AZ-102.exam.30q

AZ-102

Microsoft Azure Administrator Certification Transition

Testlet 1

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.

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 1 GB 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).

Requirements
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.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.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.
- Minimize costs whenever possible.

QUESTION 1
You discover that VM3 does NOT meet the technical requirements.

You need to verify whether the issue relates to the NSGs.

What should you use?

A. Diagnose and solve problems in Traffic Manager profiles

B. The security recommendations in Azure Advisor
C. Diagram in VNet1
D. Diagnostic settings in Azure Monitor
E. IP flow verify in Azure Network Watcher

Correct Answer: E
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Scenario: 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.

IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

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

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

What should you create and configure?

https://vceplus.com/

A. an Azure Notification Hub
B. an Azure Event Hub
C. an Azure Logic App

D. an Azure Service Bus

Correct Answer: C
Section: [none]
Explanation

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

You can start an automated logic app workflow when specific events happen in Azure resources or third-party resources. You can create a logic app that monitors changes to a virtual machine and sends emails about those changes.

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

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

What should you include in the recommendation?

A. Azure AD Identity Protection
B. Azure AD B2C
C. An Azure logic app and the Microsoft Identity Management (MIM) client
D. Dynamic groups and conditional access policies

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Scenario: Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

Conditional Access is a feature of Azure Active Directory (Azure AD) that lets you control how and when users can access applications and services.
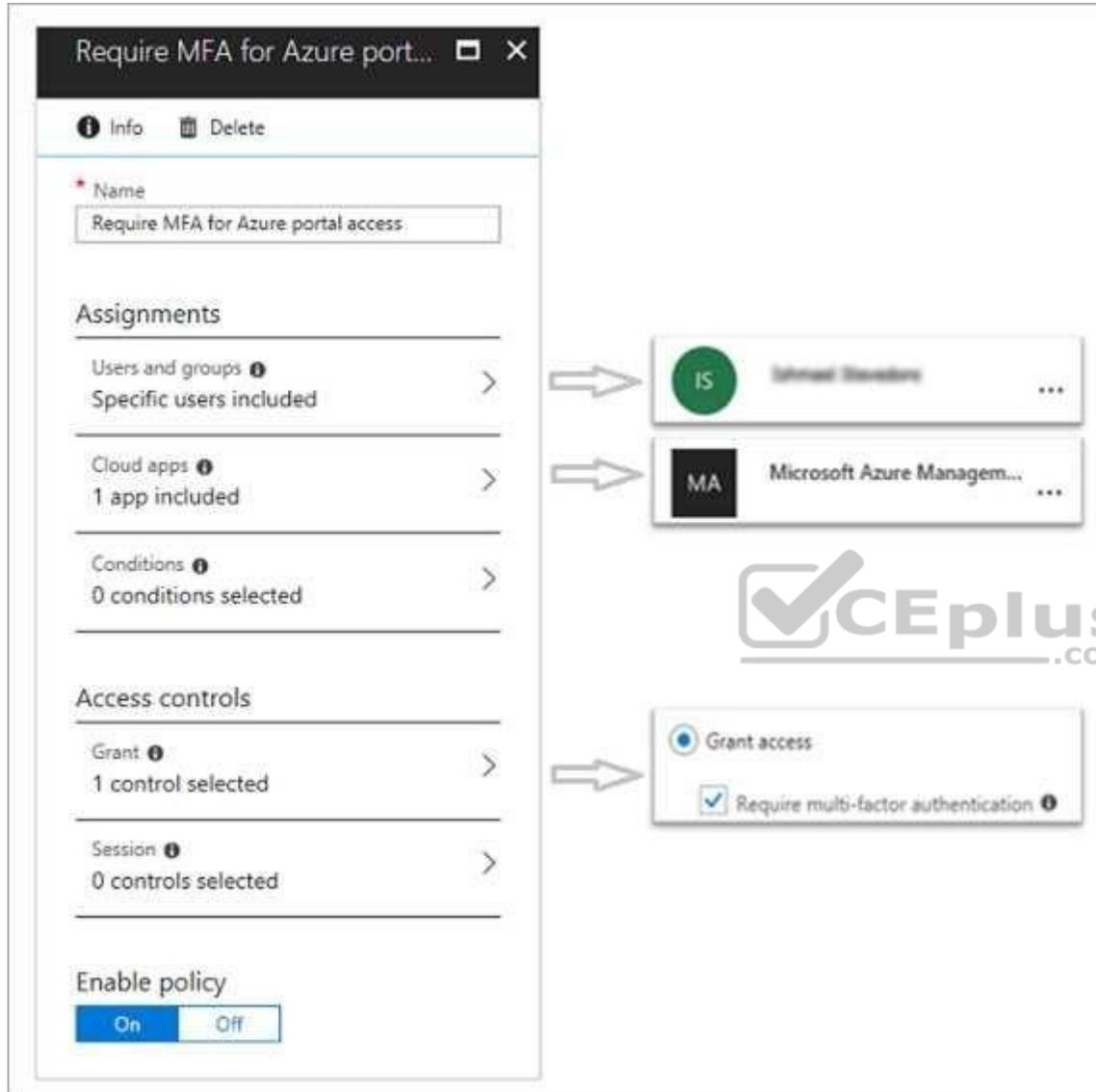
Require MFA for Azure port...

Info **Delete**

* Name

Require MFA for Azure portal access

Assignments

Users and groups
Specific users included

Cloud apps
1 app included

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy

On | Off

IS _____ ...

MA Microsoft Azure Managem... ...

● Grant access

☑ Require multi-factor authentication

Note: In Azure Active Directory (Azure AD), you can create complex attribute-based rules to enable dynamic memberships for groups. Dynamic group membership reduces the administrative overhead of adding and removing users.

When any attributes of a user or device change, the system evaluates all dynamic group rules in a directory to see if the change would trigger any group adds or removes. If a user or device satisfies a rule on a group, they are added as a member of that group. If they no longer satisfy the rule, they are removed.

References:
https://support.microsoft.com/en-ae/help/4467879/conditional-access-and-multi-factor-authentication-in-flow
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

Question Set 2

QUESTION 1
You have an on-premises network that contains a Hyper-V host named Host1. Host1 runs Windows Server 2016 and hosts 10 virtual machines that run Windows Server 2016.

You plan to replicate the virtual machines to Azure by using Azure Site recovery.

You create a Recovery Services vault named ASR1 and Hyper-V site named Site1.

You need to add Host1 to ASR1.

What should you do?

A. Download the installation file for the Azure Site Recovery Provider. Download the vault registration key.
   Install the Azure Site Recovery Provider on Host1 and register the server.
B. Download the installation file for the Azure Site Recovery Provider.
   Download the storage account key.
   Install the Azure Site Recovery Provider on each virtual machine and register the virtual machines.
C. Download the installation file for the Azure Site Recovery Provider.
   Download the vault registration key.
   Install the Azure Site Recovery Provider on each virtual machine and register the virtual machines.
D. Download the installation file for the Azure Site Recovery Provider. Download the storage account key.
   Install the Azure Site Recovery Provider on Host1 and register the server.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Download the Vault registration key. You need this when you install the Provider. The key is valid for five days after you generate it.

Install the Provider on each VMM server. You don't need to explicitly install anything on Hyper-V hosts.

Incorrect Answers:
B, D: Use the Vault Registration Key, not the storage account key.

References:

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

QUESTION 2
You have an Azure subscription that contains 100 virtual machines.

You regularly create and delete virtual machines.

You need to identify unattached disks that can be deleted.

What should you do?

A. From Azure Cost Management, open the **Optimizer** tab and create a report.
B. From Azure Cost Management, create a Cost Management report.
C. From Microsoft Azure Explorer, view the Account Management properties.
D. From the Azure portal, configure the Advisor recommendations.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
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.

Note: The ManagedBy property stores the Id of the VM to which Managed Disk is attached to. If the ManagedBy property is $null then it means that the Managed Disk is not attached to a VM

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

QUESTION 3
Your company has an Azure subscription named Subscription1.

The company also has two on-premises servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a DNS server that has a primary DNS zone named adatum.com. Adatum.com contains 1,000 DNS records.

You manage Server1 and Subscription1 from Server2. Server2 has the following tools installed:

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

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

What should you use?

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
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

QUESTION 4
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.

Select and Place:

Actions

Add a record to the public contoso.com DNS zone.

Verify the domain.

Add an Azure AD tenant.

Configure company branding.

Create an Azure DNS zone.

Add a custom domain name.

Answer Area

Correct Answer:

Actions

Add an Azure AD tenant.

Configure company branding.

Create an Azure DNS zone.

Answer Area

Add a custom domain name.

Add a record to the public contoso.com DNS zone.

Verify the domain.

Section: [none]
Explanation

Explanation/Reference:
The process is simple:

1. Add the custom domain name to your directory
2. Add a DNS entry for the domain name at the domain name registrar
3. Verify the custom domain name in Azure AD

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

QUESTION 5
You plan to migrate an on-premises Hyper-V environment to Azure by using Azure Site Recovery. The Hyper-V environment is managed by using Microsoft System Center Virtual Machine Manager (VMM).

The Hyper-V environment contains the virtual machines in the following table.

Name	Operating System (OS)	OS disk size	BitLocker Drive Encryption (BitLocker) enabled on OS disks	Generation
DC1	Windows Server 2016	500 GB	No	2
FS1	Ubuntu 16.04 LTS	200 GB	No	2
CA1	Windows Server 2012 R2	1 TB	Yes	1
SQL1	Windows Server 2016	200 GB	No	2

Which virtual machine can be migrated by using Azure Site Recovery?

A. DC1 B.
SQL1

C. CA1
D. FS1

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Up to 300 GB OS disk size is supported for generation 2 VMs and BitLocker is not enabled.

Incorrect Answers:
A: Only up to 300 GB OS disk size is supported for generation 2 VMs.
C: BitLocker must be disabled before you enable replication for a VM.
D: Linux Generation 2 VMs aren't supported.

References: https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix#azure-vm-requirements

Question Set 1

QUESTION 1
You are building a custom Azure function app to connect to Azure Event Grid.

You need to ensure that resources are allocated dynamically to the function app. Billing must be based on the executions of the app.

What should you configure when you create the function app?

A. the Windows operating system and the App Service plan hosting plan
B. the Docker container and an App Service plan that uses the B1 pricing tier
C. the Docker container and an App Service plan that uses the S1 pricing tier
D. the Windows operating system and the Consumption plan hosting plan

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure Functions runs in two different modes: Consumption plan and Azure App Service plan. The Consumption plan automatically allocates compute power when your code is running. Your app is scaled out when needed to handle load, and scaled down when code is not running.

Incorrect Answers:
A: When you run in an App Service plan, you must manage the scaling of your function app.

References: https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-first-azure-function

QUESTION 2
You have an Azure Service Bus.

You need to implement a Service Bus queue that guarantees first-in-first-out (FIFO) delivery messages.

What should you do?

A. Set the Max Size setting of the queue to 5 GB.
B. Enable duplicate detection.
C. Set the Lock Duration setting to 10 seconds.

D. Enable sessions.

E. Enable partitioning.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Through the use of messaging sessions you can guarantee ordering of messages, that is first-in-first-out (FIFO) delivery of messages.

References: https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-azure-and-service-bus-queues-compared-contrasted

QUESTION 3
You are troubleshooting a performance issue for an Azure Application Gateway.

You need to compare the total requests to the failed requests during the past six hours.

What should you use?

A. Metrics in Application Gateway

B. Diagnostics logs in Application Gateway

C. NSG flow logs in Azure Network Watcher

D. Connection monitor in Azure Network Watcher

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Application Gateway currently has seven metrics to view performance counters.

Metrics are a feature for certain Azure resources where you can view performance counters in the portal. For Application Gateway, the following metrics are available:

▪ Total Requests

▪ Failed Requests

▪ Current Connections ▪
Healthy Host Count
▪ Response Status
▪ Throughput
▪ Unhealthy Host count

You can filter on a per backend pool basis to show healthy/unhealthy hosts in a specific backend pool

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

QUESTION 4
DRAG DROP

You have an Azure subscription that contains an Azure Service Bus named Bus1.

Your company plans to deploy two Azure web apps named App1 and App2. The web apps will create messages that have the following requirements:

▪ Each message created by App1 must be consumed by only a single consumer. ▪
Each message created by App2 will be consumed by multiple consumers.

Which resource should you create for each web app? To answer, drag the appropriate resources to the correct web apps. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Resources

A Service Bus queue

A Service Bus topic

An Azure Event Grid topic

Azure Blob storage

Answer Area

App1: | Resource |

App2: | Resource |

Correct Answer:

Resources

An Azure Event Grid topic
Azure Blob storage

Answer Area

App1: A Service Bus queue

App2: A Service Bus topic

Section: [none]
Explanation

Explanation/Reference:
Explanation:

App1: A Service Bus queue

App2: A Service Bus topic

In contrast to queues, in which each message is processed by a single consumer, topics and subscriptions provide a one-to-many form of communication, in a publish/subscribe pattern.

References: https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions

QUESTION 5
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 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.

A. Install the Azure File Sync agent on Server1.
B. Create a container instance.
C. Download an automation script.
D. Create a sync group.
E. Register Server1.

Correct Answer: ADE

Section: [none]
Explanation
Explanation/Reference:
Explanation:
Azure synchronize files on-premises agent

A: The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share.

D: 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. A server can have server endpoints in multiple sync groups. You can create as many sync groups as you need to appropriately describe your desired sync topology.

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

Incorrect Answers:
B: The Resource group is used in a container.

References: https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide

QUESTION 6
You have an Azure Logic App named App1. App1 provides a response when an HTTP POST request or an HTTP GET request is received.

During peak periods, App1 is expected to receive up to 200,000 requests in a five-minute period.

You need to ensure that App1 can handle the expected load.

What should you configure?

A. Access keys
B. Access control (IAM)
C. API connections
D. Workflow settings

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:

Here are the limits for a single logic app definition:

Name	Limit	Notes
Actions per workflow	500	To extend this limit, you can add nested workflows as needed.
Allowed nesting depth for actions	8	To extend this limit, you can add nested workflows as needed.
Workflows per region per subscription	1,000	
Triggers per workflow	10	When working in code view, not the designer
Switch scope cases limit	25	
Variables per workflow	250	
Characters per expression	8,192	
Maximum size for `trackedProperties`	16,000 characters	
Name for `action` or `trigger`	80 characters	
Length of `description`	256 characters	
Maximum `parameters`	50	
Maximum `outputs`	10	

References:
https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-limits-and-config

Question Set 1

QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company registers a domain name of contoso.com.

You create an Azure DNS zone named contoso.com, and then you add an A record to the zone for a host named www that has an IP address of 131.107.1.10.

You discover that Internet hosts are unable to resolve www.contoso.com to the 131.107.1.10 IP address.

You need to resolve the name resolution issue.

Solution: You modify the name servers at the domain registrar.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You should modify the Name Server record, not the Name Servers.

Note: 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.
In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers.

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

QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company registers a domain name of contoso.com.

You create an Azure DNS zone named contoso.com, and then you add an A record to the zone for a host named www that has an IP address of 131.107.1.10.

You discover that Internet hosts are unable to resolve www.contoso.com to the 131.107.1.10 IP address.

You need to resolve the name resolution issue.

Solution: You create a PTR record for www in the contoso.com zone.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Modify the Name Server (NS) record.

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

QUESTION 3
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?

A. 80
B. 443

C. 445 D. 3389

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
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

QUESTION 4
You have a virtual network named VNet1 as shown in the exhibit.

Refresh ➡ Move 🗑 Delete

Resource group (change)
Production

Address space
10.2.0.0/16

Location
West US

DNS servers
Azure provided DNS service

Subscription (change)
Production subscription

Subscription ID
14d26092-8e42-4ea7-b770-9dcef70fb1ea

Tags (change)

Click here to add tags

Connected devices

🔍 Search connected devices

Device	Type	Ip Address	Subnet

No results.

No devices are connected to VNet1.

You plan to peer VNet1 to another virtual network named Vnet2 in the same region. VNet2 has an address space of 10.2.0.0/16.

You need to create the peering.

What should you do first?

A. Modify the address space of VNet1.

B. Configure a service endpoint on VNet2
C. Add a gateway subnet to VNet1.
D. Create a subnet on VNet1 and VNet2.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The virtual networks you peer must have non-overlapping IP address spaces.

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

QUESTION 5
You have an Azure subscription that contains three virtual networks named VNet1, VNet2, VNet3. VNet2 contains a virtual appliance named VM2 that operates as a router.

You are configuring the virtual networks in a hub and spoke topology that uses VNet2 as the hub network.

You plan to configure peering between VNet1 and VNet2 and between VNet2 and VNet3.

You need to provide connectivity between VNet1 and VNet3 through VNet2.

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

NOTE: Each correct selection is worth one point.

A. On the peering connections, allow forwarded traffic.
B. On the peering connections, allow gateway transit.
C. Create route tables and assign the table to subnets.
D. Create a route filter.
E. On the peering connections, use remote gateways.

Correct Answer: BE
Section: [none]
Explanation
Explanation/Reference:

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

QUESTION 6
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.

Hot Area:

Answer Area

Statements	Yes	No
VM1 can ping VM3.	○	○
VM2 can ping VM3.	○	○
VM2 can ping VM1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
VM1 can ping VM3.	⦿	○
VM2 can ping VM3.	⦿	○
VM2 can ping VM1.	○	⦿

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

QUESTION 7
You have an Azure DNS zone named adatum.com.

You need to delegate a subdomain named research.adatum.com to a different DNS server in Azure.

What should you do?

A. Create an A record named *.research in the adatum.com zone.
B. Modify the SOA record of adatum.com.
C. Create an PTR record named research in the adatum.com zone.
D. Create an NS record named research in the adatum.com zone.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Configure A records for the domains and sub domains.

References: http://www.stefanjohansson.org/2012/12/how-to-configure-custom-dns-names-for-multiple-subdomain-based-azure-web-sites/

QUESTION 8
You have the Azure virtual networks shown in the following table.

Name	Address space	Subnet	Resource group Azure region
VNet1	10.11.0.0/16	10.11.0.0/17	West US
VNet2	10.11.0.0/17	10.11.0.0/25	West US
VNet3	10.10.0.0/22	10.10.1.0/24	East US
VNet4	192.168.16.0/22	192.168.16.0/24	North Europe

To which virtual networks can you establish a peering connection from VNet1?

A. VNet2 and VNet3 only B.

VNet2 only

C. VNet3 and VNet4 only

D. VNet2, VNet3, and VNet4

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The virtual networks you peer must have non-overlapping IP address spaces. The VNet1 and VNhet2 address spaces overlap. The range of VNet2 is contained inside the range of VNet1.

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

QUESTION 9
You have an Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines has a public IP address.

The virtual machines host several applications that are accessible over port 443 to user on the Internet.

Your on-premises network has a site-to-site VPN connection to VNet1.

You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network.

You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure all the applications can still be accesses by the Internet users.

What should you do?

A. Modify the address space of Subnet1.
B. Remove the public IP addresses from the virtual machines.
C. Modify the address space of the local network gateway.
D. Create a deny rule in a network security group (NSG) that is linked to Subnet1.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

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

QUESTION 10
You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2.

VM1 hosts a frontend application that connects to VM2 to retrieve data.

Users report that the frontend application is slower than usual.

You need to view the average round-trip time (RTT) of the packets from VM1 to VM2.

Which Azure Network Watcher feature should you use?

A. NSG flow logs
B. Connection troubleshoot
C. IP flow verify

D. Connection monitor

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The Connection Monitor feature in Azure Network Watcher is now generally available in all public regions. Connection Monitor provides you RTT values on a perminute granularity. You can monitor a direct TCP connection from a virtual machine to a virtual machine, FQDN, URI, or IPv4 address.

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

Question Set 1

QUESTION 1
You are the global administrator for an Azure Active Directory (Azure AD) tenant named adatum.com.

You need to enable two-step verification for Azure users.

What should you do?

A. Configure a playbook in Azure AD conditional access policy.
B. Create an Azure AD conditional access policy.
C. Create and configure the Identify Hub.
D. Install and configure Azure AD Connect.

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 2
From the MFA Server blade, you open the Block/unblock users blade as shown in the exhibit.
Block/unblock users

A blocked user will not receive Multi-Factor Authentication requests. Authentication attempts for that user will be automatically denied. A user will remain blocked for 90 days from the time they are blocked. To manually unblock a user, click the "Unblock" action.

Blocked users

USER	REASON	DATE	ACTION
AlexW@M365x832514.OnMicrosoft.com	Lost phone	06/14/2018, 8:26:38 PM	Unblock

What caused AlexW to be blocked?

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
You configure Azure AD Connect for Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) for an on-premises network.

Users report that when they attempt to access myapps.microsoft.com, they are prompted multiple times to sign in and are forced to use an account name that ends with onmicrosoft.com.

You discover that there is a UPN mismatch between Azure AD and the on-premises Active Directory.

You need to ensure that the users can use single-sign on (SSO) to access Azure resources.

What should you do first?

A. From the on-premises network, deploy Active Directory Federation Services (AD FS).

B. From the server that runs Azure AD Connect, modify the filtering options.
C. From the on-premises network, request a new certificate that contains the Active Directory domain name.
D. From Azure AD, add and verify a custom domain name.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure AD Connect lists the UPN suffixes that are defined for the domains and tries to match them with a custom domain in Azure AD. Then it helps you with the appropriate action that needs to be taken. The Azure AD sign-in page lists the UPN suffixes that are defined for on-premises Active Directory and displays the corresponding status against each suffix. The status values can be one of the following: ▪ State: Verified
Azure AD Connect found a matching verified domain in Azure AD. All users for this domain can sign in by using their on-premises credentials. ▪
State: Not verified
Azure AD Connect found a matching custom domain in Azure AD, but it isn't verified. The UPN suffix of the users of this domain will be changed to the default .onmicrosoft.com suffix after synchronization if the domain isn't verified.
Action Required: Verify the custom domain in Azure AD.

References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-user-signin

QUESTION 4
HOTSPOT

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

Adatum.com contains the user accounts in the following table.

Name	Member of
User1	Domain Admins
User2	Schema Admins
User3	Incoming Forest Trust Builders
User4	Replicator
User5	Enterprise Admins

Adatum.onmicrosoft.com contains the user accounts in the following table.

Name	Role
UserA	Global administrator
UserB	User administrator
UserC	Security administrator
UserD	Service administrator

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Adatum.com:

| User1 |
| User2 |
| User3 |
| User4 |
| User5 |

Adatum.onmicrosoft.com:

| UserA |
| UserB |
| UserC |
| UserD |

Correct Answer:

Answer Area

Adatum.com:

User1
User2
User3
User4
User5

Adatum.onmicrosoft.com:

UserA
UserB
UserC
UserD

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: User5
In Express settings, the installation wizard asks for the following:

AD DS Enterprise Administrator credentials
Azure AD Global Administrator credentials

The AD DS Enterprise Admin account is used to configure your on-premises Active Directory. These credentials are only used during the installation and are not used after the installation has completed. The Enterprise Admin, not the Domain Admin should make sure the permissions in Active Directory can be set in all domains.

Box 2: UserA
Azure AD Global Admin credentials credentials are only used during the installation and are not used after the installation has completed. It is used to create the Azure AD Connector account used for synchronizing changes to Azure AD. The account also enables sync as a feature in Azure AD.

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

QUESTION 5
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 the 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?

A. From the Azure portal, modify session control of Policy1.
B. From the Azure portal, modify grant control of Policy1.
C. From the multi-factor authentication page, modify the user settings.
D. From the multi-factor authentication page, modify the service settings.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
With grant controls, you can either block access altogether or allow access with additional requirements by selecting the desired controls. For multiple controls, you can require:

- All selected controls to be fulfilled (AND) ▪
One selected control to be fulfilled (OR)
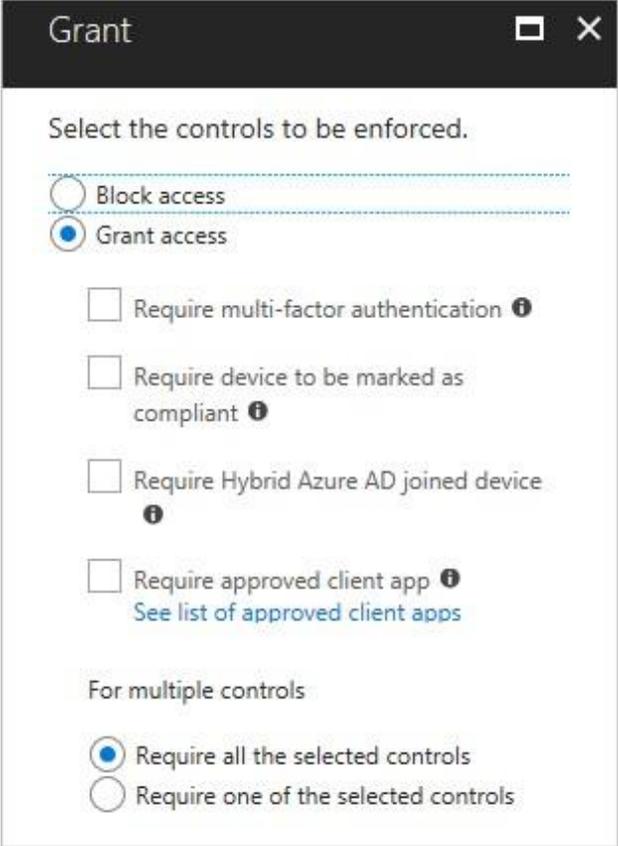
Incorrect Answers:
A: Session controls enable limited experience within a cloud app.

References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/controls

QUESTION 6
You have an Azure Active Directory (Azure AD) tenant.

All administrators must enter a verification code to access the Azure portal.

You need to ensure that the administrators can access the Azure portal only from your on-premises network.

What should you configure?

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

Correct Answer: A
Section: [none]
Explanation
Explanation/Reference: