vce trainer



Reference Solution for AZ-103.88q

AZ-103

AZ-103

Microsoft Azure Administrator

Score: 800/1000

Version:

Licensed to Berend Post berend.post@it-university.nl

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Manage Azure subscriptions and resources

(12 questions)

Question 1

You have an Azure Active Directory (Azure AD) tenant 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?

- ☒ From the Directory role blade, modify the directory role.
- ☐ From the Licenses blade, assign a new license.
- ☐ From the Groups blade, invite the user account to a new group.

Explanation:

Explanation:

Assign a role to a user

Sign in to the Azure portal with an account that's a global admin or privileged role admin for the directory.

Select Azure Active Directory, select Users, and then select a specific user from the list.

For the selected user, select Directory role, select Add role, and then pick the appropriate admin roles from the Directory roles list, such as Conditional access administrator.

Press Select to save.

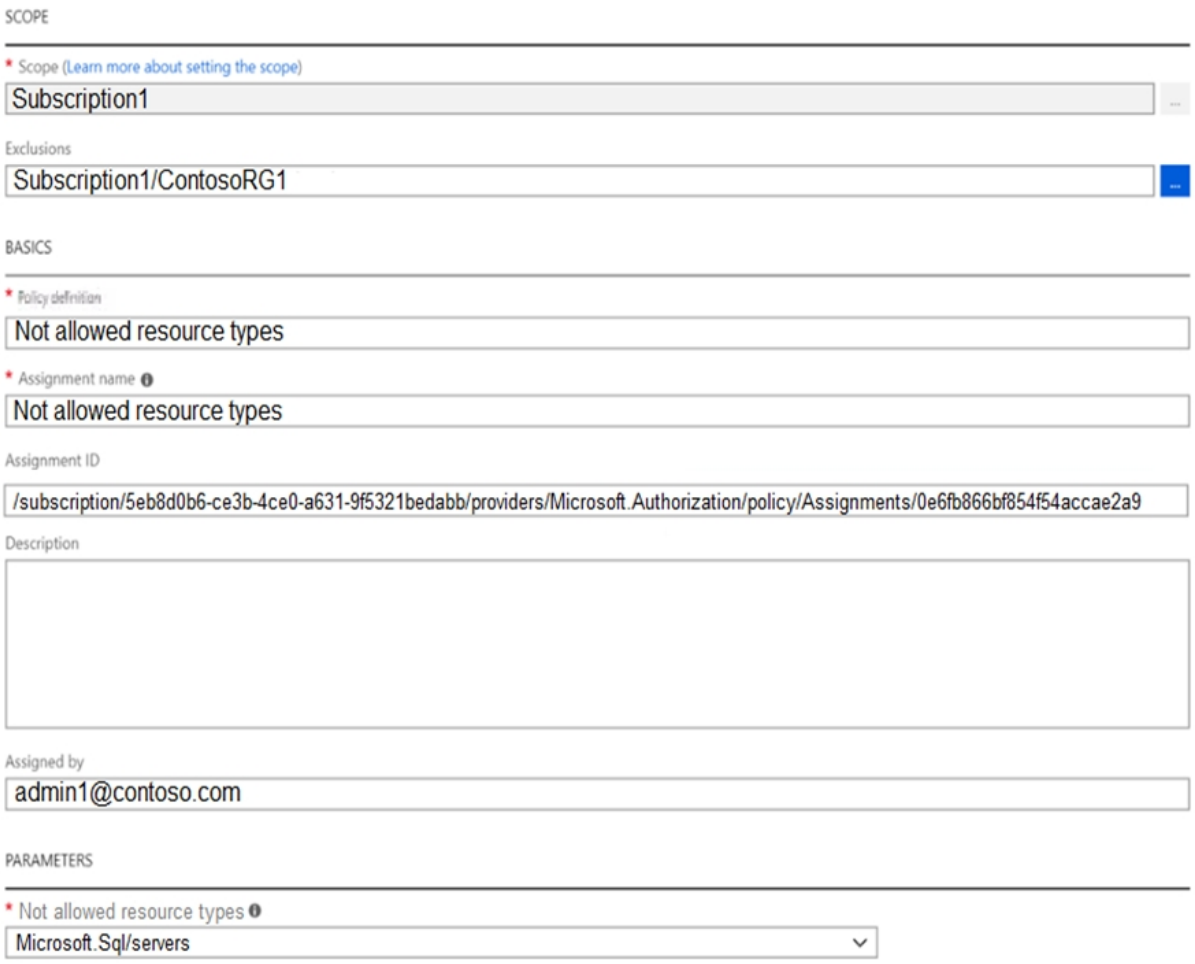
References:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

Licensed to Berend Post berend.post@it-university.nl

Question 2

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



What is the effect of the policy?

- ☐ You are prevented from creating Azure SQL Servers in ContosoRG1 only.
- ☒ You can create Azure SQL servers in ContosoRG1 only.
- ☐ You can create Azure SQL servers in any resource group within Subscription1.
- ☐ You are prevented from creating Azure SQL servers anywhere in Subscription1.

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 3

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

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

You 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?

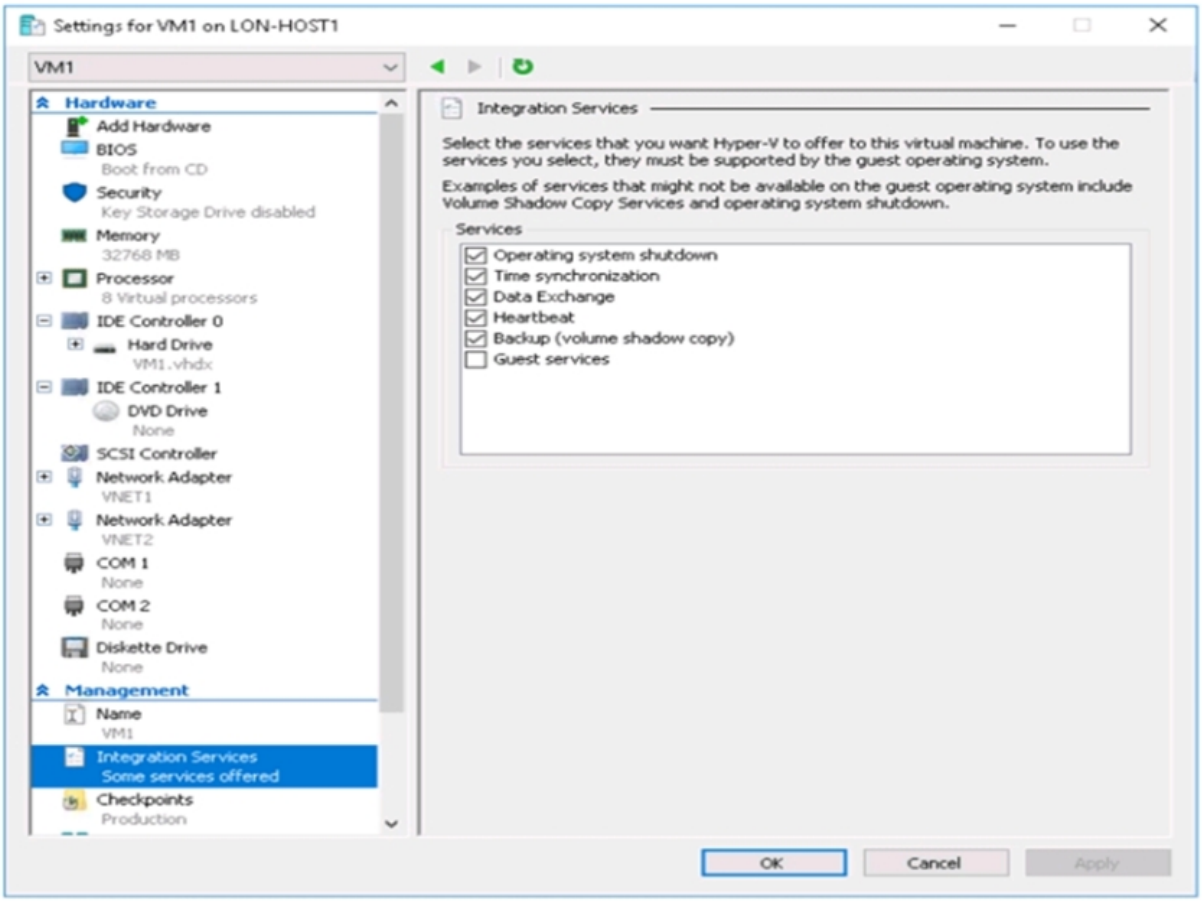
- ☐ Yes
- ☒ No

Licensed to Berend Post berend.post@it-university.nl

Question 4

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 tab.)



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?

- ☒ the hard drive
- ☐ the processor
- ☐ the network adapters
- ☐ the memory
- ☐ Integration Services

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

can convert a generation 1 VM from the VHDX file system to VHD and from a dynamically expanding disk to fixed-sized.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image?toc=%2fazure%2fvirtual-machines%2fwindows%2ftoc.json

Question 5

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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

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

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

Licensed to Berend Post berend.post@it-university.nl

Question 6

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?

- ☐ Configure locks for the virtual machine.
- ☐ Add an extension to the virtual machines.
- ☒ Assign tags to the virtual machines.
- ☐ Modify the inventory settings of the virtual machine.

Explanation:

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

Question 7

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?

- ☐ Yes
- ☒ No

Licensed to Berend Post berend.post@it-university.nl

Question 8

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?

- ☐ The App Service plan for WebApp1 moves to North Europe. Policy2 applies to WebApp1.
- ☒ The App Service plan for WebApp1 remains in West Europe. Policy2 applies to WebApp1.
- ☐ The App Service plan for WebApp1 moves to North Europe. Policy1 applies to WebApp1.
- ☐ The App Service plan for WebApp1 remains in West Europe. Policy1 applies to WebApp1.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 9

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?

- ☐ the Azure portal
- ☐ the DNS Manager console
- ☐ Azure PowerShell
- ☒ Azure CLI

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 10

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?

- ☐ Get-Event Event | where ($_.EventType –eq "error")
- ☐ Get-Event Event | where ($_.EventType == "error")
- ☐ search in (Event) * | where EventType –eq "error"
- ☒ search in (Event) "error"
- ☐ select *from Event where EventType == "error"
- ☐ Event | where EventType is "error"

Explanation:

Explanation:

To search a term in a specific table, add in (table-name) just after the search operator

References:

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/search-queries

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal

Question 11

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?

- ☐ Yes
- ☒ No

Licensed to Berend Post berend.post@it-university.nl

Question 12

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?

- ☒ Yes
- ☐ No

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Case Study (2 questions)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an AllInformation tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Humongous Insurance is an insurance company that has three offices in Miami, Tokyo and Bangkok. Each office has 5,000 users.

Existing Environment
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.

 Licensed to Berend Post berend.post@it-university.nl

Licensing Issue
You attempt to assign a license in Azure to several users and receive the following error message: "Licenses not assigned. License assignment 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.

 Licensed to Berend Post berend.post@it-university.nl

Question 13

You need to resolve the Active Directory issue.

What should you do?

- ☒ Run the IdFix tool then use the Update actions.
- ☐ From Active Directory Domains and Trusts, modify the list of UPN suffixes.
- ☐ From Azure AD Connect, modify the outbound synchronization rule.
- ☐ From Active Directory Users and Computers, select the user accounts and then modify the UPN suffix value.

Explanation:

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

Question 14

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

What should you do?

- ☒ From the Groups blade, invite the user accounts to a new group.
- ☐ From the Profile blade, modify the usage location.
- ☐ From the Directory role blade, modify the directory role.

Explanation:

Explanation:

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

Scenario: Licensing Issue

Licensed to Berend Post berend.post@it-university.nl

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.

Licensed to Berend Post berend.post@it-university.nl

Implement and manage storage

(9 questions)

Question 15

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?

- ☐ Create a new backup policy.
- ☐ Configure the extensions for VM3 and VM4.
- ☐ Create a storage account.
- ☒ Create a new Recovery Services vault.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 16

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 answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Explanation:

Explanation:

D: 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

Navigate to the storage account you want to secure.

Click on the settings menu called Firewalls and virtual networks.

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'.

Click Save to apply your changes.

E: Grant access from a Virtual Network

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

Licensed to Berend Post berend.post@it-university.nl

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

Question 17

You create an Azure Storage account named contosostorage.

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 outbound port should you open between the home computers and the data file share?

- ☐ 80
- ☐ 443
- ☒ 445
- ☐ 3389

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 18

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 driveset CSV file
- ☐ a JSON configuration file
- ☐ a PowerShell PS1 file
- ☐ an XML manifest file
- ☒ a dataset CSV file

Explanation:

Explanation:

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

E: 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

Question 19

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, delete the backup data.
- ☐ Modify the disaster recovery properties of each virtual machine.
- ☒ From the Recovery Service vault, stop the backup of each backup item.
- ☐ Modify the locks of each virtual machine.

Explanation:

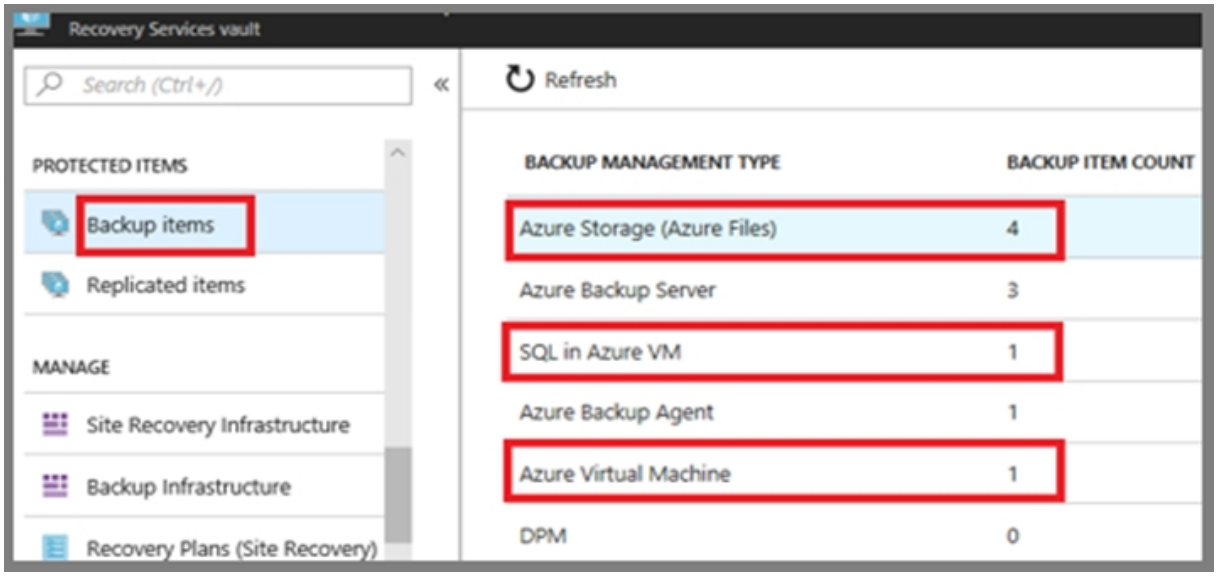
Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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.



Reference:

https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault

Licensed to Berend Post berend.post@it-university.nl

Question 20

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.

NOTE: Each correct selection is worth one point.

- ☐ Download an automation script.
- ☒ Register Server1.
- ☒ Create a sync group.
- ☐ Create a container instance.
- ☒ Install the Azure File Sync agent on Server1.

Explanation:

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 (B): 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

Licensed to Berend Post berend.post@it-university.nl

Question 21

SIMULATION

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g, copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

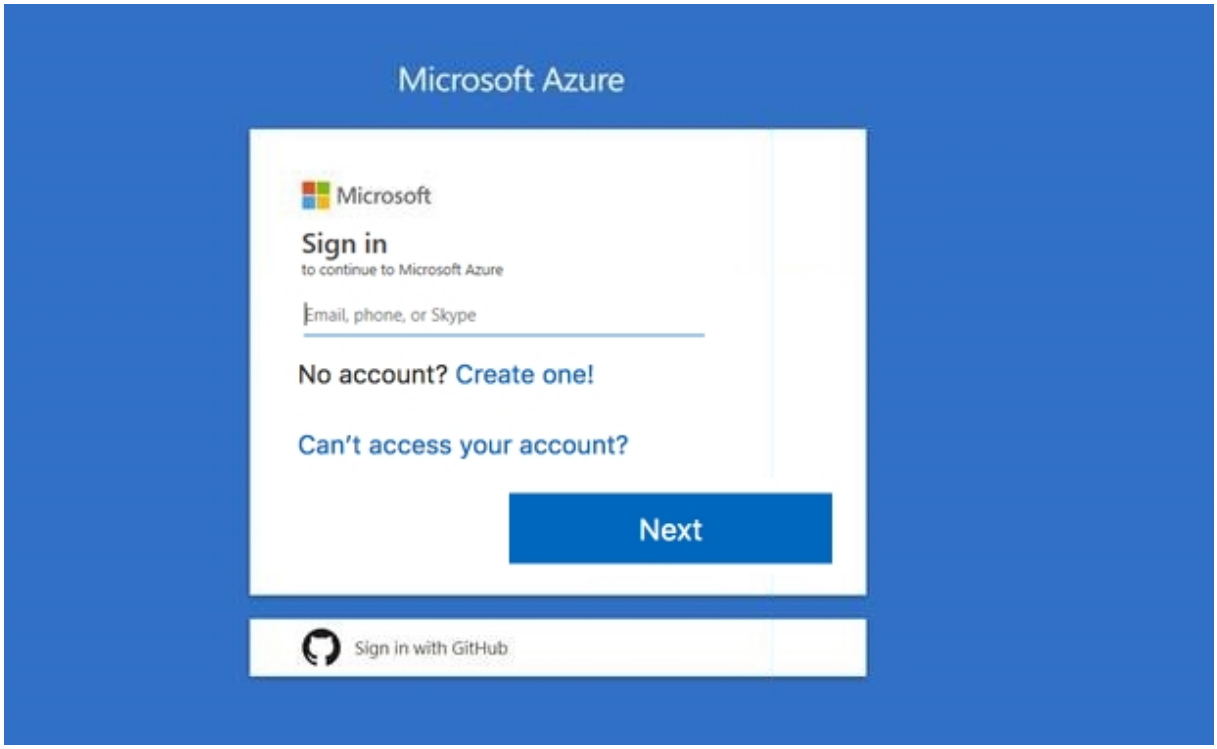
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

You may now click next to proceed to the lab.

Use the following login credentials as needed:

Azure Username: XXXXXXX
Azure Password: XXXXXXX
The following information is for technical support purposes only:
Lab Instance: 9172796

Licensed to Berend Post berend.post@it-university.nl



You recently created a virtual machine named Web01.

You need to attach a new 80-GB standard data disk named Web01-Disk1 to Web01.

What should you do from the Azure portal?

Explanation:

Explanation:

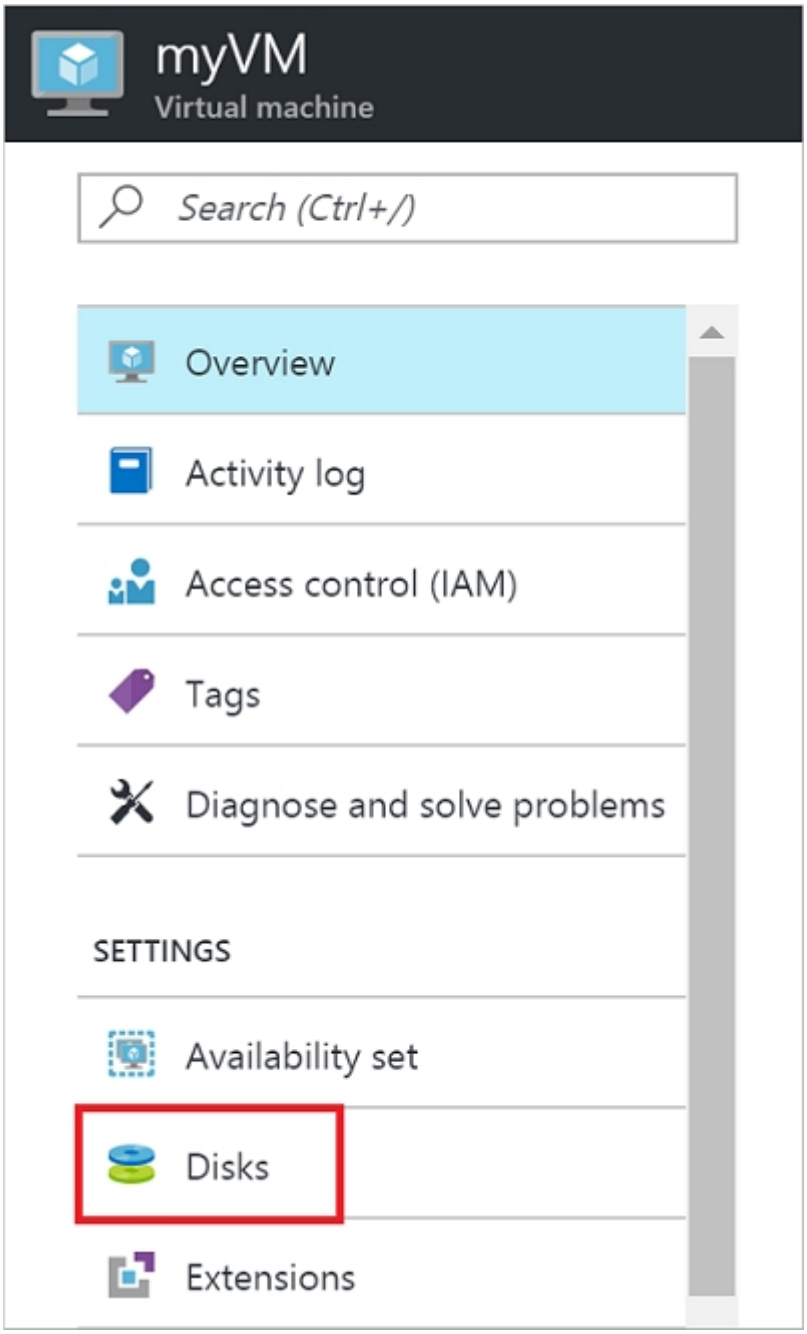
Add a data disk

Step 1: In the Azure portal, from the menu on the left, select Virtual machines.

Step 2: Select the Web01 virtual machine from the list.

Step 3: On the Virtual machine page, , in Essentials, select Disks.

Licensed to Berend Post berend.post@it-university.nl

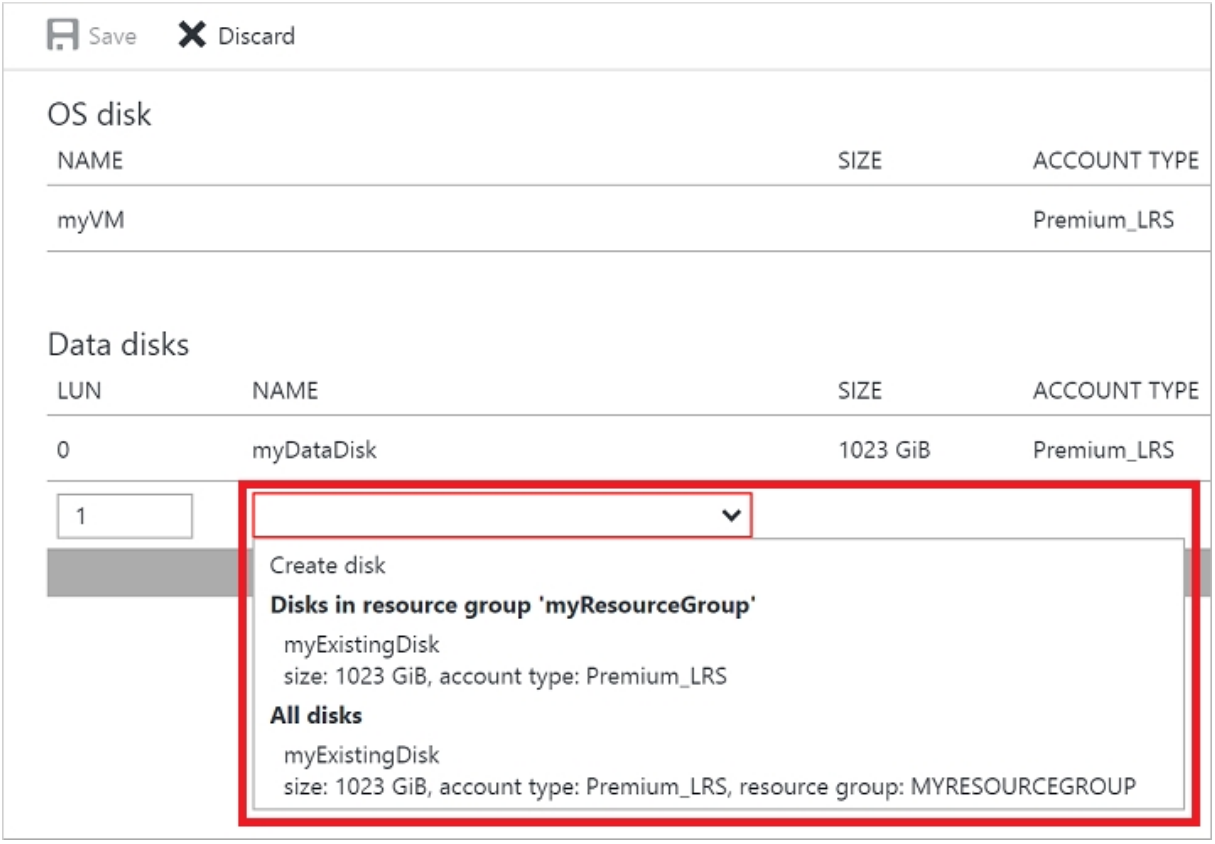


Step 4: On the Disks page, select the Web01-Disk1 from the list of existing disks.

Step 5: In the Disks pane, click + Add data disk.

Step 6: Click the drop-down menu for Name to view a list of existing managed disks accessible to your Azure subscription. Select the managed disk Web01-Disk1 to attach:

Licensed to Berend Post berend.post@it-university.nl



References:

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/attach-disk-portal

Question 22

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?

- ☒ From the VM2 blade, click Disaster recovery, click Replication settings, and then select RSV2 as the Recovery Services vault.
- ☐ From the RSV2 blade, click Backup. From the Backup blade, select the backup for the virtual machine, and then click Backup.
- ☐ From the RSV1 blade, click Backup Jobs and export the VM2 job.
- ☐ From the RSV1 blade, click Backup items and stop the VM2 backup.

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm

Licensed to Berend Post berend.post@it-university.nl

Question 23

HOTSPOT

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

Minimize 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 ]
```

Solution:

Answer Area

```
az storage account create -g RG1 -n storageaccount1
--kind [ BlobStorage | Storage | StorageV2 ]  --sku [ Standard_GRS | Standard_LRS | Standard_RAGRS | Premium_LRS ]
```

Explanation:

Explanation:

Box 1: StorageV2

Licensed to Berend Post berend.post@it-university.nl

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.

Incorrect Answers:

Locally-redundant storage (LRS): A simple, low-cost replication strategy. Data is replicated within a single storage scale unit.

Read-access geo-redundant storage (RA-GRS): Cross-regional replication with read access to the replica. RA-GRS provides read-only access to the data in the secondary location, in addition to geo-replication across two regions, but is more expensive compared to GRS.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

Licensed to Berend Post berend.post@it-university.nl

Case Study (2 questions)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an AllInformation tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a 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

Licensed to Berend Post berend.post@it-university.nl

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 passwprds 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 admin for 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.

Question 24

You need to move the blueprint files to Azure.

What should you do?

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

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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

Question 25

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

What should you create first?

- ☐ a recovery plan
- ☒ a Recovery Services vault
- ☐ an Azure Backup Server
- ☐ a backup policy

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

Licensed to Berend Post berend.post@it-university.nl

Deploy and manage virtual machines (VMs)

(13 questions)

Question 26

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.

- ☒ Modify the extensionProfile section of the Azure Resource Manager template.
- ☐ Create an automation account.
- ☐ Upload a configuration script.
- ☒ Create a new virtual machine scale set in the Azure portal.
- ☐ Create an Azure policy.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 27

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?

- ☐ Add the Puppet Agent extension.
- ☒ Change the size to D8s v3.
- ☐ Add a 500-GB managed disk.
- ☐ Attach an additional network interface.

Explanation:

Explanation:

While resizing the VM it must be in a stopped state.

References:

https://azure.microsoft.com/en-us/blog/resize-virtual-machines/

Question 28

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?

- ☐ metric alert
- ☐ Azure Log Analytics workspace
- ☐ virtual machine
- ☒ virtual machine extension

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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

Incorrect Answers:

B: Azure Log Analytics workspace is 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

Question 29

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?

- ☐ Container1
- ☒ RG1
- ☐ VM1
- ☐ Storage2

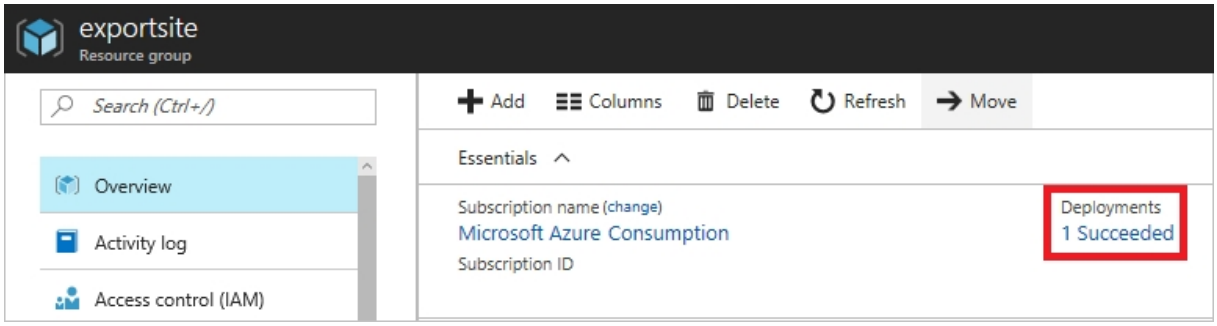
Explanation:

Explanation:

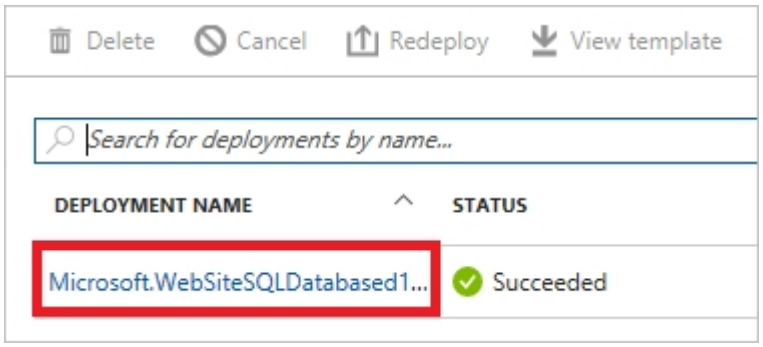
View template from deployment history

1. Go to the resource group for your new resource group. Notice that the portal shows the result of the last deployment. Select this link.

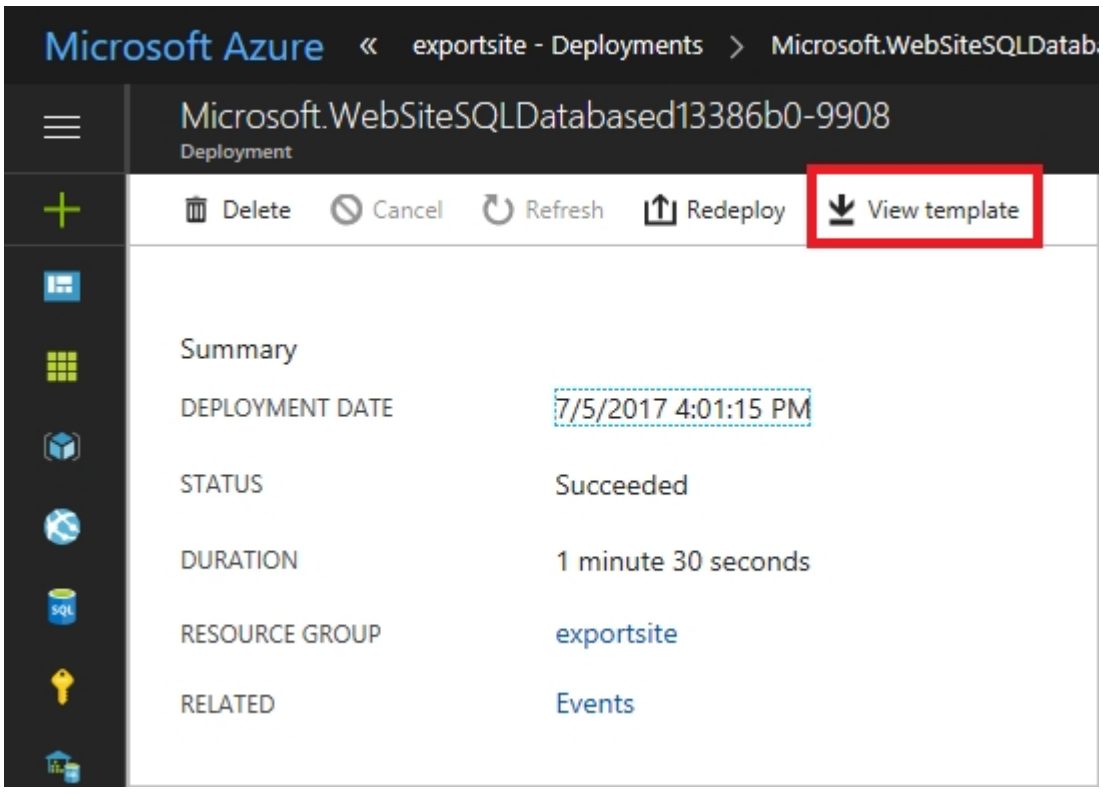
Licensed to Berend Post berend.post@it-university.nl



2. You see a history of deployments for the group. In your case, the portal probably lists only one deployment. Select this deployment.



3. 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.



Licensed to Berend Post berend.post@it-university.nl

References:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template

Question 30

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?

- ☐ Delete the Recovery Services vault.
- ☐ Delete the storage account.
- ☐ Stop the backup
- ☒ Modify the backup policy.

Explanation:

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.

Incorrect Answers:

B: 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.

References:

https://azure.microsoft.com/en-in/updates/azure-vm-backup-policy-management/

Licensed to Berend Post berend.post@it-university.nl

Question 31

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?

- ☒ the AzurePerformanceDiagnostics extension
- ☐ Azure HDInsight
- ☐ Linux Diagnostic Extension (LAD) 3.0
- ☐ Azure Analysis Services

Explanation:

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-monitoring

Licensed to Berend Post berend.post@it-university.nl

Question 32

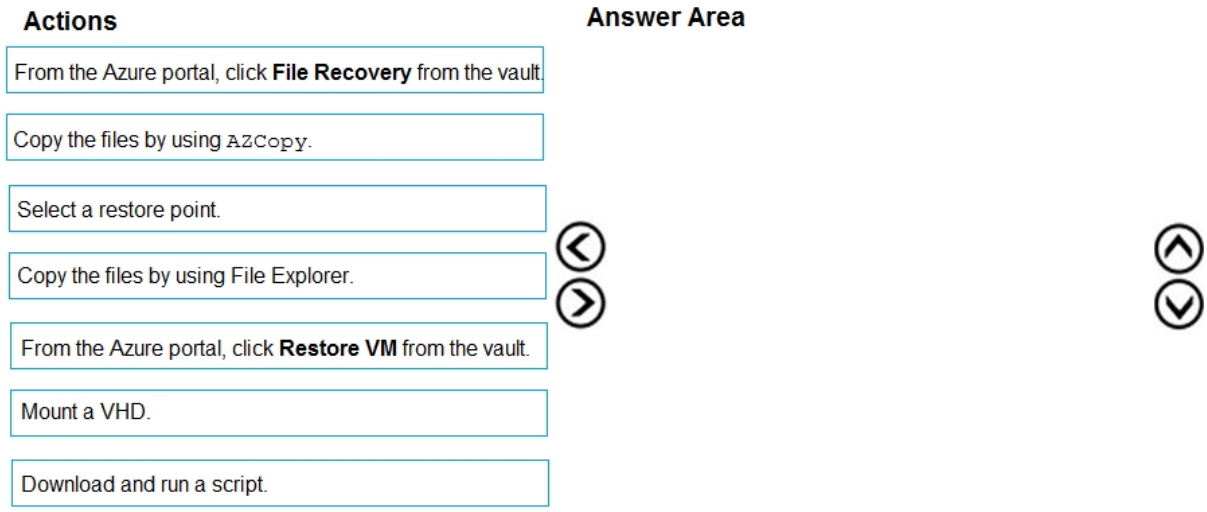
DRAG DROP

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

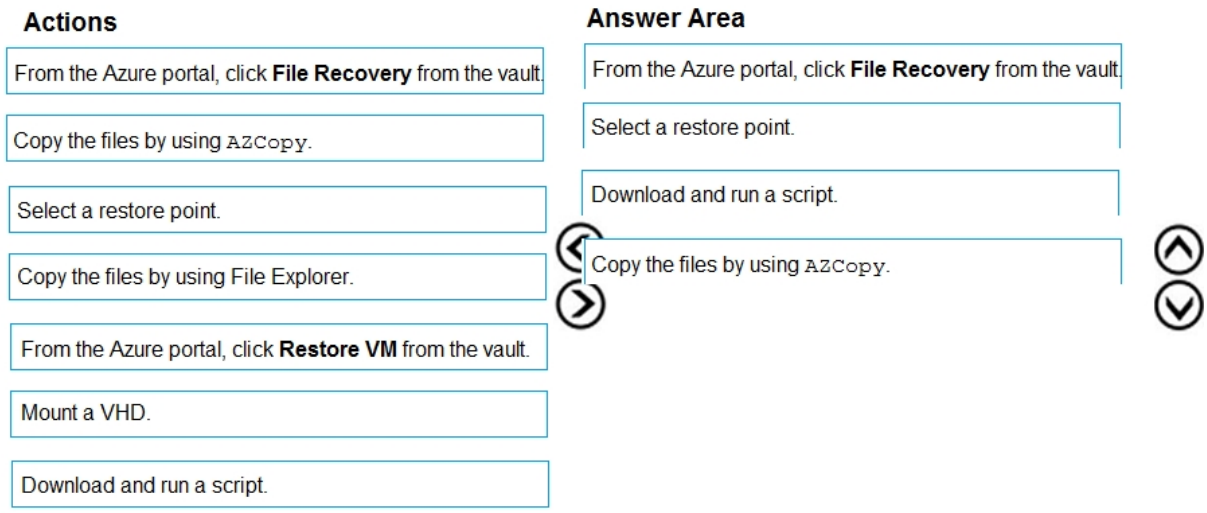
One week ago, two files were deleted from the virtual machine.

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.



Solution:



Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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

Licensed to Berend Post berend.post@it-university.nl

Question 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 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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

You would need to redeploy the VM.

References:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node

Question 34

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?

- ☒ From Microsoft Azure Storage Explorer, view the Account Management properties.
- ☐ From the Azure portal, configure the Advisor recommendations.
- ☐ From Azure Cost Management, view Advisor Recommendations.
- ☐ From Azure Cost Management, view Cost Analysis.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

https://cloud.netapp.com/blog/reduce-azure-storage-costs

Question 35

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 machine	West US
VNET2	Virtual machine	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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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

Question 36

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?

- ☒ an Azure Key Vault and an access policy
- ☐ a Recovery Services vault and a backup policy
- ☐ Azure Active Directory (AD) Identity Protection and an Azure policy
- ☐ an Azure Storage account and an access policy

Explanation:

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/

Licensed to Berend Post berend.post@it-university.nl

Question 37

SIMULATION

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g, copy and paste, ability to navigate to external websites) will not be possible by design.

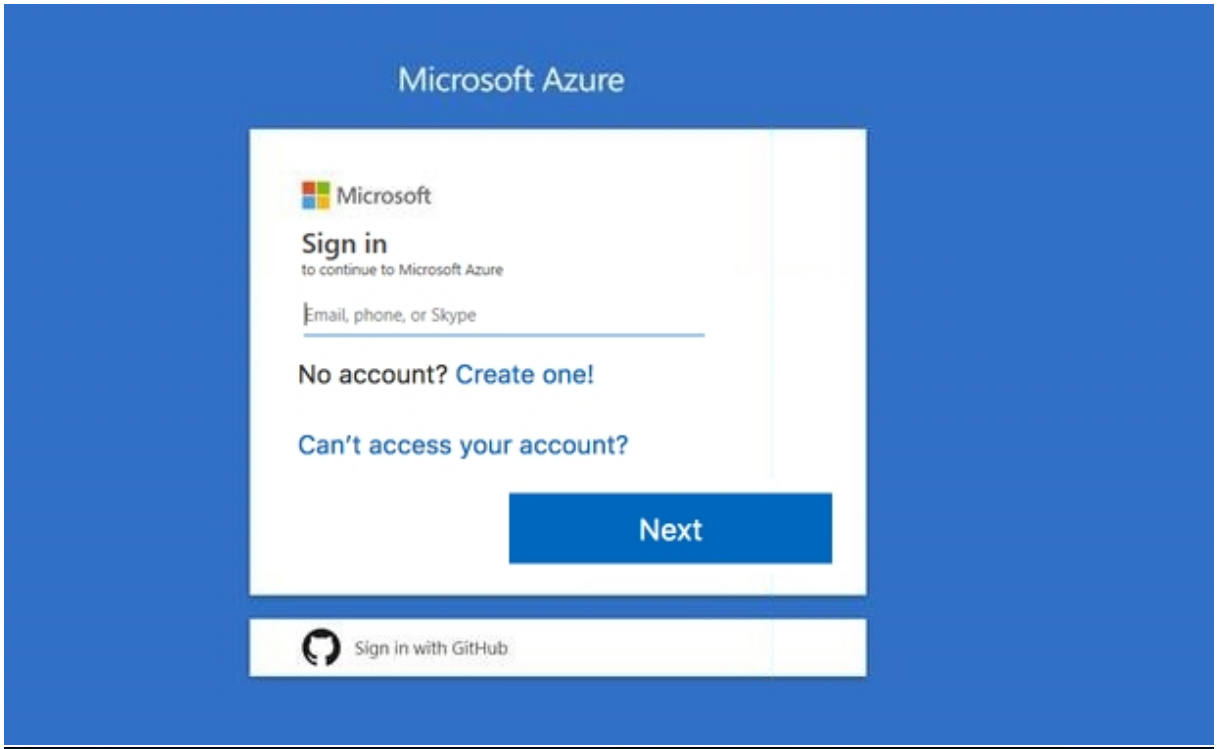
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

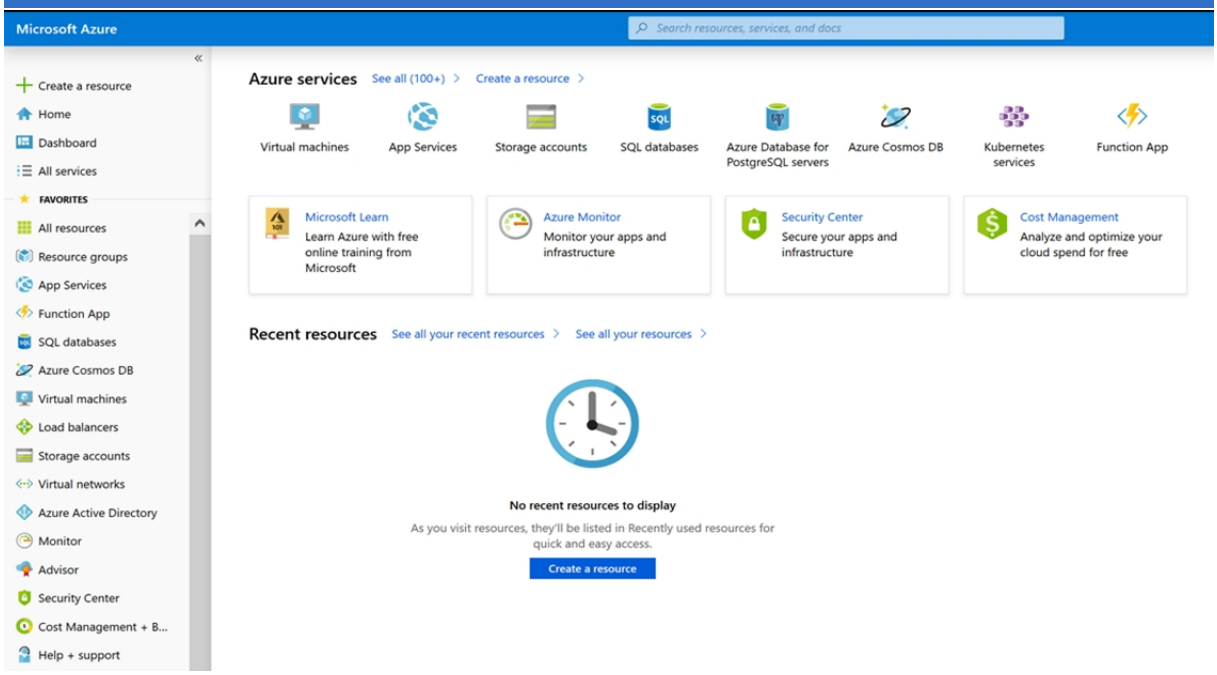
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

You may now click next to proceed to the lab.

Licensed to Berend Post berend.post@it-university.nl





You need to deploy an Azure virtual machine named VM1004a based on an Ubuntu Server image, and then configure VM1004a to meet the following requirements:

The virtual machine must contain data disks that can store at least 15 TB of data.
The data disks must be able to provide at least 2.000 IOPS.
Storage costs must be minimized.

What should you do from the Azure portal?

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Step 1: Open the Azure portal.

Step 2: On the left menu, select All resources. You can sort the resources by Type to easily find your images.

Step 3: Select the image you want to use from the list. The image Overview page opens.

Step 4: Select Create VM from the menu.

Step 5: Enter the virtual machine information.

Select VM1004a as the name for the first Virtual machine.

The user name and password entered here will be used to log in to the virtual machine. When complete, select OK. You can create the new VM in an existing resource group, or choose Create new to create a new resource group to store the VM.

Step 6: Select a size for the VM. To see more sizes, select View all or change the Supported disk type filter.

To meet the requirements select Standard SSD E70.

Standard SSD E70: Up to 16 TB, IOPS up to 4000, $1,228.80/month

Standard SSD Managed Disks, a low-cost SSD offering, are optimized for test and entry-level production workloads requiring consistent latency.

Step 7: Under Settings, make changes as necessary and select OK.

Step 8: On the summary page, you should see your image name listed as a Private image. Select Ok to start the virtual machine deployment.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-vm-generalized-managed

Licensed to Berend Post berend.post@it-university.nl

Question 38

You plan to back up an Azure virtual machine named VM1.

You discover that the Backup Pre-Check status displays a status of Warning.

What is a possible cause of the Warning status?

- ☐ VM1 is stopped.
- ☒ VM1 does not have the latest version of WaAppAgent.exe installed.
- ☐ VM1 has an unmanaged disk.
- ☐ A Recovery Services vault is unavailable.

Explanation:

Explanation:

The Warning state indicates one or more issues in VM's configuration that might lead to backup failures and provides recommended steps to ensure successful backups. Not having the latest VM Agent installed, for example, can cause backups to fail intermittently and falls in this class of issues.

References:

https://azure.microsoft.com/en-us/blog/azure-vm-backup-pre-checks/

Licensed to Berend Post berend.post@it-university.nl

Case Study (1 questions)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an AllInformation tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview

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

The 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 Contoso are hosted on-premises.

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

Existing Environment

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

Contoso 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.

Licensed to Berend Post berend.post@it-university.nl

Contoso.com contains a user named User1.

All the offices connect by using private links.

Contoso 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

Contoso 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

Contoso 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

Contoso 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.
Ensure 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.contoso.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.

Licensed to Berend Post berend.post@it-university.nl

Minimize costs whenever possible.

Question 39

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?

- ☐ Diagram in VNet1
- ☐ the security recommendations in Azure Advisor
- ☐ Diagnostic settings in Azure Monitor
- ☐ Diagnose and solve problems in Traffic Manager profiles
- ☒ IP flow verify in Azure Network Watcher

Explanation:

Explanation:

Scenario: Contoso 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

Licensed to Berend Post berend.post@it-university.nl

Configure and manage virtual networks

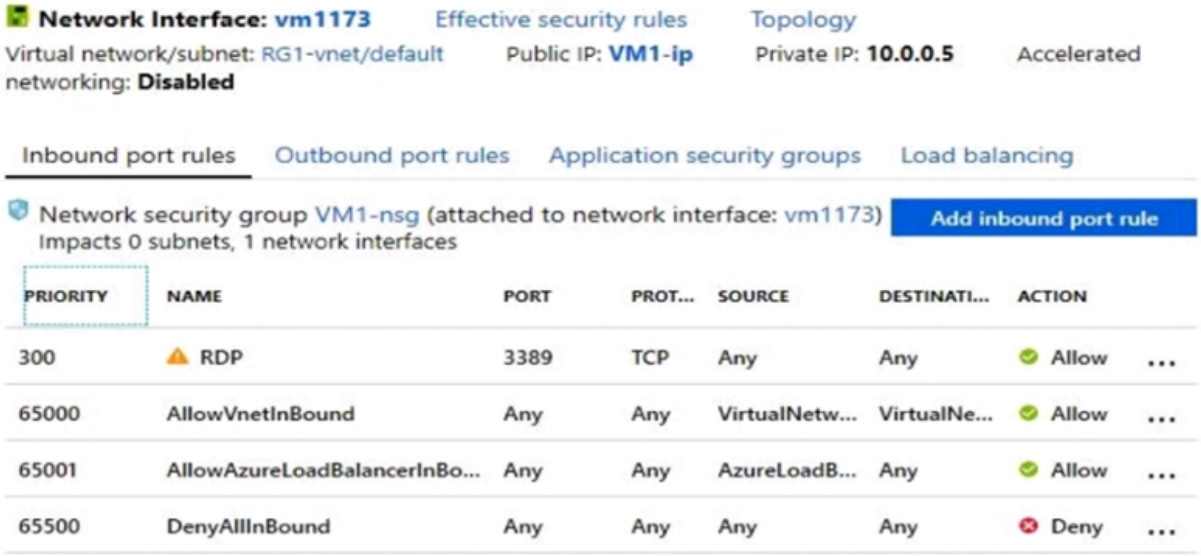
(32 questions)

Question 40

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 tab.)



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?

- ☐ Change the priority of the RDP rule.
- ☐ Attach a network interface.
- ☐ Delete the DenyAllInBound rule.
- ☒ Start VM1.

Explanation:

Explanation:

Incorrect Answers:

A: 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. RDP already has the lowest number and thus the highest priority.

Licensed to Berend Post berend.post@it-university.nl

B: The network interface has already been added to VM.

C: The Outbound rules are fine.

Reference:

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

Question 41

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?

- ☐ Protocol to UDP
- ☐ Session persistence to None
- ☒ Session persistence to Client IP
- ☐ Idle Time-out (minutes) to 20

Explanation:

Explanation:

You can set the sticky session in load balancer rules with setting the session persistence as the client IP.

References:

https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/

Licensed to Berend Post berend.post@it-university.nl

Question 42

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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

Use the Connection Monitor feature of Azure Network Watcher.

References:

https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/

Licensed to Berend Post berend.post@it-university.nl

Question 43

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?

- ☐ 1
- ☐ 3
- ☒ 4
- ☐ 12

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 44

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 VNet1 to an on-premises computer.

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

NOTE: Each correct selection is worth one point.

- ☐ Reset GW1.
- ☒ Create a route-based virtual network gateway.
- ☒ Delete GW1.
- ☐ Add a public IP address space to VNet1.
- ☐ Add a connection to GW1.
- ☐ Add a service endpoint to VNet1.

Explanation:

Explanation:

B: 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).

C: 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.

Incorrect Answers:

D: Point-to-Site connections do not require a VPN device or a public-facing IP address.

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 45

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?

- ☐ Move VM1 to Subscription2.
- ☐ Modify the IP address space of VNet2.
- ☒ Provision virtual network gateways.
- ☐ Move VNet1 to Subscription2.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

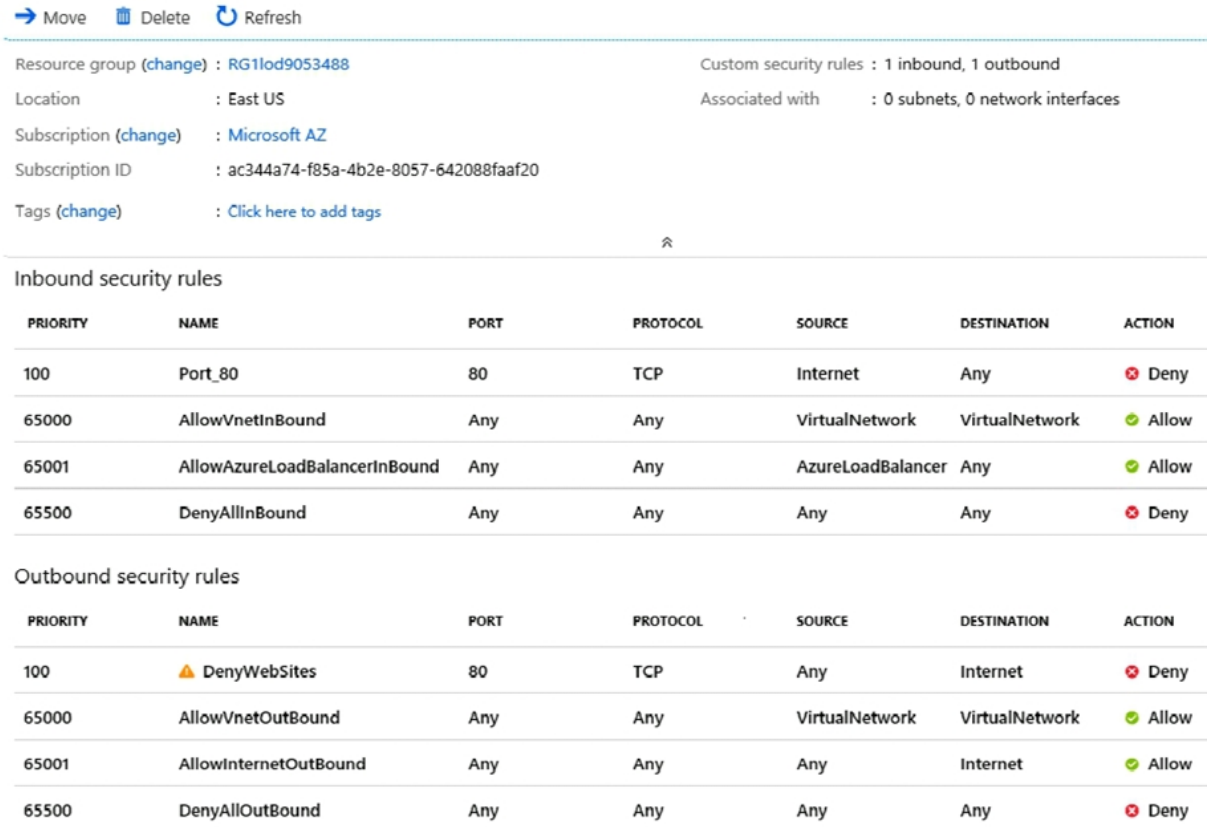
Question 46

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

Name	Type	Details
VNet1	Virtual network	*Not applicable*
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 tab.)



You need to prevent users of VM1 and VM2 from accessing websites on the Internet over TCP port 80.

What should you do?

- ☐ Change the DenyWebSites outbound security rule.
- ☐ Change the Port_80 inbound security rule.
- ☐ Disassociate the NSG from a network interface.
- ☒ Associate the NSG to Subnet1.

Explanation:

Explanation:

You can associate or dissociate a network security group from a network interface or subnet.

Licensed to Berend Post berend.post@it-university.nl

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

Licensed to Berend Post berend.post@it-university.nl

Question 47

SIMULATION

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g, copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

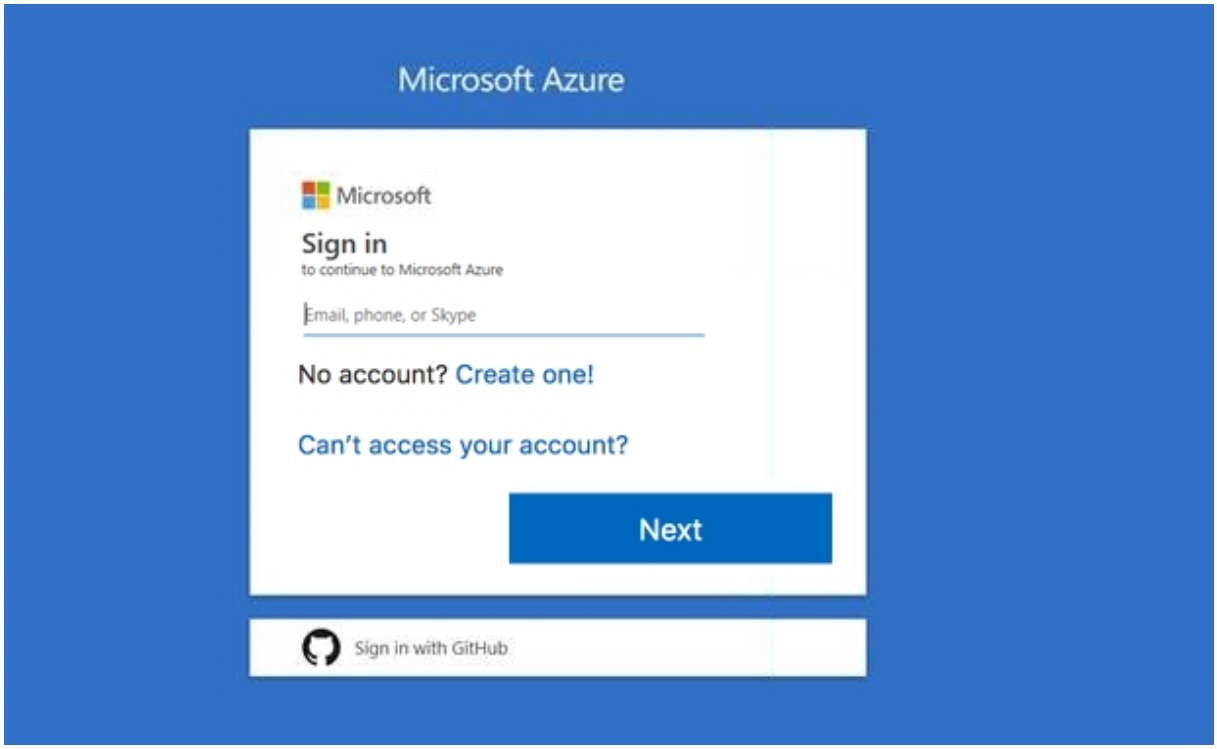
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

You may now click next to proceed to the lab.

Use the following login credentials as needed:

Azure Username: XXXXXXX
Azure Password: XXXXXXX
The following information is for technical support purposes only:
Lab Instance: 9172796

Licensed to Berend Post berend.post@it-university.nl



Your on-premises network uses an IP address range of 131.107.2.0 to 131.107.2.255.

You need to ensure that only device from the on-premises network can connect to the rg1lod9172796n1 storage account.

What should you do from the Azure portal?

Explanation:

Explanation:

Step 1: Navigate to the rg1lod9172796n1 storage account.

Step 2: Click on the settings menu called Firewalls and virtual networks.

Step 3: Ensure that you have elected to allow access from 'Selected networks'.

Step 4: To grant access to an internet IP range, enter the address range of 131.107.2.0 to 131.107.2.255 (in CIDR format) under Firewall, Address Ranges.

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 48

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 the goal?

- ☒ Yes
- ☐ No

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 49

You have an Azure subscription named Subscription1 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 VNET1, 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.

- ☒ Create VNET1 in RG2, and then set East Asia as the location.
- ☐ Create VNET1 in a new resource group in the West US location, and then set West US as the location.
- ☐ Create VNET1 in RG1, and then set East US as the location.
- ☐ Create VNET1 in RG2, and then set East US as the location.
- ☒ Create VNET1 in RG1, and then set East Asia as the location.

Question 50

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?

- ☐ VNet2 and VNet3 only
- ☐ VNet2 only
- ☐ VNet3 and VNet4 only
- ☒ VNet2, VNet3, and VNet4

Explanation:

References:

https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal

Licensed to Berend Post berend.post@it-university.nl

Question 51

SIMULATION

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g, copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

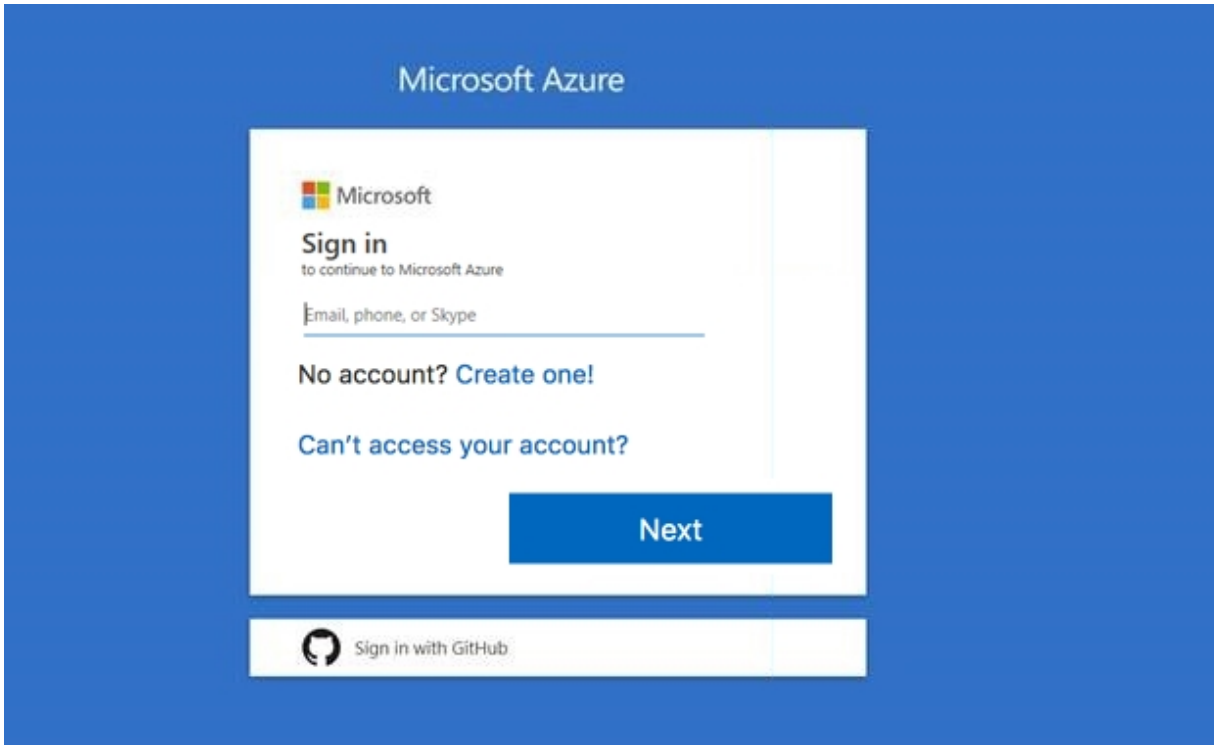
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

You may now click next to proceed to the lab.

Use the following login credentials as needed:

Azure Username: XXXXXXX
Azure Password: XXXXXXX
The following information is for technical support purposes only:
Lab Instance: 9172796

Licensed to Berend Post berend.post@it-university.nl



You plan to allow connections between the VNET01-USEA2 and VNET01-USWE2 virtual networks.

You need to ensure that virtual machines can communicate across both virtual networks by using their private IP address. The solution must NOT require any virtual network gateways.

What should you do from the Azure portal?

Explanation:

Explanation:

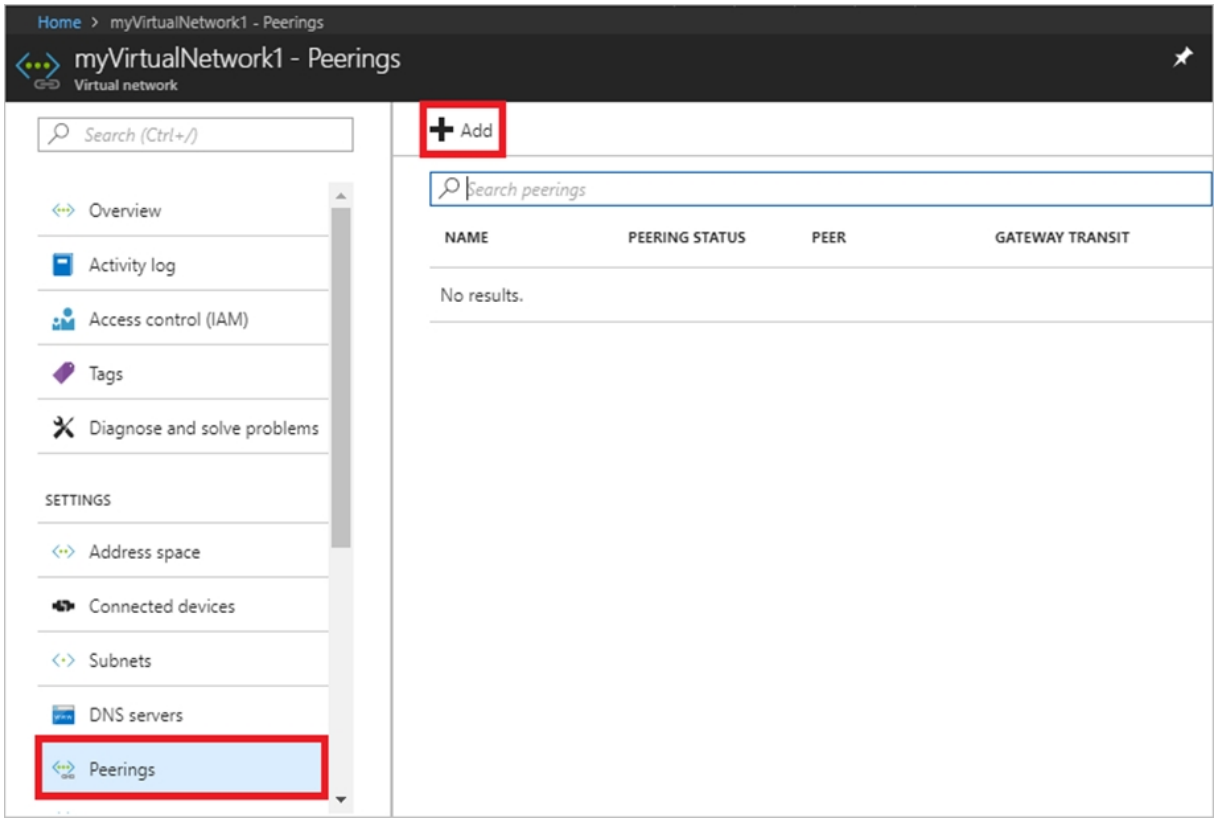
Virtual network peering enables you to seamlessly connect two Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes.

Peer virtual networks

Step 1. In the Search box at the top of the Azure portal, begin typing VNET01-USEA2. When VNET01-USEA2 appears in the search results, select it.

Step 2. Select Peerings, under SETTINGS, and then select + Add, as shown in the following picture:

Licensed to Berend Post berend.post@it-university.nl



Step 3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select OK.

Name: myVirtualNetwork1-myVirtualNetwork2 (for example)

Subscription: elect your subscription.

Virtual network: VNET01-USWE2 - To select the VNET01-USWE2 virtual network, select Virtual network, then select VNET01-USWE2. You can select a virtual network in the same region or in a different region.

Now we need to repeat steps 1-3 for the other network VNET01-USWE2:

Step 4. In the Search box at the top of the Azure portal, begin typing VNET01- USEA2. When VNET01-USEA2 appears in the search results, select it.

Step 5. Select Peerings, under SETTINGS, and then select + Add.

References:

https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal

Licensed to Berend Post berend.post@it-university.nl

Question 52

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.

- ☒ Create a gateway subnet.
- ☒ Create a VPN gateway that uses the Basic SKU.
- ☒ Create a connection.
- ☐ Create a local site VPN gateway.
- ☐ Create a VPN gateway that uses the VpnGw1 SKU.

Explanation:

References:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Question 53

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?

- ☐ Idle Time-out (minutes) to 20
- ☐ Floating IP (direct server return) to Disabled
- ☐ Floating IP (direct server return) to Enabled
- ☒ Session persistence to Client IP and protocol
- ☐ a health probe

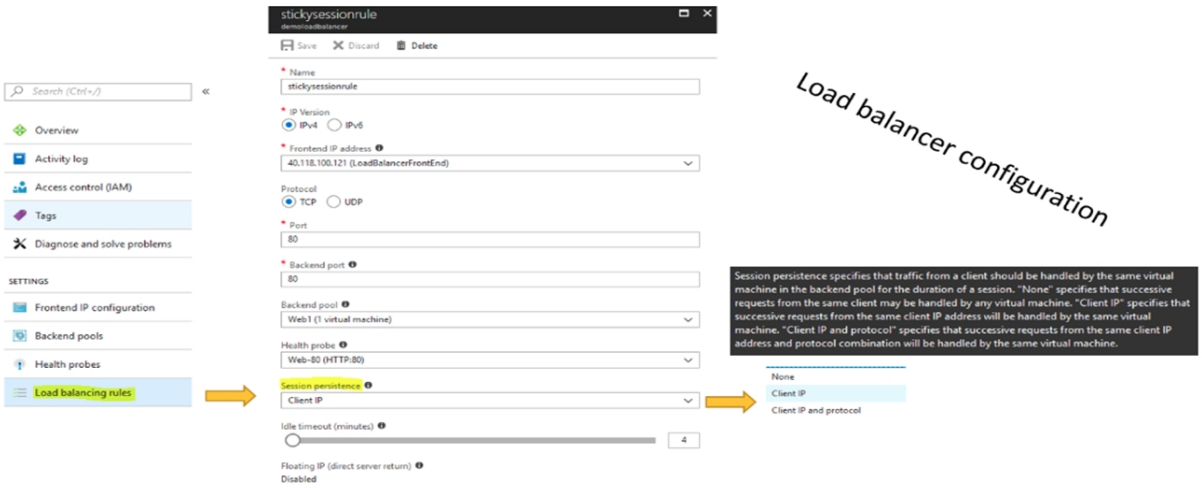
Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

On the following image you can see sticky session configuration:



Reference:

https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/

Question 54

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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

You should use a policy definition.

Licensed to Berend Post berend.post@it-university.nl

Reference:

https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition

Question 55

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?

- ☒ an inbound NAT rule
- ☐ a load balancing rule
- ☐ a new public load balancer for VM3
- ☐ a frontend IP configuration

Explanation:

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/

Licensed to Berend Post berend.post@it-university.nl

Question 56

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?

- ☐ Yes
- ☒ No

Explanation:

Modify the Name Server (NS) record.

References:

https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns

Question 57

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?

- ☐ NSG flow logs in Azure Network Watcher
- ☒ Metrics in Application Gateway
- ☐ Connection monitor in Azure Network Watcher
- ☐ Diagnostics logs in Application Gateway

Explanation:

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-diagnostics#metrics

Question 58

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

- ☒ On the peering connections, use remote gateways.
- ☐ On the peering connections, allow forwarded traffic.
- ☒ On the peering connections, allow gateway transit.
- ☐ Create route tables and assign the table to subnets.
- ☐ Create a route filter.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 59

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?

- ☐ the subnets on VNet2 only
- ☐ the subnets on VNet2 and VNet3 only
- ☐ the subnets on VNet1, VNet2, and VNet3
- ☐ the subnets on VNet1 only
- ☒ the subnets on VNet3 only

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 60

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains four subnets named Gateway, Perimeter, NVA, and Production.

The NVA subnet contains two network virtual appliances (NVAs) that will perform 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 NVAs must load balance traffic to two services on the Profuction subnet. The services have different IP addresses.

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

NOTE: Each correct selection is worth one point.

- ☐ Add two load balancing rules that have HA Ports enabled and Floating IP disabled.
- ☒ Add a frontend IP configuration, two backend pools, and a health probe.
- ☒ Add two load balancing rules that have HA Ports and Floating IP enabled.
- ☒ Deploy a standard load balancer.
- ☐ Deploy a basic load balancer.
- ☐ Add a frontend IP configuration a backend pool, and a health probe.

Explanation:

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.

Incorrect Answers:

F: HA Ports are not available for the basic load balancer.

References:

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-overview

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview

Licensed to Berend Post berend.post@it-university.nl

Question 61

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 LB2.

You need to ensure that an administrator named Admin1 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: Each 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 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

Solution:

Licensed to Berend Post berend.post@it-university.nl

Question 62

You have an Azure subscription named Subscription1 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?

- ☐ Select Allow gateway transit on VNet2.
- ☐ Enable BGP on VPNGW1.
- ☐ Select Allow gateway transit on VNet1.
- ☒ Download and re-install the VPN client configuration package on Client1.

Explanation:

References:

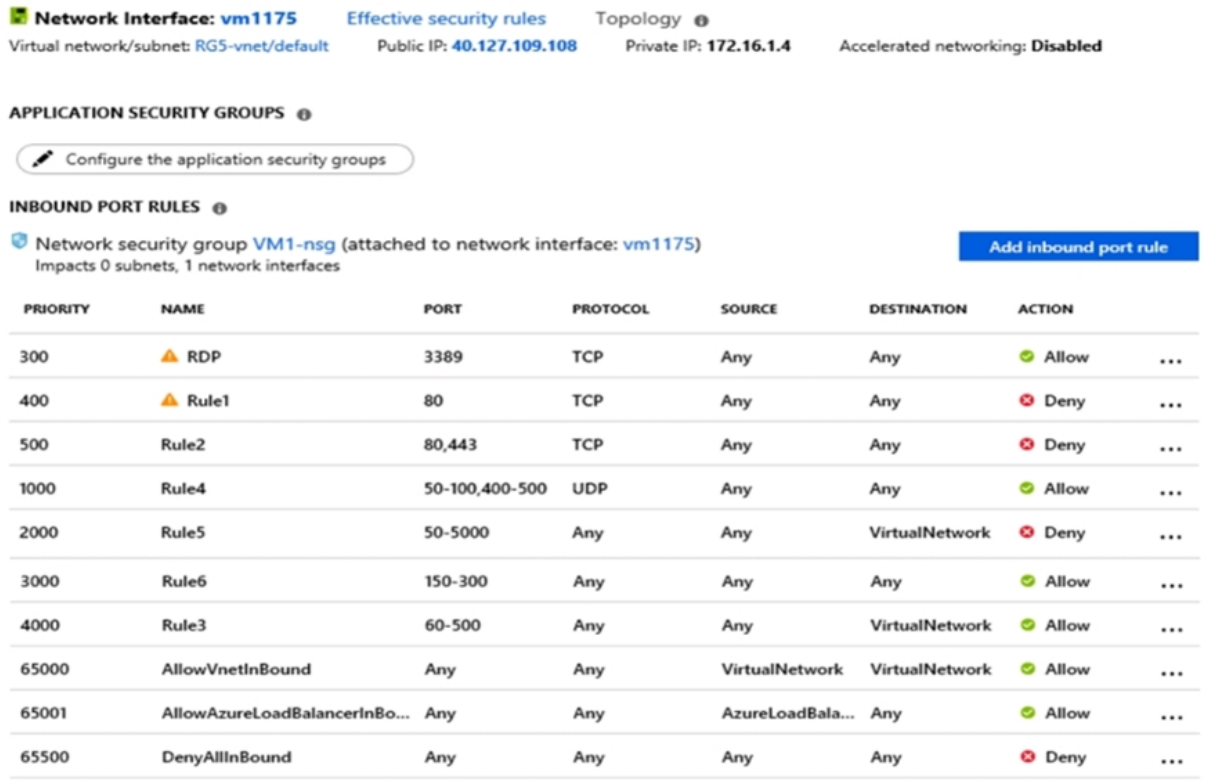
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

Licensed to Berend Post berend.post@it-university.nl

Question 63

You have an Azure virtual machine named VM1.

The network interface for VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)



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.

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

Incorrect Answers:

A: Rule 2 is blocking HTTPS access (port 443) and has a priority of 500. Creating a rule for the same protocol (443) with a higher priority number will not help.

C: Rule 1 blocks access to port 80, which is used for HTTP, not HTTPS.

D: Rule 2 is blocking HTTPS access (port 443). Changing Rule 4 allows access on UDP but is a higher priority number than Rule. Changing the protocol on Rule 4 to TCP will not help if we don't also change the priority to a lower number.

References:

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

Question 64

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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

How can I freeze or lock my production/critical Azure resources from accidental deletion? There is a way to do this with both ASM and ARM resources using Azure resource lock.

Reference:

Licensed to Berend Post berend.post@it-university.nl

https://blogs.msdn.microsoft.com/azureedu/2016/04/27/using-azure-resource-manager-policy-and-azure-lock-to-control-your-azure-resources/

Licensed to Berend Post berend.post@it-university.nl

Question 65

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	10.1.1.0/24
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

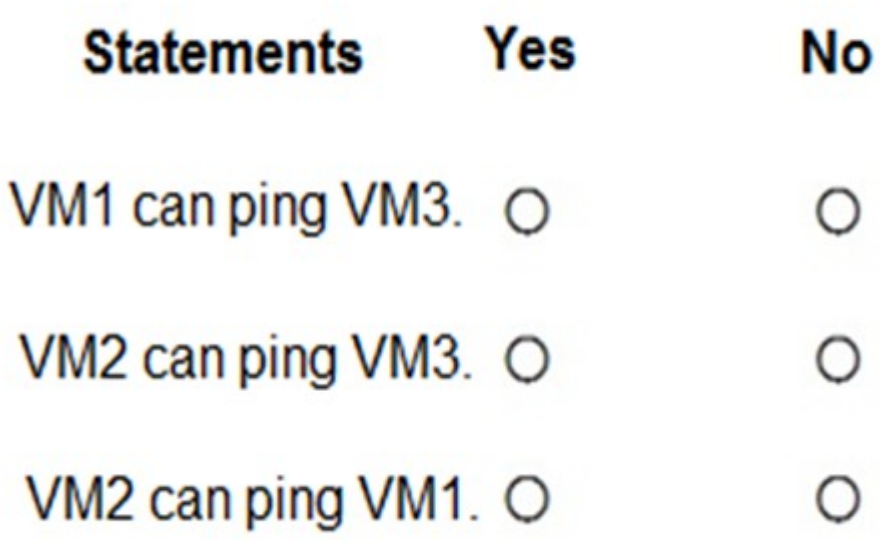
The firewalls on all the virtual machines are configured to allow all ICMP traffic.

You add the peerings in the following table.

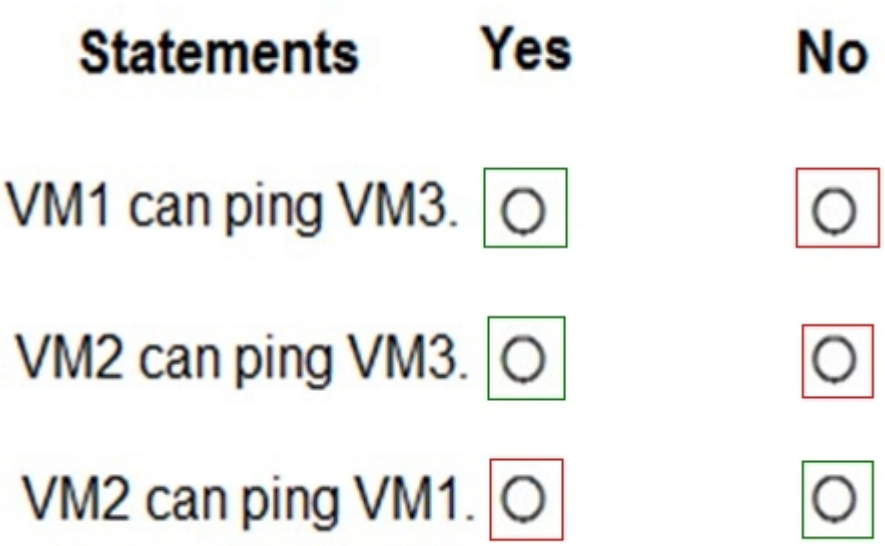
Virtual network	Peering network
VNet1	VNet3
VNet2	VNet3
VNet3	VNet1

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

NOTE: Each correct selection is worth one point.



Licensed to Berend Post berend.post@it-university.nl



Solution:

Explanation:

Explanation:

Box 1: Yes

Vnet1 and Vnet3 are peers.

Box 2: Yes

Vnet2 and Vnet3 are peers.

Box 3: No

Peering connections are non-transitive.

References:

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke

Licensed to Berend Post berend.post@it-university.nl

Question 66

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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

Modify the Name Server (NS) record.

References:

https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns

Licensed to Berend Post berend.post@it-university.nl

Question 67

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?

- ☒ Yes
- ☐ No

Explanation:

References:

https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/

Licensed to Berend Post berend.post@it-university.nl

Question 68

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?

- ☒ Yes
- ☐ No

Explanation:

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.

Reference:

https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition

Licensed to Berend Post berend.post@it-university.nl

Question 69

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.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 70

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.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 71

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?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

Use the Connection Monitor feature of Azure Network Watcher.

References:

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

Licensed to Berend Post berend.post@it-university.nl

Case Study (1 questions)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an AllInformation tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview

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

The 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 Contoso are hosted on-premises.

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

Existing Environment

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

Contoso 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.

Licensed to Berend Post berend.post@it-university.nl

Contoso.com contains a user named User1.

All the offices connect by using private links.

Contoso 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

Contoso 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

Contoso 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

Contoso 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.
Ensure 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.contoso.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.

Licensed to Berend Post berend.post@it-university.nl

Minimize costs whenever possible.

Question 72

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.

Answer Area

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.

Solution:

Answer Area

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.

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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:

Virtual network gateway. A resource that provides a virtual VPN appliance for the VNet. It is responsible for routing traffic from the on-premises network to the VNet.

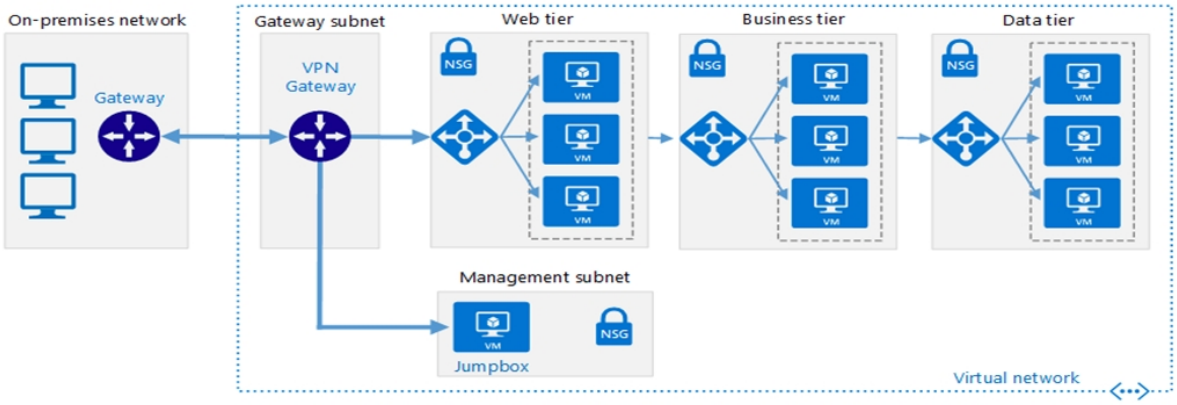
Local network gateway. An abstraction of the on-premises VPN appliance. Network traffic from the cloud application to the on-premises network is routed through this gateway.

Connection. The connection has properties that specify the connection type (IPSec) and the key shared with the on-premises VPN appliance to encrypt traffic.

Gateway subnet. The virtual network gateway is held in its own subnet, which is subject to various requirements, described in the Recommendations section below.

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.

Incorrect Answers:

Azure ExpressRoute: Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not go over the internet.

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn

Licensed to Berend Post berend.post@it-university.nl

Manage identities

(15 questions)

Question 73

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?

- ☐ From the Device settings blade, modify the Users may join devices to Azure AD setting.
- ☒ From the Device settings blade, modify the Maximum number of devices per user setting.
- ☐ Create a point-to-site VPN from the home network of User1 to Azure.
- ☐ Assign the User administrator role to User1.

Explanation:

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.

Incorrect Answers:

A: The Users may join devices to Azure AD setting enables you to select the users who can join devices to Azure AD. Options are All, Selected and None. The default is All.

C: Azure AD Join enables users to join their devices to Active Directory from anywhere as long as they have connectivity with the Internet.

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

http://techgenix.com/pros-and-cons-azure-ad-join/

Question 74

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?

- ☐ Run Azure AD Connect and set the SSO method to Pass-through Authentication.
- ☐ From Synchronization Service Manager, run a full import.
- ☐ From Azure PowerShell, run Start-AdSyncSyncCycle –PolicyType Initial.
- ☒ Run Azure AD Connect and disable staging mode.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Question 75

You have an Azure Active Directory (Azure AD) tenant.

You have an existing Azure AD conditional access policy named Policy1. Policy1 enforces the use of Azure AD-joined devices when members of the Global Administrators group authenticate to Azure AD from untrusted locations.

You need to ensure that members of the Global Administrators group will also be forced to use multi-factor authentication when authenticating from untrusted locations.

What should you do?

- ☐ From the Azure portal, modify session control of Policy1.
- ☐ From the multi-factor authentication page, modify the user settings.
- ☒ From the Azure portal, modify grant control of Policy1.
- ☐ From the multi-factor authentication page, modify the service settings.

Explanation:

Explanation:

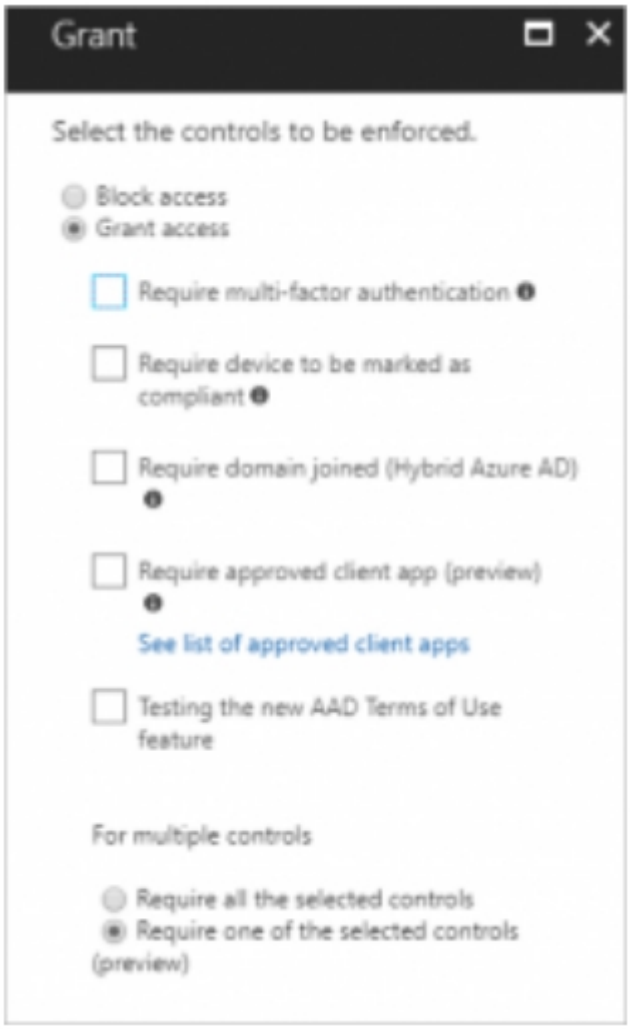
There are two types of controls:

Grant controls – To gate access

Session controls – To restrict access to a session

Grant controls oversee whether a user can complete authentication and reach the resource that they're attempting to sign-in to. If you have multiple controls selected, you can configure whether all of them are required when your policy is processed. The current implementation of Azure Active Directory enables you to set the following grant control requirements:

Licensed to Berend Post berend.post@it-university.nl



Reference:

https://blog.lumen21.com/2017/12/15/conditional-access-in-azure-active-directory/

Question 76

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?

- ☒ Providers from the MFA Server blade
- ☐ Device settings from the Groups blade
- ☐ General settings from the Groups blade
- ☐ User settings from the Users blade

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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:

Sign in to your Azure portal as a global administrator or device administrator.

On the left navbar, click Azure Active Directory.

In the Manage section, click Devices.

On the Devices page, click Device settings.

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

Licensed to Berend Post berend.post@it-university.nl

Question 77

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com that is configured for hybrid coexistence with the on-premises Active Directory domain. The tenant contains the users shown in the following table.

Name	User Type	Source	Sign-in
User1	Member	Azure AD	User1@contoso.com
User2	Member	Windows Server Active Directory	User2@contoso.com
User3	Guest	Multiple	User3@outlook.com
User4	Guest	Multiple	User4@gmail.com

Whenever possible, you need to enable Azure Multi-Factor Authentication (MFA) for the users in contoso.com.

Which users should you enable for Azure MFA?

- ☐ User1 only
- ☐ User1, User2, and User3 only
- ☐ User1 and User2 only
- ☒ User1, User2, User3, and User4
- ☐ User2 only

Licensed to Berend Post berend.post@it-university.nl

Question 78

HOTSPOT

Your network contains an Active Directory domain named adatum.com and an Azure Active Directory (Azure AD) tenant named adatum.onmicorosft.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

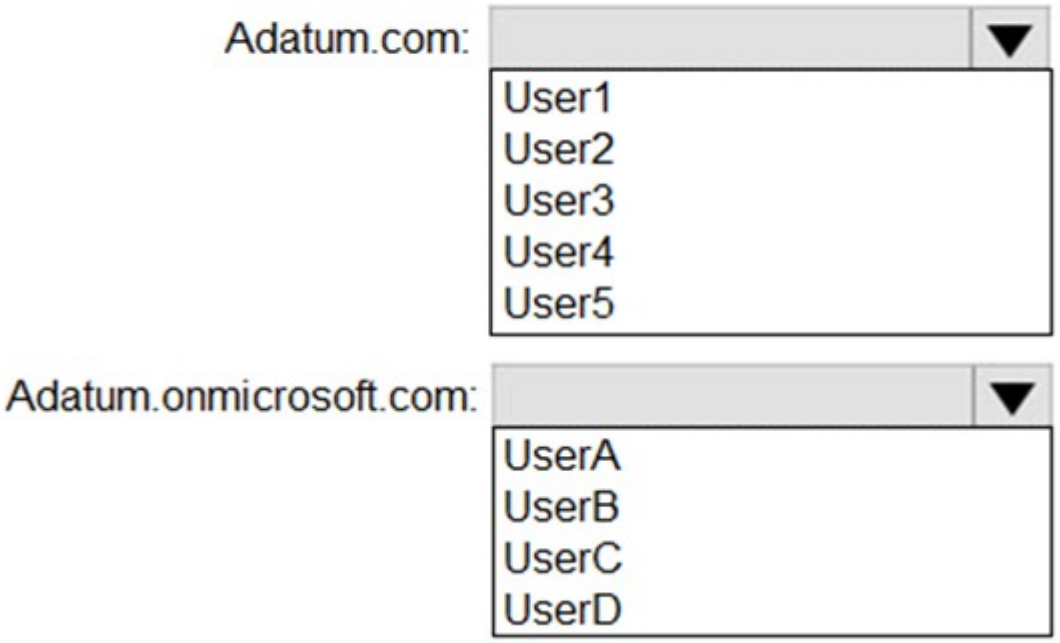
You need to implement Azure AD Connect. The solution must follow the principle of least privilege.

Which user accounts should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

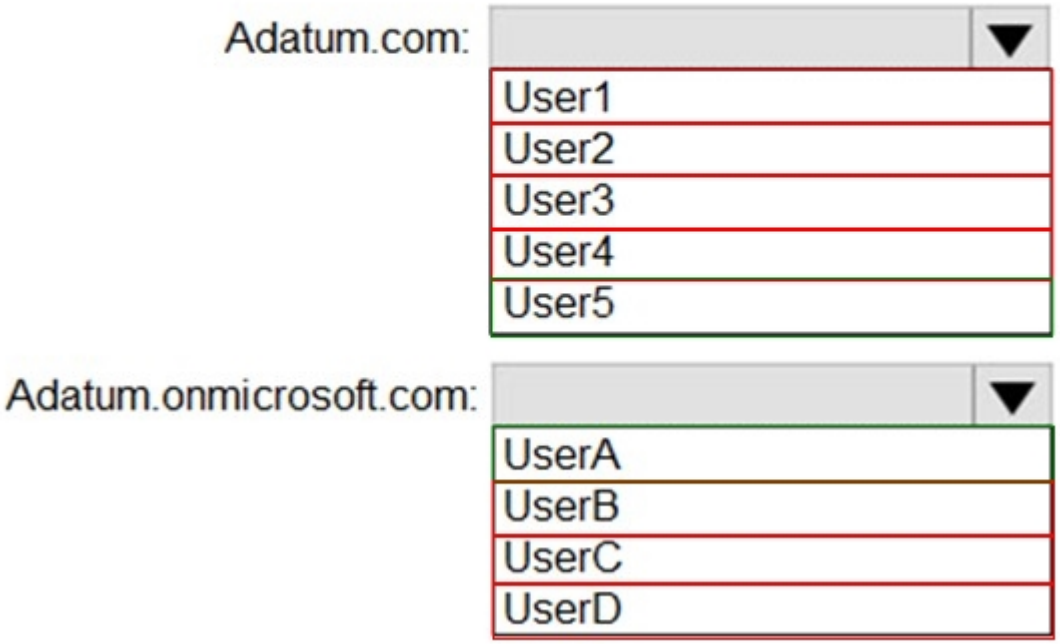
Licensed to Berend Post berend.post@it-university.nl

Answer Area



Solution:

Answer Area



Explanation:

Licensed to Berend Post berend.post@it-university.nl

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 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.

Reference:

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

Question 79

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?

- ☒ MX
- ☐ SRV
- ☐ DNSKEY
- ☐ NSEC

Explanation:

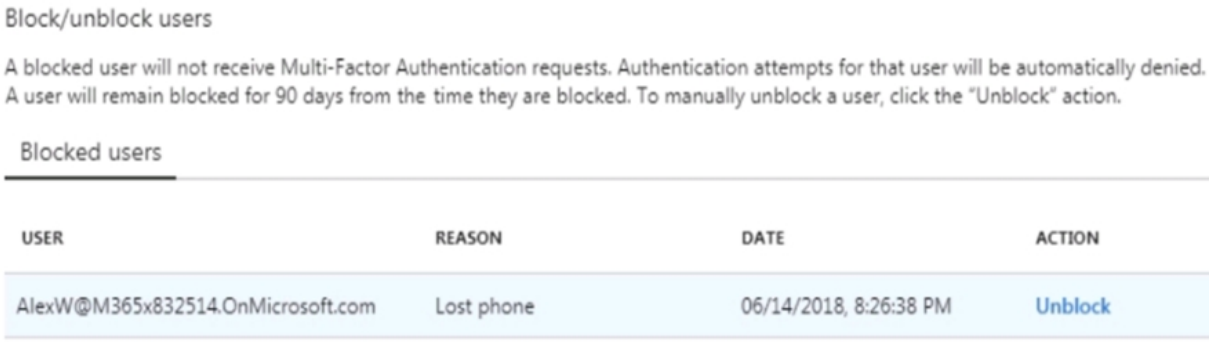
References:

Licensed to Berend Post berend.post@it-university.nl

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

Question 80

From the MFA Server blade, you open the Block/unblock users blade as shown in the exhibit.



What caused AlexW to be blocked?

- ☐ The user account password expired.
- ☐ The user entered an incorrect PIN four times within 10 minutes.
- ☒ An administrator manually blocked the user.
- ☐ The user reported a fraud alert when prompted for additional authentication.

Explanation:

Explanation:

An Administrator can block a user:

Sign in to the Azure portal as an administrator.

Browse to Azure Active Directory > MFA > Block/unblock users.

Select Add to block a user.

Select the Replication Group. Enter the username for the blocked user as username@domain.com. Enter a comment in the Reason field, for example: Lost phone.

Select Add to finish blocking the user.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Licensed to Berend Post berend.post@it-university.nl

Question 81

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?

- ☐ Create an A record named *.research in the adatum.com zone.
- ☐ Create a PTR record named research in the adatum.com zone.
- ☐ Modify the SOA record of adatum.com.
- ☒ Create an NS record named research in the adatum.com zone.

Explanation:

Explanation:

You need to create a name server (NS) record for the zone.

References:

https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain

Question 82

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?

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

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 83

You set the multi-factor authentication status for a user named admin1@contoso.com to Enabled.

Admin1 accesses the Azure portal by using a web browser.

Which additional security verifications can Admin1 use when accessing the Azure portal?

- ☒ a phone call, a text message that contains a verification code, and a notification or a verification code sent from the Microsoft Authenticator app
- ☐ an app password, a text message that contains a verification code, and a notification sent from the Microsoft Authenticator app
- ☐ an app password, a text message that contains a verification code, and a verification code sent from the Microsoft Authenticator app
- ☐ a phone call, an email message that contains a verification code, and a text message that contains an app password

Question 84

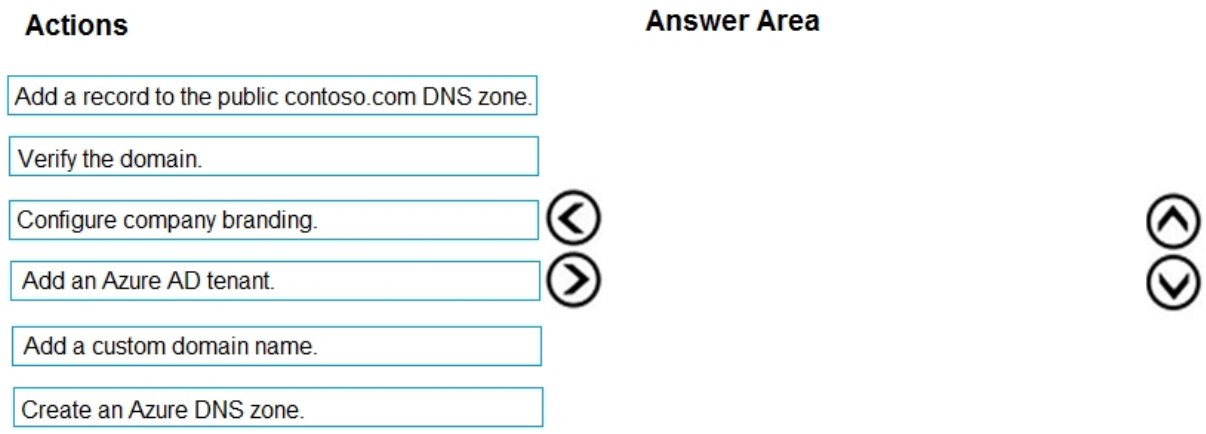
DRAG DROP

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.

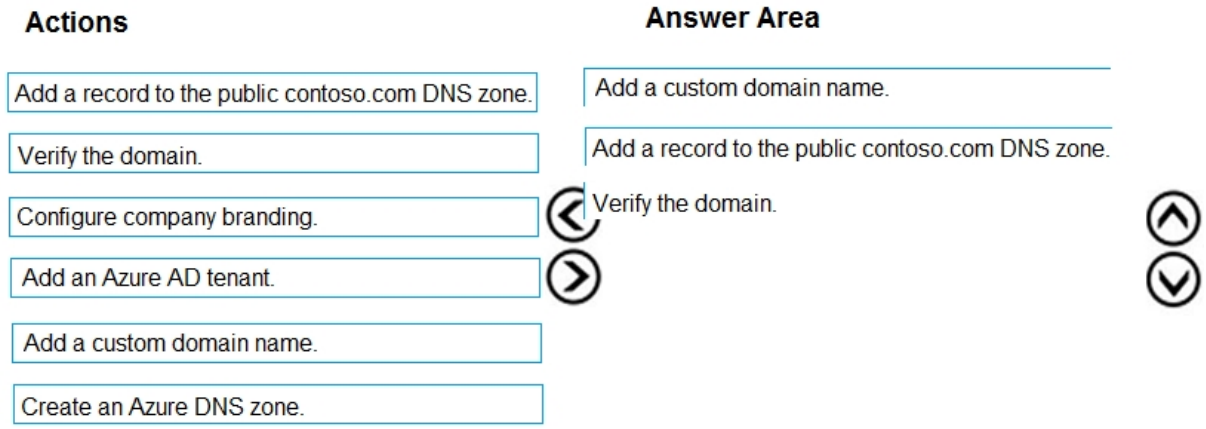
You need to ensure that you can create Azure AD users that have names containing a suffix of @contoso.com.

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.



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

References:

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

Question 85

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?

- ☐ SRV
- ☐ PTR
- ☐ RRSIG
- ☒ TXT

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 86

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?

- ☐ an Azure AD Identity Protection user risk policy.
- ☒ the multi-factor authentication service settings.
- ☐ the default for all the roles in Azure AD Privileged Identity Management
- ☐ an Azure AD Identity Protection sign-in risk policy

Question 87

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 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.
- ☒ From Windows PowerShell, run the New-AzureADUser cmdlet and specify the
- ☒ –UserPrincipalName user1@outlook.com parameter.

Explanation:

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"

Licensed to Berend Post berend.post@it-university.nl

References:

https://docs.microsoft.com/bs-cyrl-ba/powershell/azure/active-directory/new-user-sample?view=azureadps-2.0

Licensed to Berend Post berend.post@it-university.nl

Case Study (1 questions)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an AllInformation tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview

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

The 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 Contoso are hosted on-premises.

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

Existing Environment

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

Contoso 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.

Licensed to Berend Post berend.post@it-university.nl

Contoso.com contains a user named User1.

All the offices connect by using private links.

Contoso 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

Contoso 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

Contoso 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

Contoso 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.
Ensure 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.contoso.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.

Licensed to Berend Post berend.post@it-university.nl

Minimize costs whenever possible.

Question 88

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 recommendation?

- ☐ Azure AD B2C
- ☐ Azure AD Identity Protection
- ☐ an Azure logic app and the Microsoft Identity Management (MIM) client
- ☒ dynamic groups and conditional access policies

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl