP address from the subnet and can be accessed directly. These IP addresses must be unique across your network space, and must be planned in advance. Each node has a configuration parameter for the maximum number of pods that it supports. The equivalent number of IP addresses per node are then reserved up front for that node. This approach requires more planning, as can otherwise lead to IP address exhaustion or the need to rebuild clusters in a larger subnet as your application demands grow.

Nodes use the Azure Container Networking Interface (CNI) Kubernetes plugin.

Kubenet : Incorrect Choice

The kubenet networking option is the default configuration for AKS cluster creation. With kubenet, nodes get an IP address from the Azure virtual network subnet. Pods receive an IP address from a logically different address space to the Azure virtual network subnet of the nodes. Service Endpoints: Incorrect Choice

Capabilities like service endpoints or UDRs are supported with both kubenet and Azure CNI, the support

policies for AKS define what changes you can make.

For example:

- If you manually create the virtual network resources for an AKS cluster, you're supported when configuring your own UDRs or service endpoints.
- If the Azure platform automatically creates the virtual network resources for your AKS cluster, it isn't supported to manually change those AKS-managed resources to configure your own UDRs or service endpoints.

Network security groups: Incorrect Choice

A network security group filters traffic for VMs, such as the AKS nodes. As you create Services, such as a LoadBalancer, the Azure platform automatically configures any network security group rules that are needed.

Reference: <https://docs.microsoft.com/en-us/azure/aks/concepts-network>

357.HOTSPOT

You have an Azure subscription that contains several virtual machines and an Azure Log Analytics workspace named Workspace1.

You create a log search query as shown in the following exhibit.



The screenshot shows the Azure Log Analytics query editor. At the top, there are buttons for 'Run', 'Time range: Set in query', 'Save', 'Copy link', 'Export', 'Set alert', and 'Pin'. The query itself is named 'Perf' and contains the following code:

```

Perf
| where ObjectName == "Processor" and CounterName == "% Processor Time"
| where TimeGenerated between (startofweek(ago(9d)) .. endofweek(ago(2d)) )
| summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)
| render timechart

```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

If you run the query on Monday, the query will return the events from the last

▼

1 days
7 days
8 days
14 days
21 days

The query results will be displayed in a

▼

table that has two columns
table that has three columns
graph that has the Computer values on the Y axis
graph that has the avg(CounterValue) values on the Y axis

Answer:

If you run the query on Monday, the query will return the events from the last

1 days
7 days
8 days
14 days
21 days

The query results will be displayed in a

table that has two columns
table that has three columns
graph that has the Computer values on the Y axis
graph that has the avg(CounterValue) values on the Y axis

Explanation:

Box 1: 14 days

Two weeks will be covered.

Note: Startofweek returns the start of the week containing the date, shifted by an offset, if provided.

Start of the week is considered to be a Sunday.

Endofweek returns the end of the week containing the date, shifted by an offset, if provided.

Last day of the week is considered to be a Saturday.

Box 2:

The render operator renders results in as graphical output. Timechart is a Line graph, where the first column is x-axis, and should be datetime. Other columns are y-axes. In this case the Y axis has avg(CounterValue) Values.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview>

https://docs-analytics-eus.azurewebsites.net/queryLanguage/query_language_renderoperator.html

358.HOTSPOT

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Resource group
VNET1	Virtual network	RG1
VNET2	Virtual network	RG2
VM1	Virtual machine	RG2

The status of VM1 is Running.

You assign an Azure policy as shown in the exhibit. (Click the Exhibit tab.)

Home > Policy - Assignments > Assign policy

Assign policy

SCOPE

* Scope (Learn more about setting the scope)

Azure Pass/RG2

Exclusions

Optionally select resources to exempt from the policy assignment

BASICS

* Policy definition

Not allowed resource types

* Assignment name ①

Not allowed resource types

Description

Assigned by

First User

PARAMETERS

* Not allowed resource types ①

3 selected

Assign

Cancel

You assign the policy by using the following parameters:

Microsoft.ClassicNetwork/virtualNetworks

Microsoft.Network/virtualNetworks

Microsoft.Compute/virtualNetworks

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 administrator can move VNET1 to RG2.	<input type="radio"/>	<input type="radio"/>
The state of VM1 changed to deallocated.	<input type="radio"/>	<input type="radio"/>
An administrator can modify the address space of VNET2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
An administrator can move VNET1 to RG2.	<input checked="" type="radio"/>	<input type="radio"/>
The state of VM1 changed to deallocated.	<input type="radio"/>	<input checked="" type="radio"/>
An administrator can modify the address space of VNET2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Not allowed resource types (Deny): Prevents a list of resource types from being deployed. This means this policy specifically prevents a list of resource types from being deployed. So that refers that except deployment all the other operations like start/stop or move etc. are not prevented. But to be noted if the resource already exists, it just marks it as non-compliant.

Replicated this scenario in LAB keeping VM running and below are the outcome:

- VM is not deallocated
- Able to stop and start VM successfully.
- Not able to create new virtual network or VM.
- Not able to modify VM size.
- Not able change the address space of the virtual network.
- Successfully moved virtual network and VM in another resource group.

Statement 1: Yes

Based on above experiment the policy will mark the VNET1 as non-compliant but it can be moved to RG2. Hence this statement is true.

Statement 2: No

Based on above experiment the policy will mark the VM as non-compliant but it will still be running, not deallocated. Hence this statement is False.

Statement 3: No

Based on above experiment the address space for VNET2 can not be modified. Hence this statement is False.

Reference: <https://docs.microsoft.com/en-us/azure/governance/policy/assign-policy-portal>

359. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company registers a domain name of contoso.com.

You create an Azure DNS zone named contoso.com, and then you add an A record to the zone for a host named www that has an IP address of 131.107.1.10.

You discover that Internet hosts are unable to resolve www.contoso.com to the 131.107.1.10 IP address.

You need to resolve the name resolution issue.

Solution: You modify the name servers at the domain registrar.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Explanation

Modify the Name Server (NS) record.

References: <https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

360.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company registers a domain name of contoso.com.

You create an Azure DNS zone named contoso.com, and then you add an A record to the zone for a host named www that has an IP address of 131.107.1.10.

You discover that Internet hosts are unable to resolve www.contoso.com to the 131.107.1.10 IP address.

You need to resolve the name resolution issue.

Solution: You modify the SOA record in the contoso.com zone.

A. Yes

B. No

Answer: B

Explanation:

Modify the NS record, not the SOA record.

Note: The SOA record stores information about the name of the server that supplied the data for the zone; the administrator of the zone; the current version of the data file; the number of seconds a secondary name server should wait before checking for updates; the number of seconds a secondary name server should wait before retrying a failed zone transfer; the maximum number of seconds that a secondary name server can use data before it must either be refreshed or expire; and a default number of seconds for the time-to live file on resource records.

References: <https://searchnetworking.techtarget.com/definition/start-of-authority-record>

361.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company registers a domain name of contoso.com.

You create an Azure DNS zone named contoso.com, and then you add an A record to the zone for a host named www that has an IP address of 131.107.1.10.

You discover that Internet hosts are unable to resolve www.contoso.com to the 131.107.1.10 IP address.

You need to resolve the name resolution issue.

Solution: You add an NS record to the contoso.com Azure DNS zone.

A. Yes

B. No

Answer: B

Explanation:

Before you can delegate your DNS zone to Azure DNS, you need to know the name servers for your zone.

The NS record set contains the names of the Azure DNS name servers assigned to the zone.

References: <https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

362. You are troubleshooting a performance issue for an Azure Application Gateway.

You need to compare the total requests to the failed requests during the past six hours.

What should you use?

A. Metrics in Application Gateway

B. Diagnostics logs in Application Gateway

C. NSG flow logs in Azure Network Watcher

D. Connection monitor in Azure Network Watcher

Answer: A

Explanation:

Application Gateway currently has seven metrics to view performance counters.

Metrics are a feature for certain Azure resources where you can view performance counters in the portal.

For Application Gateway, the following metrics are available:

You can filter on a per backend pool basis to show healthy/unhealthy hosts in a specific backend pool

References:

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gatewaydiagnostics#Metrics>

363. DRAG DROP

You have an Azure subscription that contains an Azure virtual machine named VM1. VM1 runs Windows Server 2016 and is part of an availability set.

VM1 has virtual machine-level backup enabled.

VM1 is deleted.

You need to restore VM1 from the backup. VM1 must be part of the availability set.

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

From the Restore configuration blade, set Restore Type to **Create virtual machine**.

From the VM1 blade, edit the disk settings of the OS disk.

From the Restore configuration blade, set Restore Type to **Restore disks**.

From the Recovery Services vault, deploy a template.

From the VM1 blade, add a disk.

From the Recovery Services vault, select a restore point for VM1.

Answer:

Actions

Answer Area

From the Restore configuration blade, set Restore Type to **Create virtual machine**.

From the Recovery Services vault, select a restore point for VM1.

From the VM1 blade, edit the disk settings of the OS disk.

From the Restore configuration blade, set Restore Type to **Restore disks**.

From the Restore configuration blade, set Restore Type to **Restore disks**.

From the Recovery Services vault, deploy a template.

From the Recovery Services vault, deploy a template.

From the VM1 blade, add a disk.

From the Recovery Services vault, select a restore point for VM1.

364. You have an Azure App Service plan named AdatumASP1 that uses the P2v2 pricing tier.

AdatumASP1 hosts 1 Azure web app named adatumwebapp1. You need to delegate the management of adatumwebapp1 to a group named Devs.

Devs must be able to perform the following tasks:

- Add deployment slots.
- View the configuration of AdatumASP1.
- Modify the role assignment for adatumwebapp1.

Which role should you assign to the Devs group?

- A. Owner
- B. Contributor

C. Web Plan Contributor

D. Website Contributor

Answer: A

Explanation:

Owner: Correct Choice

The Owner role lets you manage everything, including access to resources.

Contributor: Incorrect Choice

With contributor role you can Add deployment slots and View the configuration of App service plan but you can't Modify the role assignment. For this you need User Access Administrator or Owner role. So this is incorrect.

Web Plan Contributor: Incorrect Choice

The Web Plan Contributor role lets you manage the web plans for websites, but not access to them. So this option is incorrect.

Website Contributor: Incorrect Choice

The Website Contributor role lets you manage websites (not web plans), but not access to them.

So this is incorrect option.

Note:

As per least privilege principle it is not advisable to provide owner role to any group, rather you should create custom RBAC role with custom policy and use that role for this operation. However as this option is not available here so only option to go with owner role.

References:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

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

365. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure web app named App1. App1 runs in an Azure App Service plan named Plan1.

Plan1 is associated to the Free pricing tier.

You discover that App1 stops each day after running continuously for 60 minutes.

You need to ensure that App1 can run continuously for the entire day.

Solution: You change the pricing tier of Plan1 to Basic.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

The Free Tier provides 60 CPU minutes / day. This explains why App1 is stops. The Basic tier has no such cap.

References: <https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

366.HOTSPOT

You create an Azure web app named WebApp1.

WebApp1 has the autoscale settings shown in the following exhibit.

Autoscale setting name: Rule1

Resource group: VMRG

Instance count: 1

Default Auto created scale condition

Scale mode: Scale based on a metric Scale to a specific instance count

Instance count: 1

Schedule: This scale condition is executed when none of the other scale condition(s) match

Auto created scale condition 1

Scale mode: Scale based on a metric Scale to a specific instance count

Scale out

When Plan1 (Average) CpuPercentage > 80 Increase instance count by 2

Rules Scale in

When Plan1 (Average) CpuPercentage > 25 Decrease instance count by 1

[+Add a rule](#)

Instance limits: Minimum 2, Maximum 10, Default 4

Schedule: Specify start/end dates Repeat specific days

Timezone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Sto..

Start date: 2018-07-01 12:00:00 AM

End date: 2018-07-31 11:59:00 PM

The scale out and scale in rules are configured to have a duration of 10 minutes and a cool down time of five minutes.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

If on August 8, 2018, WebApp1 is used at more than 85 percent for 15 minutes, WebApp1 will be running [answer choice].

one instance
two instances
four instances
six instances
ten instances

If on July 8, 2018, WebApp1 is used at less than 15 percent for 60 minutes, WebApp1 will be running [answer choice].

one instance
two instances
three instances
four instances
six instances

Answer:

If on August 8, 2018, WebApp1 is used at more than 85 percent for 15 minutes, WebApp1 will be running [answer choice].

one instance
two instances
four instances
six instances
ten instances

If on July 8, 2018, WebApp1 is used at less than 15 percent for 60 minutes, WebApp1 will be running [answer choice].

one instance
two instances
three instances
four instances
six instances

Explanation:

Box 1: one instance

Refer to scaling condition provided in the question, August 8, 2018 is outside the schedule of the scale condition 1, and Default instance count is 1.

Box 2: two instances

The default instance count is important because autoscale scales your service to that count when metrics are not available. Therefore, select a default instance count that's safe for your workloads. The Default instance count of scale condition 1 is 4, and the Scale in rule decreases the count with 1.

So initial instance count before scale in condition met = 4

CPU utilization was at 15% for 60 mins so after first 10 mins (The scale out and scale in rules are configured to have a duration of 10 minutes) instance count reduces by 1 hence after first 10 mins instance count is 4-1=3

Now cool down period is 5 mins, after first 15 mins instance count is 3.

After next 15 mins, instance count will be 3-1=2.

After next 15 mins, instance count will be =2 because minimum instance count must be 2, it can't get reduced beyond 2.

So after 60 mins instance count will be at 2.

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-best-practices>

367.You have 100 Azure subscriptions. All the subscriptions are associated to the same Azure Active Directory (Azure AD) tenant named contoso.com.

You are a global administrator.

You plan to create a report that lists all the resources across all the subscriptions.

You need to ensure that you can view all the resources in all the subscriptions.

What should you do?

- A. From the Azure portal, modify the profile settings of your account.
- B. From Windows PowerShell, run the Add-AzureADAdministrativeUnitMember cmdlet.
- C. From Windows PowerShell, run the New-AzureADUserAppRoleAssignment cmdlet.
- D. From the Azure portal, modify the properties of the Azure AD tenant.

Answer: C

Explanation:

The New-AzureADUserAppRoleAssignment cmdlet assigns a user to an application role in Azure Active Directory (AD). Use it for the application report.

References:

<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureaduserapproleassignment?view=azureadps-2.0>

368.You have a Microsoft SQL Server Always On availability group on Azure virtual machines. You need to configure an Azure internal load balancer as a listener for the availability group.

What should you do?

- A. Enable Floating IP.
- B. Set Session persistence to Client IP and protocol.
- C. Set Session persistence to Client IP.
- D. Create an HTTP health probe on port 1433.

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sql/virtual-machines-windows-portal-sql-always-on-int-listener>

369.DRAG DROP

You have an Azure subscription that contains the following resources:

- a virtual network named VNet1
- a replication policy named ReplPolicy1
- a Recovery Services vault named Vault1
- an Azure Storage account named Storage1

You have an Amazon Web Services (AWS) EC2 virtual machine named VM1 that runs Windows Server

You need to migrate VM1 to VNet1 by using Azure Site Recovery.

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

Install Azure Site Recovery Unified Setup.

Create an Azure Migrate project.

Enable Windows PowerShell remoting on VM1.

Deploy an EC2 virtual machine as a configuration server.

Enable replication for VM1.

Answer:

Actions

Answer Area

Install Azure Site Recovery Unified Setup.

Deploy an EC2 virtual machine as a configuration server.

Create an Azure Migrate project.

Install Azure Site Recovery Unified Setup.

Enable Windows PowerShell remoting on VM1.

Enable replication for VM1.

Deploy an EC2 virtual machine as a configuration server.

Enable replication for VM1.

Explanation:

Step 1: Deploy an EC2 virtual machine as a configuration server

Prepare source include:

Step 2: Install Azure Site Recovery Unified Setup.

Download Microsoft Azure Site Recovery Unified Setup. You can download it to your local machine and

then copy it to the VM you're using as the configuration server.

Step 3: Enable replication for VM1.

Enable replication for each VM that you want to migrate. When replication is enabled, Site Recovery automatically installs the Mobility service.

References: <https://docs.microsoft.com/en-us/azure/site-recovery/migrate-tutorial-aws-azure>

370. You deploy an Azure Application Gateway.

You need to ensure that all the traffic requesting <https://adatum.com/internal> resources is directed to an internal server pool and all the traffic requesting <https://adatum.com/external> resources is directed to an external server pool.

What should you configure on the Application Gateway?

- A. URL path-based routing
- B. multi-site listeners
- C. basic routing
- D. SSL termination

Answer: A

Explanation:

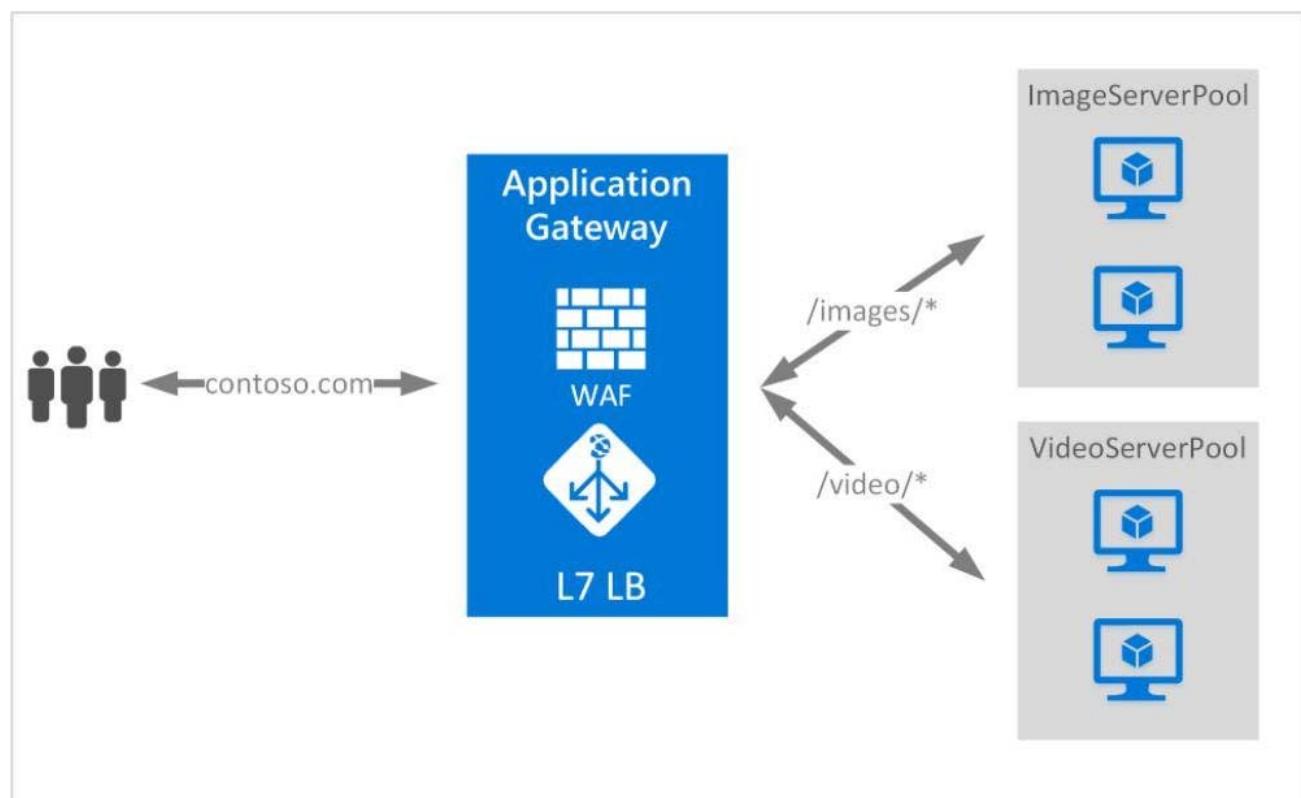
URL Path Based Routing allows you to route traffic to back-end server pools based on URL Paths of the request.

In the question there are two different path from where the traffic is getting generated as below

<https://adatum.com/internal>

<https://adatum.com/external>

So in this case we can use URL path-based routing feature of Application Gateway.



Reference: <https://docs.microsoft.com/en-us/azure/application-gateway/url-route-overview>

371. You are building a custom Azure function app to connect to Azure Event Grid.

You need to ensure that resources are allocated dynamically to the function app. Billing must be based on the executions of the app.

What should you configure when you create the function app?

- A. the Windows operating system and the Consumption plan hosting plan
- B. the Windows operating system and the App Service plan hosting plan
- C. the Docker container and an App Service plan that uses the B1 pricing tier
- D. the Docker container and an App Service plan that uses the S1 pricing

Answer: A

Explanation:

Azure Functions runs in two different modes: Consumption plan and Azure App Service plan. The Consumption plan automatically allocates compute power when your code is running. Your app is scaled out when needed to handle load, and scaled down when code is not running.

372. You have an Azure web app named App1 that streams video content to users. App1 is located in the East US Azure region.

Users in North America stream the video content without any interruption.

Users in Asia and Europe report that the video buffer often and do not play back smoothly.

You need to recommend a solution to improve video streaming to the European and Asian users.

What should you recommend?

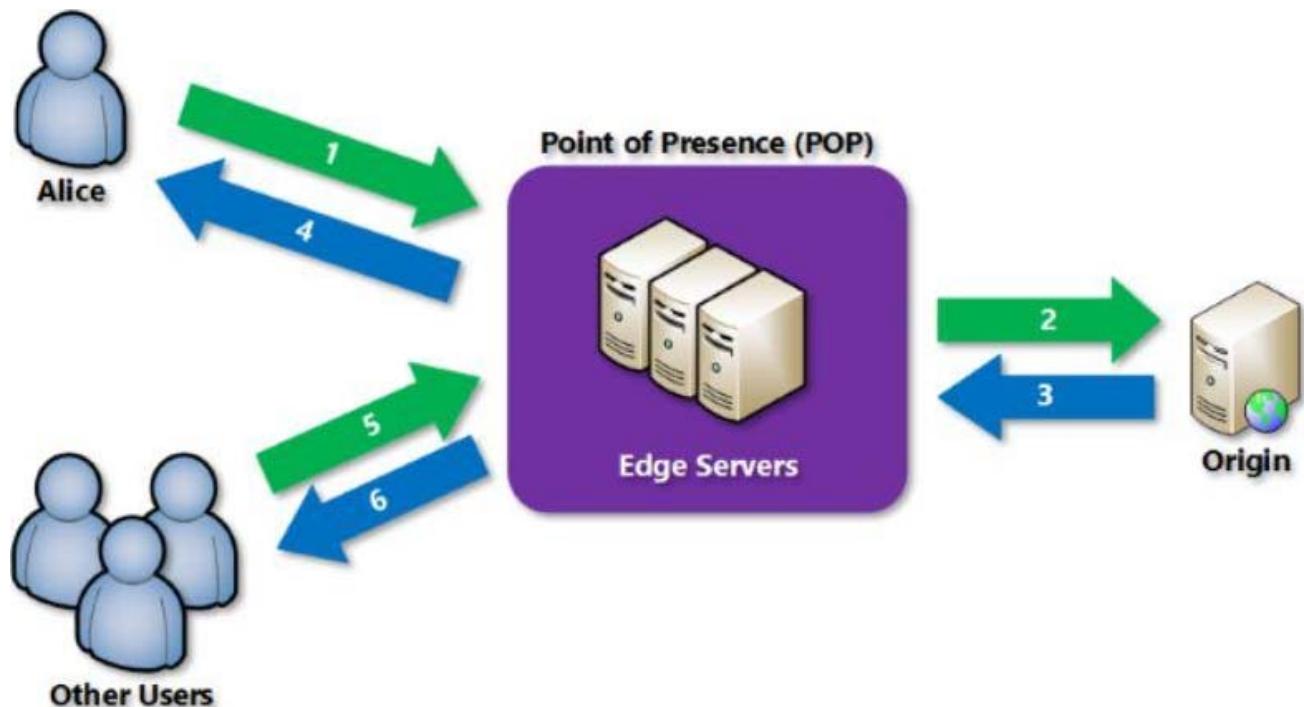
- A. Scale out the App Service plan.
- B. Scale up the App Service plan.
- C. Configure an Azure Content Delivery Network (CDN) endpoint.
- D. Configure Azure File Sync.

Answer: C

Explanation:

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs' store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world.



Reference: <https://docs.microsoft.com/en-us/azure/cdn/cdn-overview>

373.HOTSPOT

You have an Azure web app named App1 that has two deployment slots named Production and Staging. Each slot has the unique settings shown in the following table.

Setting	Production	Staging
Web sockets	Off	On
Custom domain name	App1-prod.contoso.com	App1-staging.contoso.com

You perform a slot swap.

What are the configurations of the Production slot after the swap? To answer, select the appropriate options in the answer area. NOTE: Each correction is worth one point.

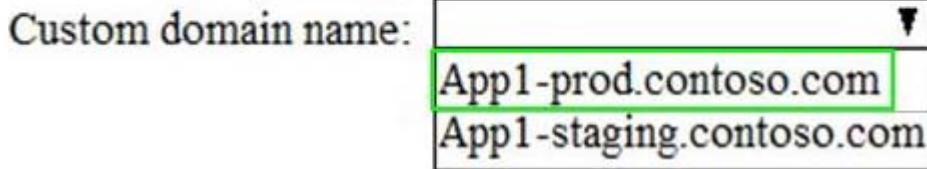
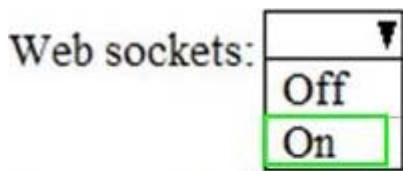
Web sockets:

Off
On

Custom domain name:

App1-prod.contoso.com
App1-staging.contoso.com

Answer:



Explanation:

Which settings are swapped?

When you clone configuration from another deployment slot, the cloned configuration is editable.

Some configuration elements follow the content across a swap (not slot specific), whereas other configuration elements stay in the same slot after a swap (slot specific). The following lists show the settings that change when you swap slots.

Box 1: On

Settings that are swapped:

General settings, such as framework version, 32/64-bit, web sockets

App settings (can be configured to stick to a slot)

Connection strings (can be configured to stick to a slot)

Handler mappings

Public certificates

WebJobs content

Hybrid connections *

Virtual network integration *

Service endpoints *

Azure Content Delivery Network *

Features marked with an asterisk (*) are planned to be unswapped.

So web sockets settings will be swapped. So Production will have web sockets settings from "Off" to "On" after the swap slot.

Box 2: App1-prod.contoso.com

Settings that aren't swapped:

Publishing endpoints

Custom domain names

Non-public certificates and TLS/SSL settings

Scale settings

WebJobs schedulers

IP restrictions

Always On

Diagnostic settings

Cross-origin resource sharing (CORS)

So Custom domain names will not be swapped. So Production will have Custom domain names of its own after the swap slot.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots#what-happens-during-a-swap>

374. You have an Azure subscription that contains a virtual network named VNet1. VNet 1 has two subnets named Subnet1 and Subnet2. VNet1 is in the West Europe Azure region.

The subscription contains the virtual machines in the following table.

Name	Connected to
VM1	Subnet1
VM2	Subnet1
VM3	Subnet2

You need to deploy an application gateway named AppGW1 to VNet1.

What should you do first?

- A. Add a service endpoint.
- B. Add a virtual network.
- C. Move VM3 to Subnet1.
- D. Stop VM1 and VM2.

Answer: D

Explanation:

If you have an existing virtual network, either select an existing empty subnet or create a new subnet in your existing virtual network solely for use by the application gateway.

Verify that you have a working virtual network with a valid subnet. Make sure that no virtual machines or cloud deployments are using the subnet. The application gateway must be by itself in a virtual network subnet.

References:

<https://social.msdn.microsoft.com/Forums/azure/en-US/b09367f9-5d01-4cda-9127-b7a506a0a151/cant-create-application-gateway?forum=WAVirtualMachinesVirtualNetwork>

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-create-gateway>

375. A web developer creates a web application that you plan to deploy as an Azure web app. Users must enter credentials to access the web application.

You create a new web app named WebApp1 and deploy the web application to WebApp1.

You need to disable anonymous access to WebApp1.

What should you configure?

- A. Access control (IAM)
- B. Advanced Tools
- C. Deployment credentials
- D. Authentication/Authorization

Answer: D

Explanation:

Anonymous access is an authentication method. It allows users to establish an anonymous connection.

References:

<https://docs.microsoft.com/en-us/biztalk/core/guidelines-for-resolving-iis-permissions-problems>

376. HOTSPOT

You have an Azure subscription named Subscription1 that contains the resources in the following table.

Name	Type
VM1	Virtual machine
VM2	Virtual machine
AppGW1	Application gateway

VM1 and VM2 run the websites in the following table.

Name	Host header
Default	Not applicable
Web1	Site1.contoso.com
Web2	Site2.contoso.com

AppGW1 has the backend pools in the following table.

Name	Virtual machines
Pool1	VM1
Pool2	Vm2

DNS resolves site1.contoso.com, site2.contoso.com, and site3.contoso.com to the IP address of AppGW1.

AppGW1 has the listeners in the following table.

Name	Protocol	Associated rule	Host name
Listener1	HTTP	Not applicable	Site1.contoso.com
Listener2	HTTP	Rule2	Site2.contoso.com
Listener3	HTTP	Rule3	Not applicable

AppGW1 has the rules in the following table.

Name	Type	Listener	Backend pool
Rule2	Basic	Listener2	Pool1
Rule3	Basic	Listener3	Pool2

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 browse to site1.contoso.com from the Internet, you will be directed to VM1.	<input type="radio"/>	<input type="radio"/>
If you browse to site2.contoso.com from the Internet, you will be directed to VM1.	<input type="radio"/>	<input type="radio"/>
If you browse to site3.contoso.com from the Internet, you will be directed to VM1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If you browse to site1.contoso.com from the Internet, you will be directed to VM1.	<input type="radio"/>	<input checked="" type="radio"/>
If you browse to site2.contoso.com from the Internet, you will be directed to VM1.	<input checked="" type="radio"/>	<input type="radio"/>
If you browse to site3.contoso.com from the Internet, you will be directed to VM1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Vm1 is in Pool1. Rule2 applies to Pool1, Listener 2, and site2.contoso.com

377.Your company has a main office in Australia and several branch offices in Asia.

The company's data center uses a VMware virtualization infrastructure to host several virtualized servers.

You purchase an Azure subscription and plan to move all virtual machines to Azure to a resource group in the Australia Southeast location.

You need to create an Azure Migrate migration project.

Which geography should you select?

- A. Central India
- B. Australia Central
- C. Australia Southeast
- D. United States

Answer: C

Explanation:

In Project Details, specify the project name, and geography in which you want to create the project.

Review supported geographies for public and government clouds.

Add a tool

Migrate project Select assessment tool Select migration tool Review + add tool(s)

A migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project.

* Subscription

* Resource group
Create new

PROJECT DETAILS

Specify the name of the migrate project and the preferred geography.

* Migrate project

* Region

References: <https://docs.microsoft.com/en-us/azure/migrate/how-to-add-tool-first-time>

378.HOTSPOT

You have an Azure web app named WebApp1.

You need to provide developers with a copy of WebApp1 that they can modify without affecting the production WebApp1. When the developers finish testing their changes, you must be able to switch the current live version of WebApp1 to the new version.

Which command should you run prepare the environment? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

-ResourceGroupName AdatumWebApps -Name WebApp1 -AppServicePlan ADatumASPl

New-AzureRmWebApp

New-AzureRmWebAppBackup

New-AzureRMWebAppSlot

Switch-AzureRmWebAppSlot

-WebApp1 -Slot Staging

-AseName

-DefaultProfile

-SourceWebApp

Answer:

-ResourceGroupName AdatumWebApps -Name WebApp1 -AppServicePlan ADatumASPl

New-AzureRmWebApp

New-AzureRmWebAppBackup

New-AzureRMWebAppSlot

Switch-AzureRmWebAppSlot

-WebApp1 -Slot Staging

-AseName

-DefaultProfile

-SourceWebApp

Explanation:

Box 1: New-AzureRmWebAppSlot

The New-AzureRmWebAppSlot cmdlet creates an Azure Web App Slot in a given a resource group that uses the specified App Service plan and data center.

Box 2: -SourceWebApp

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.websites/new-azurermwebappslot>

379.DRAG DROP

You are configuring serverless computing in Azure.

You need to receive an email message whenever a resource is created in or deleted from a resource group.

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

Create an Azure Event Grid trigger

Create an Azure Service Bus namespace

Create conditions and actions

Create an Azure Logic App

Create an event subscription

Answer Area

Answer:

Actions

Create an Azure Event Grid trigger

Create an Azure Service Bus namespace

Create conditions and actions

Create an Azure Logic App

Create an event subscription

Answer Area

Create an Azure Logic App

Create an Azure Event Grid trigger

Create conditions and actions

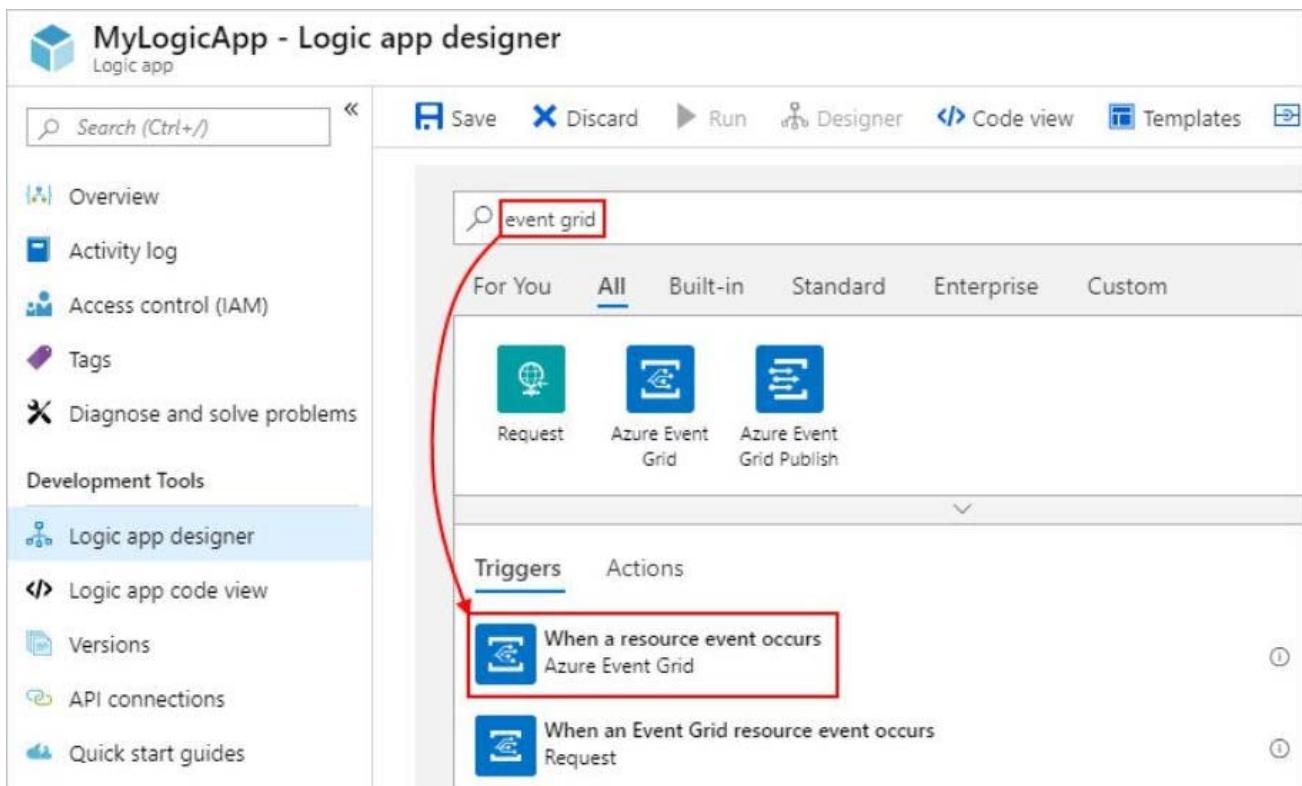
Explanation:

Action 1: Create an Azure Logic App

The screenshot shows the Microsoft Azure portal interface. On the left, a vertical sidebar menu is open, with the 'Create a resource' option highlighted by a red box. The main content area is titled 'New' and shows the 'Azure Marketplace' with a search bar. The 'Featured' tab is selected. A red box highlights the 'Integration' category in the list of services. The 'Logic App' service is also highlighted with a red box and a red arrow points from the 'Integration' box to it. The 'Logic App' card includes a 'Quickstart tutorial' link. Other services listed include API Management, Service Bus, Integration Account, Integration Service Environment, Logic Apps Custom Connector, and Data Factory, each with a 'Quickstart tutorial' link.

Service	Quickstart tutorial
Logic App	Quickstart tutorial
API Management	Quickstart tutorial
Service Bus	Quickstart tutorial
Integration Account	Quickstart tutorial
Integration Service Environment	Learn more
Logic Apps Custom Connector	Learn more
Data Factory	Quickstart tutorial

Action 2: Create an Azure Event Grid Trigger



The screenshot shows the Azure Logic App designer interface for a logic app named "MyLogicApp". The left sidebar lists various development tools, with "Logic app designer" selected. The main area shows a search bar with "event grid" typed in, a list of triggers, and a selected trigger highlighted with a red box.

MyLogicApp - Logic app designer

Search (Ctrl+ /)

Save Discard Run Designer Code view Templates

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Development Tools

Logic app designer (selected)

Logic app code view Versions API connections Quick start guides

event grid

For You All Built-in Standard Enterprise Custom

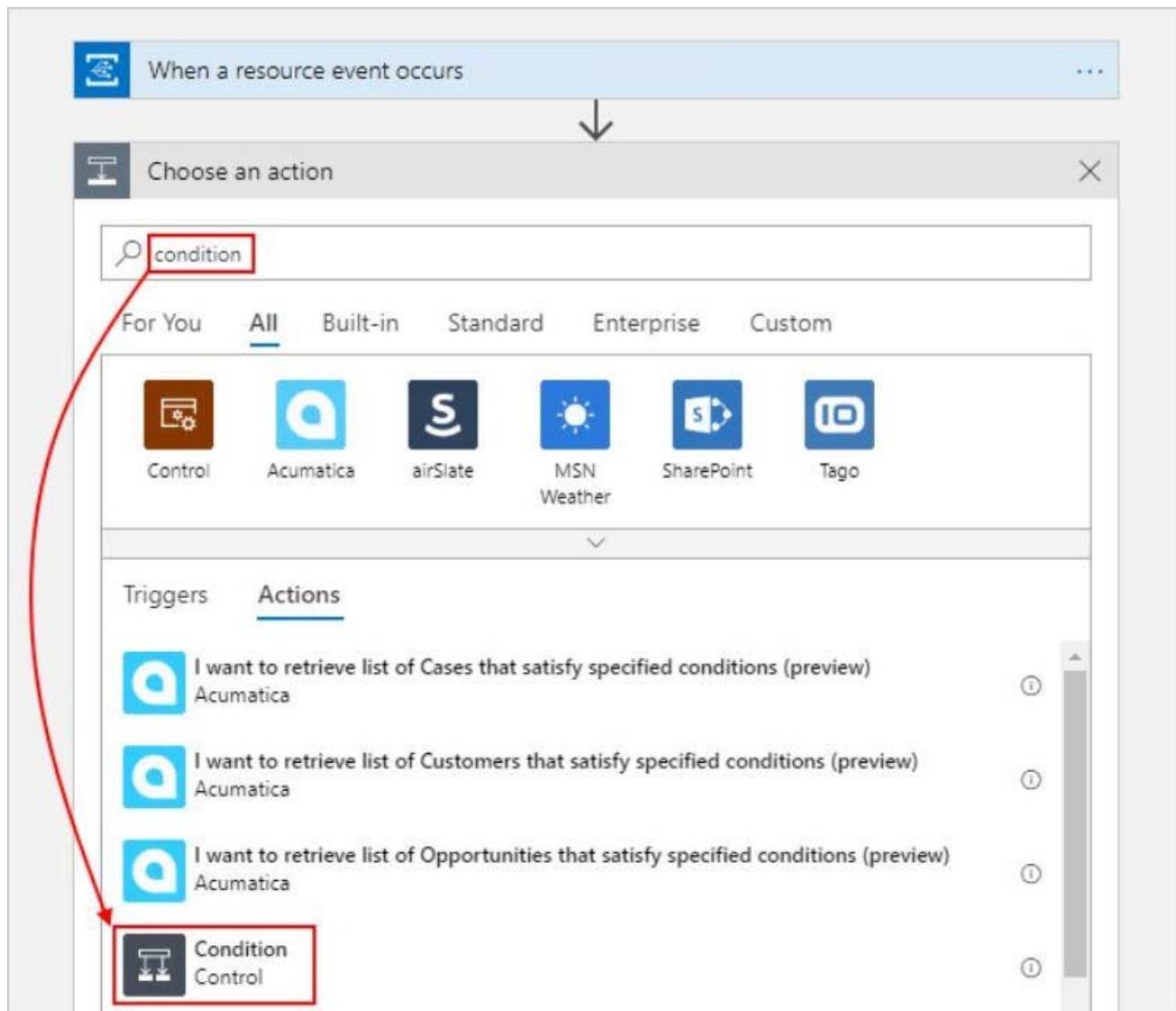
Request Azure Event Grid Azure Event Grid Publish

Triggers Actions

When a resource event occurs Azure Event Grid

When an Event Grid resource event occurs Request

Action 3: Create conditions and actions



References:

<https://docs.microsoft.com/en-us/azure/event-grid/monitor-virtual-machine-changes-event-grid-logic-app>

380.DRAG DROP

You have an Azure subscription that contains an Azure Service Bus named Bus1.

Your company plans to deploy two Azure web apps named App1 and App2.

The web apps will create messages that have the following requirements:

- Each message created by App1 must be consumed by only a single consumer
- Each message created by App2 will be consumed by multiple consumers.

Which resource should you create for each web app? To answer, drag the appropriate resources to the correct web apps. Each resource 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.

Resource	Answer Area
A Service Bus queue	App1
An Azure Event Grid topic	App2
A Service Bus topic	
Azure Blob storage	

Answer:

Resource	Answer Area
A Service Bus queue	App1
An Azure Event Grid topic	App2
A Service Bus topic	
Azure Blob storage	

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions>

381.HOTSPOT

You have an Azure Service Bus.

You create a queue named Queue1.

Queue1 is configured as shown in the following exhibit.

* Name 

Queue1

Max queue size

1 GB

Message time to live 

Days	Hours	Minutes	Seconds
0	2	0	0

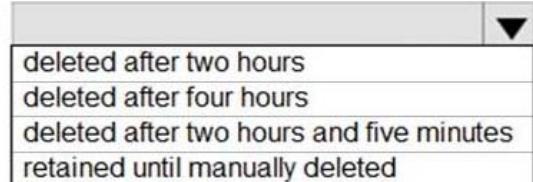
Lock duration 

Days	Hours	Minutes	Seconds
0	0	5	0

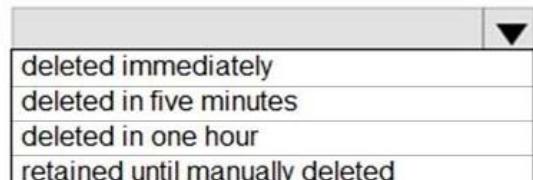
 Enable duplicate detection  Enable dead lettering on message expiration  Enable sessions  Enable partitioning 

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

If a message that has a TTL of four hours is written to Queue1 and is never read, the message will be

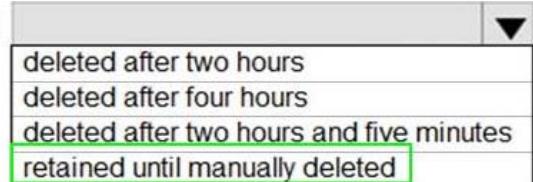
 deleted after two hours
deleted after four hours
deleted after two hours and five minutes
retained until manually deleted

If a message that has a TTL of two hours is written to Queue1, and then read after one hour, the message will be

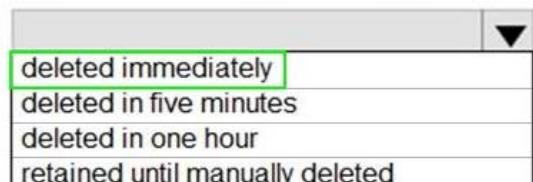
 deleted immediately
deleted in five minutes
deleted in one hour
retained until manually deleted

Answer:

If a message that has a TTL of four hours is written to Queue1 and is never read, the message will be

 deleted after two hours
deleted after four hours
deleted after two hours and five minutes
retained until manually deleted

If a message that has a TTL of two hours is written to Queue1, and then read after one hour, the message will be

 deleted immediately
deleted in five minutes
deleted in one hour
retained until manually deleted

Explanation:

Box 1: retained until manually deleted

Since by default PeekLock shall be enabled in Queue, so it will move to DeadLetter after 2hours and stays there until manually deleted. Messages in the dead letter queue should be deleted manually.

Box 2: deleted immediately

Once a message is pulled, it will be deleted immediately. It does not make sense to keep the message further 5 minutes "locked" in the queue. Locking the message makes sense, for the case, when processing the message from a receiver, to lock the message, to avoid processing/receiving the message simultaneously by another receiver.

The receiving client initiates settlement of a received message with a positive acknowledgment when it calls Complete at the API level. This indicates to the broker that the message has been successfully processed and the message is removed from the queue or subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/message-expiration>

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/message-transfers-locks-settlement>

382. You are configuring Azure Active Directory (AD) Privileged Identity Management.

You need to provide a user named Admm1 with read access to a resource group named RG1 for only one month.

The user role must be assigned immediately.

What should you do?

- A. Assign an active role.
- B. Assign an eligible role.
- C. Assign a permanently active role.
- D. Create a custom role and a conditional access policy.

Answer: B

Explanation:

Azure AD Privileged Identity Management introduces the concept of an eligible admin. Eligible admins should be users that need privileged access now and then, but not all-day, every day. The role is inactive until the user needs access, then they complete an activation process and become an active admin for a predetermined amount of time.

References: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

383. You have an Azure App Service plan named AdatumASP1 that hosts several Azure web apps.

You discover that the web apps respond slowly.

You need to provide additional memory and CPU resources to each instance of the web apps.

What should you do?

- A. Add continues WebJob that use the multi-instance scale
- B. Scale out AdatumASP1
- C. Add a virtual machine scale set
- D. Scale up AdatumASP1

Answer: D

Explanation:

Scale up: Correct Choice

Scale up: Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more. You scale up by changing the pricing tier of the App Service plan that your app belongs to. Scale out : Incorrect Choice

Scale out: Increase the number of VM instances that run your app. You can scale out to as many as 30 instances, depending on your pricing tier. App Service Environments in Isolated tier further increases your scale-out count to 100 instances. For more information about scaling out, see Scale instance count manually or automatically.

Add continuous WebJobs: Incorrect Choice

WebJobs is a feature of Azure App Service that enables you to run a program or script in the same instance as a web app, API app, or mobile app. Add continuous WebJobs will Starts immediately when the WebJob is created. To keep the job from ending, the program or script typically does its work inside an endless loop. If the job does end, you can restart it. Starts only when triggered manually or on a schedule.

Add a virtual machine scale set: Incorrect Choice

A virtual machine scale set allows you to deploy and manage a set of identical, autoscaling virtual machines. You can scale the number of VMs in the scale set manually. You can also define rules to autoscale based on resource usage such as CPU, memory demand, or network traffic. It will not increase the slowness of the apps.

References:

<https://docs.microsoft.com/en-us/azure/app-service/manage-scale-up>

<https://docs.microsoft.com/en-us/azure/app-service/webjobs-create#webjob-types>

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/app-service/web-sites-scale.md>

384. You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Cluster1	Azure Kubernetes Service (AKS)
Registry1	Azure Container Registry
Application1	Container image

You need to deploy Application1 to Cluster1.

Which command should you run?

- A. az acr build
- B. az aks create
- C. docker build
- D. kubectl apply

Answer: A

385. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log

on VM1 within an hour.

Solution: You create an Azure storage account and configure shared access signatures (SASs). You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the storage account as the source.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

386.HOTSPOT

You have the App Service plans shown in the following table.

Name	Operating system	Location
ASP1	Windows	West US
ASP2	Windows	Central US
ASP3	Linux	West US

You plan to create the Azure web apps shown in the following table.

Name	Runtime stack	Location
WebApp1	.NET Core 3.0	West US
WebApp2	ASP.NET 4.7	West US

You need to identify which App Service plans can be used for the web apps.

What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

WebApp1:

ASP1 only

ASP3 only

ASP1 and ASP2 only

ASP1 and ASP3 only

ASP1, ASP2, and ASP3

WebApp2:

ASP1 only

ASP3 only

ASP1 and ASP2 only

ASP1 and ASP3 only

ASP1, ASP2, and ASP3

Answer:

WebApp1:

ASP1 only
ASP3 only
ASP1 and ASP2 only
ASP1 and ASP3 only
ASP1, ASP2, and ASP3

WebApp2:

ASP1 only
ASP3 only
ASP1 and ASP2 only
ASP1 and ASP3 only
ASP1, ASP2, and ASP3

Explanation:

Box 1: ASP1 ASP3

Asp1, ASP3: ASP.NET Core apps can be hosted both on Windows or Linux.

Not ASP2: The region in which your app runs is the region of the App Service plan it's in.

Box 2: ASP1

ASP.NET apps can be hosted on Windows only.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/quickstart-dotnetcore?pivots=platform-linux><https://docs.microsoft.com/en-us/azure/app-service/app-service-plan-manage#>**387.HOTSPOT**

You have an Azure Kubernetes Service (AKS) cluster named AKS1 and a computer named Computer1 that runs Windows 10. Computer1 that has the Azure CLI installed.

You need to install the kubectl client on Computer1.

Which command should you run? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

az
docker
msiexec.exe
Install-Module

aks
/package
-name
pull

Install-cli

Answer:

az	▼
docker	
msiexec.exe	
Install-Module	

aks	▼
/package	
-name	
pull	

Install-cli

Explanation:

To install kubectl locally, use the az aks install-cli command:

az aks install-cli

Reference: <https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

388.DRAG DROP

You onboard 10 Azure virtual machines to Azure Automation State Configuration.

You need to use Azure Automation State Configuration to manage the ongoing consistency of the virtual machine configurations.

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. NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Answer Area

Assign tags to the virtual machines

Check the compliance status of the node

Compile a configuration into a node configuration

Upload a configuration to Azure Automation State Configuration

Create a management group

Answer:

Actions	Answer Area
Assign tags to the virtual machines	Upload a configuration to Azure Automation State Configuration
Check the compliance status of the node	Compile a configuration into a node configuration
Compile a configuration into a node configuration	Assign tags to the virtual machines
Upload a configuration to Azure Automation State Configuration	
Create a management group	

Explanation:

Step 1: Upload a configuration to Azure Automation State Configuration.

Import the configuration into the Automation account.

Step 2: Compile a configuration into a node configuration.

A DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

Step 3: Assign the node configuration

Step 4: Check the compliance status of the node

Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node. On the blade for an individual report, you can see the following status information for the corresponding consistency check:

The report status — whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant"

Reference: <https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

389. You have an Azure Resource Manager template named Template1 that is used to deploy an Azure virtual machine.

Template1 contains the following text:

```

"location": {
  "type": "String",
  "defaultValue": "eastus",
  "allowedValues": [
    "canadacentral",
    "eastus",
    "westeurope",
    "westus" ]
}
  
```

The variables section in Template1 contains the following text:

"location": "westeurope"

The resources section in Template1 contains the following text:

```
"type": "Microsoft.Compute/virtualMachines",
"apiVersion": "2018-10-01",
"name": "[variables('vmName')]",
"location": "westeurope",
```

You need to deploy the virtual machine to the West US location by using Template1.

What should you do?

- A. Modify the location in the resource section to westus
- B. Select West US during the deployment
- C. Modify the location in the variables section to westus

Answer: A

390. You plan to move a distributed on-premises app named App1 to an Azure subscription.

After the planned move, App1 will be hosted on several Azure virtual machines.

You need to ensure that App1 always runs on at least eight virtual machines during planned Azure maintenance.

What should you create?

- A. one virtual machine scale set that has 10 virtual machines instances
- B. one Availability Set that has three fault domains and one update domain
- C. one Availability Set that has 10 update domains and one fault domain
- D. one virtual machine scale set that has 12 virtual machines instances

Answer: C

Explanation:

An update domain is a logical group of underlying hardware that can undergo maintenance or be rebooted at the same time. As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these update domains. This approach ensures that at least one instance of your application always remains running as the Azure platform undergoes periodic maintenance.

Reference: <http://www.thatlazyadmin.com/azure-fault-update-domains/>