Vendor: Microsoft

Exam Code:AZ-800

Exam Name: Administering Windows Server Hybrid Core Infrastructure

Version: Demo

QUESTION 1

DRAG DROP

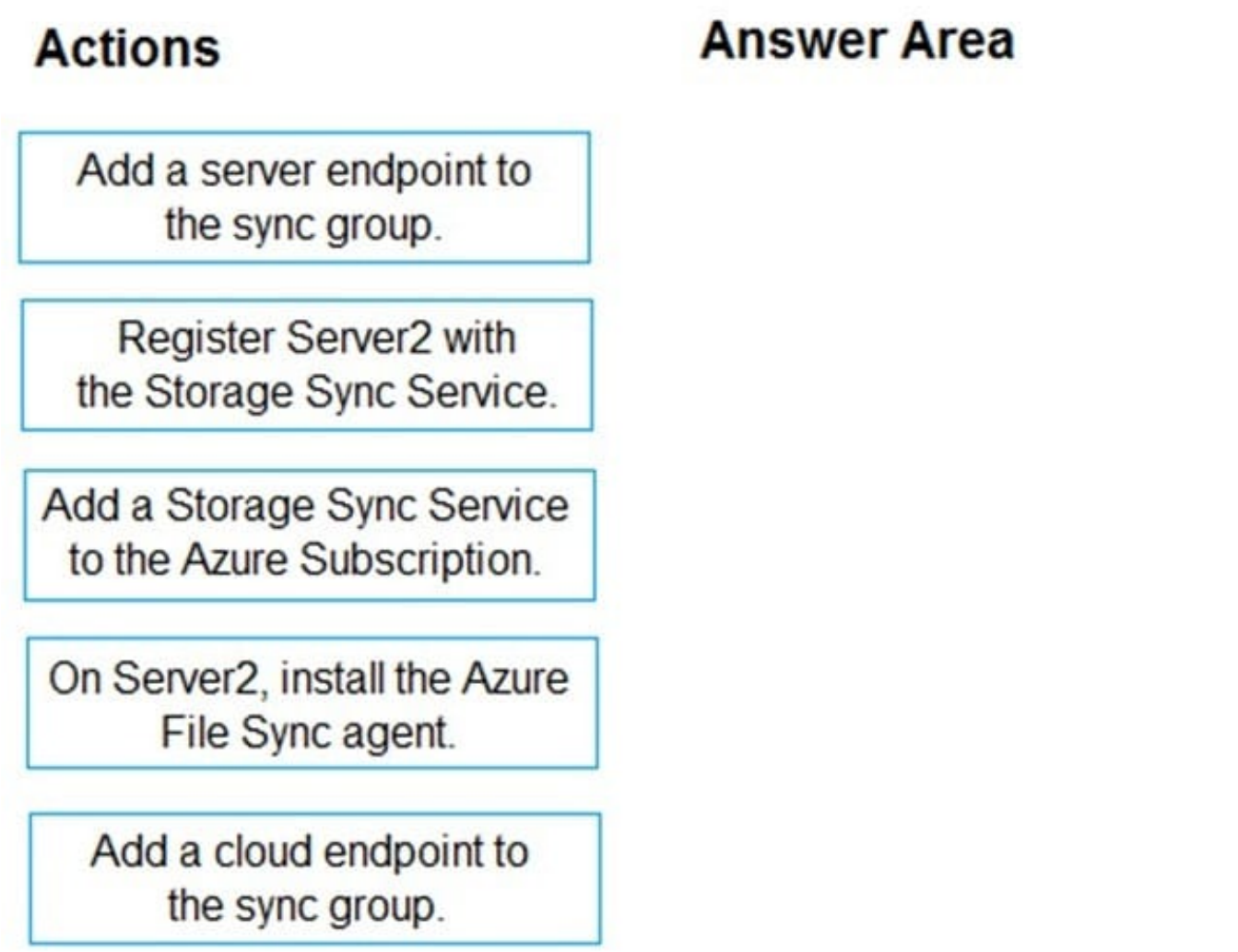
You have two on-premises servers named Server1 and Server2 that run Windows Server.

You have an Azure Storage account named storage1 that contains a file share named share1. Server1 syncs with share1 by using Azure File Sync.

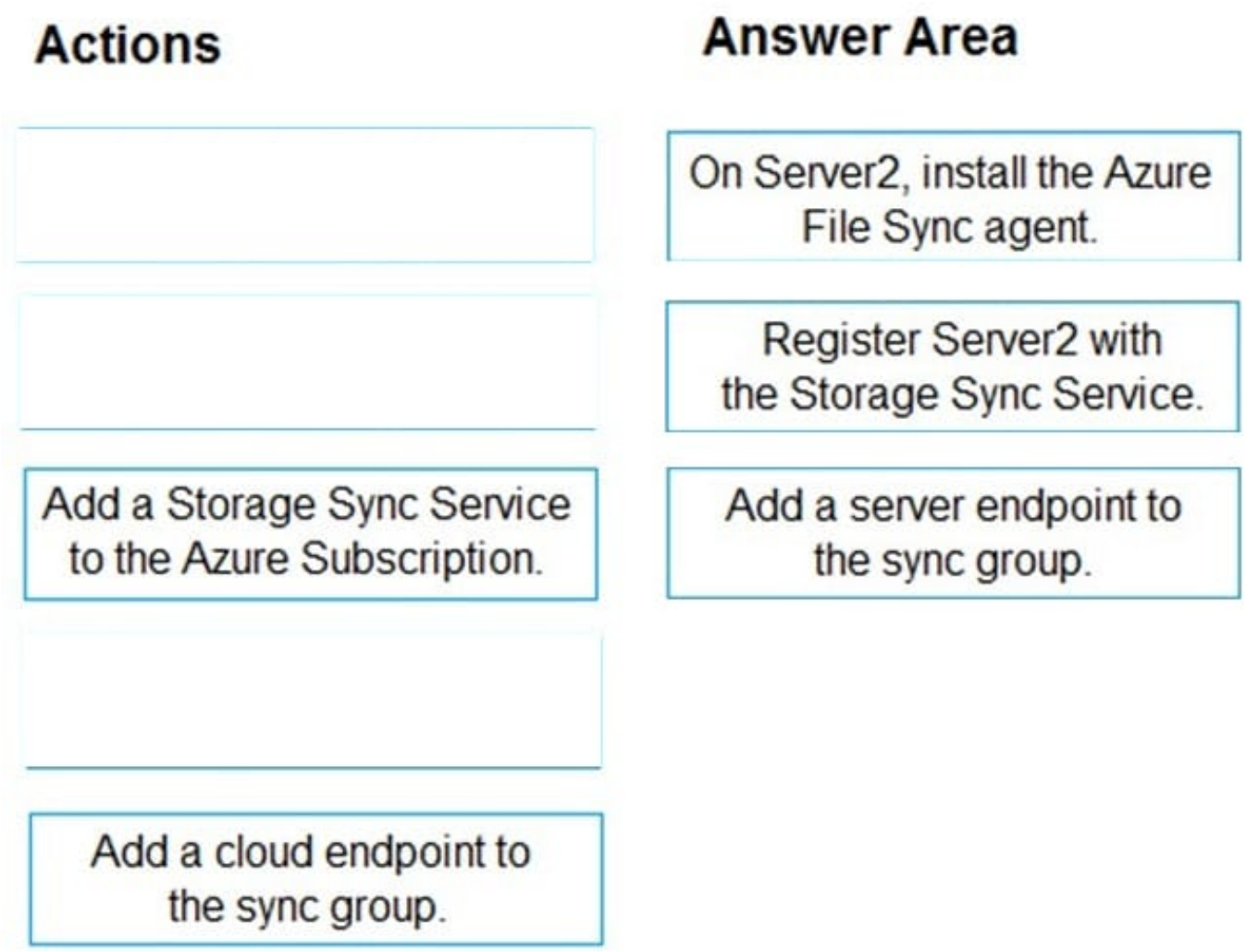
You need to configure Server2 to sync with share1.

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

Select and Place:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-server-registration
https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-server-endpoint-create?tabs=azure-portal

---

QUESTION 2

Your network contains an Active Directory Domain Services (AD DS) forest. The forest contains three domains. Each domain contains 10 domain controllers.

You plan to store a DNS zone in a custom Active Directory partition.

You need to create the Active Directory partition for the zone. The partition must replicate to only four of the domain controllers.

What should you use?

A. dnscmd.exe

B. Active Directory Sites and Services

C. Set-DnsServer

D. DNS Manager

Correct Answer: D

You can create DNS application directory partition to host DNS zone containing user account entries with the use of NTDSUTIL.EXE and DNSMGMT.MSC tools.

Note 1: You can also create a custom Active Directory partition by using the DnsCmd command.

Note 2: Implementing DNS Application Directory Partition

1.

Login to the forest root domain controller using your forest root domain admin account or enterprise administrator account

2.

Start the command prompt.

3.

Type NTDSUTIL and hit enter

4.

Type PARTITION MANAGEMENT and hit enter

5.

Type CONNECTIONS and hit enter

6.

Type CONNECT TO SERVER or ex. CONNECT TO SERVER DC01.AMRS.SYNERGIX.DS

1.

Type QUIT

2.

Type LIST to view all known naming contexts

3.

Type CREATE NC DC=dnsADPUsers,DC=Local domainControllerFQDN ex. CONNECT TO SERVER DC01.AMRS.SYNERGIX.DS

1.

Type LIST to view all previously known naming context and the newly created DC=dnsADPUsers,DC=Local naming context

2.

Do NOT add another replica for the naming context DC=dnsADPUsers,DC=Local

This DNS Application Directory Partition is for a special purpose DNS zone and we wish to avoid Active Directory Replication delays. A backup of this DNS zone\\'s content can be maintained in a secondary DNS zone on any DNS server.

Reference: https://synergixdesk.zendesk.com/hc/en-us/articles/202927548-Create-DNS-application-directory-partition-to-host-DNS-zone-containing-user-account-entries

---

QUESTION 3

You have an Azure virtual machine named VM1 that runs Windows Server.

You need to configure the management of VM1 to meet the following requirements:

1.

Require administrators to request access to VM1 before establishing a Remote Desktop connection.

2.

Limit access to VM1 from specific source IP addresses.

3.

Limit access to VM1 to a specific management port. What should you configure?

A. a network security group (NSG)

B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

C. Microsoft Defender for Cloud

D. Azure Front Door

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage?tabs=jit-config-asc%2Cjit-request-asc

---

QUESTION 4

Your network contains an Active Directory Domain Services (AD DS) forest named contoso.com. The forest root domain contains a server named server1.contoso.com.

A two-way forest trust exists between the contoso.com forest and an AD DS forest named fabrikam.com. The fabrikam.com forest contains 10 child domains.

You need to ensure that only the members of a group named fabrikam\Group1 can authenticate to server1.contoso.com.

What should you do first?

A. Add fabrikam\Group1 to the local Users group on server1.contoso.com.

B. Enable SID filtering for the trust.

C. Enable Selective authentication for the trust.

D. Change the trust to a one-way external trust.

Correct Answer: C

Selective authentication restricts access over an external or forest trust to only those users in a trusted domain or forest who have been explicitly given authentication permissions to computer objects (resource computers) residing in the

trusting domain or forest. This authentication setting must be manually enabled.

Note: When a two way Forest Trust is created between Forest A and Forest B, all domains in Forest A will trust all domains in Forest B and vice versa.

Incorrect:

Not B: When SID Filtering is enabled, all the foreign SIDs will be removed (quarantined) from user\\'s access token while accessing any resource through Forest Trust. The most common impact of this is, a migrated user account which is still

using any resource using old SID will not be able to access that resource anymore. This is because when SID Filtering is enabled, it will block (filter) SID History through a Forest Trust.

When we create a forest Trust, SID Filtering is enabled by default. In some cases, we need to disable SID Filtering.

Not D: When a two way Forest Trust is created between Forest A and Forest B, all domains in Forest A will trust all domains in Forest B and vice versa.

If a one way Forest Trust is created, where Forest A is Trusting Domain and Forest B is Trusted Domain, then Forest B can access resources within Forest A, however Forest A cannot access resources within Forest B.

Reference:

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10)

QUESTION 5

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 network contains an Active Directory Domain Services (AD DS) forest. The forest contains three Active Directory sites named Site1, Site2, and Site3. Each site contains two domain controllers. The sites are connected by using

DEFAULTIPSITELINK.

You open a new branch office that contains only client computers.

You need to ensure that the client computers in the new office are primarily authenticated by the domain controllers in Site1.

Solution: You create a new subnet object that is associated to Site1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Yes, creating a new subnet object that is associated with Site1 would meet the goal of ensuring that client computers in the new office are primarily authenticated by the domain controllers in Site1. When a client computer requests authentication, Active Directory will use the subnet-to-site association to determine which site the client computer is in, and will then direct the authentication request to a domain controller in that site. By associating the new subnet with Site1, client computers in the new office will be directed to authenticate with domain controllers in Site1.

QUESTION 6

HOTSPOT

You have an on-premises DNS server named Server1 that runs Windows Server. Server1 hosts a DNS zone named fabnkam.com.

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

Name	Type	Description
Vnet1	Virtual network	Connects to the on-premises network by using a Site-to-Site VPN
VM1	Virtual machine	Runs Windows Server and has the DNS Server role installed
contoso.com	Private DNS zone	Linked to Vnet1
contoso.com	Public DNS zone	Contains the DNS records of all the platform as a service (PaaS) resources

You need to design a solution that will automatically resolve the names of any PaaS resources for which you configure private endpoints in Vnet1.

How should you configure the name resolution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On Vnet1

Configure VM1 to forward requests for the contoso.com zone to the public DNS zone
Configure Vnet1 to use a custom DNS server that is set to the Azure-provided DNS at 168.63.129.16
Configure VM1 to forward requests for the contoso.com zone to the Azure-provided DNS at 168.63.129.16

On the on-premises network

Configure forwarding for the contoso.com zone to VM1
Configure forwarding for the contoso.com zone to the public DNS zone
Configure forwarding for the contoso.com zone to the Azure-provided DNS at 168.63.129.16

Correct Answer:

Answer Area

On Vnet1

Configure VM1 to forward requests for the contoso.com zone to the public DNS zone
Configure Vnet1 to use a custom DNS server that is set to the Azure-provided DNS at 168.63.129.16
Configure VM1 to forward requests for the contoso.com zone to the Azure-provided DNS at 168.63.129.16

On the on-premises network

Configure forwarding for the contoso.com zone to VM1
Configure forwarding for the contoso.com zone to the public DNS zone
Configure forwarding for the contoso.com zone to the Azure-provided DNS at 168.63.129.16

QUESTION 7

HOTSPOT

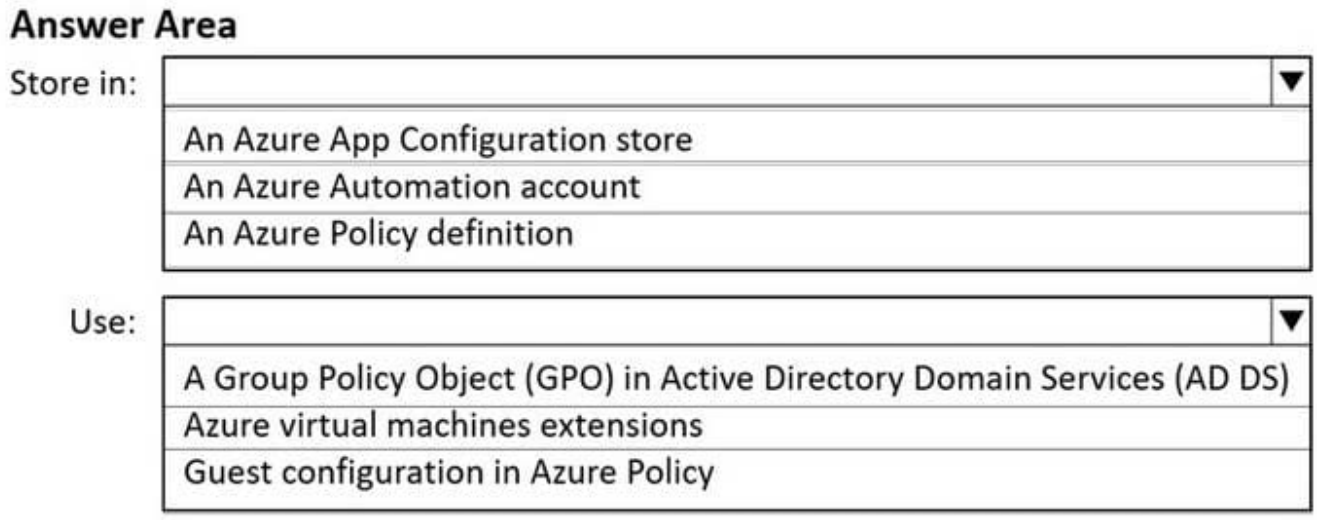
Your on-premises network contains an Active Directory domain named contoso.com and 500 servers that run Windows Server. All the servers are Azure Arc-enabled and joined to contoso.com.

You need to implement PowerShell Desired State Configuration (DSC) on all the servers. The solution must minimize administrative effort.

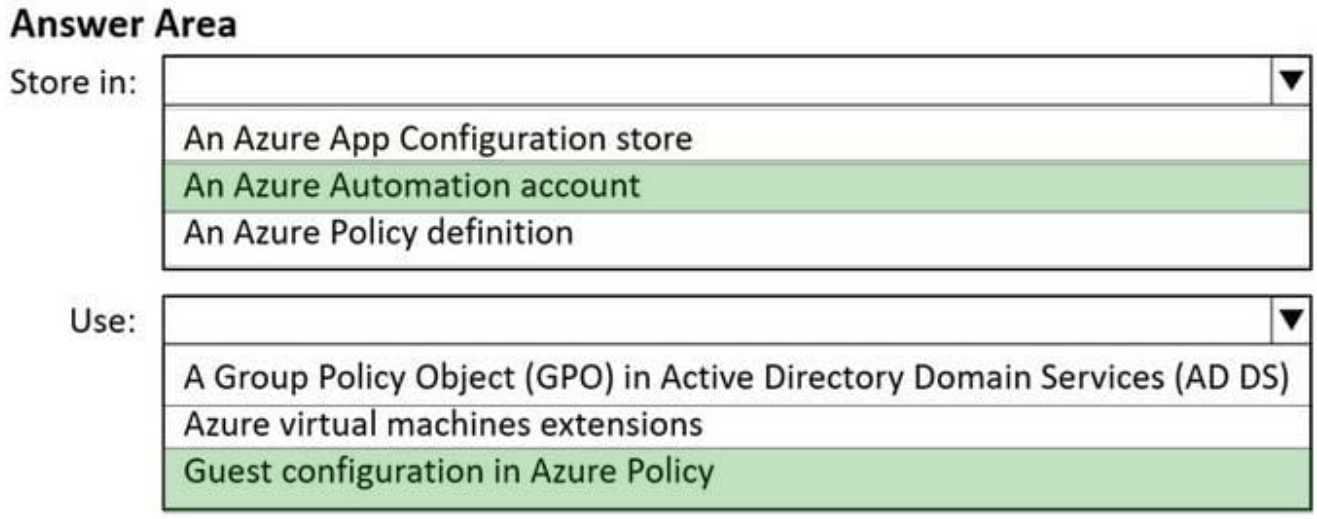
Where should you store the DSC scripts, and what should you use to apply DSC to the servers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: An Azure Automation account

Azure Automation allows you to automate tasks against resources in Azure, on-premises, and with other cloud providers such as Amazon Web Services (AWS).

When you start Azure Automation for the first time, you must create at least one Automation account.

Azure Automation State Configuration

Prerequisites include: An Azure Automation account

Azure Automation State Configuration is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations for nodes in any cloud or on-premises

datacenter.

Box 2: Guest configuration in Azure policy

Note: Before you enable Automation State Configuration, we would like you to know that a newer version of DSC is now generally available, managed by a feature of Azure Policy named guest configuration. The guest configuration service

combines features of DSC Extension, Azure Automation State Configuration, and the most commonly requested features from customer feedback. Guest configuration also includes hybrid machine support through Arc-enabled servers.

Reference:

https://learn.microsoft.com/en-us/azure/automation/automation-security-overview

https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview

---

QUESTION 8

You need to use the principle of least privilege.

Choose a solution to meet the technical requirements for User1.

A. Create a delegation on contoso.com.

B. Create a delegation on OU3.

C. Add Users1 to the Server Operators group in contoso.com.

D. Add Users1 to the Account Operators group in contoso.com.

Correct Answer: B

QUESTION 9

Your network contains a multi-site Active Directory Domain Services (AD DS) forest. Each Active Directory site is connected by using manually configured site links and automatically generated connections.

You need to minimize the convergence time for changes to Active Directory.

What should you do?

A. For each site link, modify the options attribute.

B. For each site link, modify the site link costs.

C. For each site link, modify the replication schedule.

D. Create a site link bridge that contains all the site links.

Correct Answer: C

Reconfigure the link site option to use notification.

Details: Active Directory – Change Notification (Inter-Site Replication)

Since we know Active Directory, we know also that its replication works automatically between the domain controllers. The lowest value of this replication schedule is 15 minutes. You can\\'t get lower. If there aren\\'t that many frequent changes,

or the active directory site is not large (probably with only one site) then this value should work for you.

But what if your active directory environment is larger? What if you have more than one site, on different locations, with different networks? Or what if you've got some remotedesktop services running in your main site and some users working

with them in a branch office? What about the "I forgot my password" cases?

Well, there is a solution for you. We can tune-up the Active Directory Inter-Site Replication. The inter-site replication works also automatically, and you can also schedule the replication only for 15 minutes. But there are some settings we can

tweak to get the domain controllers pulling the changes made recently.

1.

First open "Active Directory Sites and Services" on your primary domain controller (that\\'s the icon with the blue "building").

2.

Let\\'s start now with the tuning operation. Expand "Sites" and "Inter-Site Transports" (if you haven\\'t already). Click on the IP folder.

3.

Now right-click (or double-click) on your site link on the right hand side. If you did not rename it, it\\'s just the DEFAULTIPSITELINK. Then click "Properties". Then click on the "Attribute Editor" tab.

4.

The attribute we should edit is called "options".

We now have to change this attribute to a specific value which allows us to tweak the inter-site replication.

Value,

1 USE_NOTIFY (use this setting!)

2 TWOWAY_SYNC

4 DISABLE_COMPRESSION

Incorrect:

Not B: Two scenarios in which you need a site link bridge design to control replication flow include controlling replication failover and controlling replication through a firewall.

Not D: The minimal replication schedule is 15 minutes. When you use manual site link replication interval is set to 15 minutes and cannot be lowered further.

Reference: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/determining-the-interval

---

QUESTION 10

HOTSPOT

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
Admin1 must use a password that has at least 14 characters.	○	○
User1 must use a password that has at least 10 characters.	○	○
If Admin1 creates a new local user on Server1, the password for the new user must be at least eight characters.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Admin1 must use a password that has at least 14 characters.	○	○
User1 must use a password that has at least 10 characters.	○	○
If Admin1 creates a new local user on Server1, the password for the new user must be at least eight characters.	○	○

QUESTION 11

You have an Azure virtual machine named Server1 that runs a network management application. Server1 has the

following network configurations:

1.

Network interface: Nic1

2.

IP address: 10.1.1.1/24

3.

Connected to: Vnet1/Subnet1

You need to connect Server1 to an additional subnet named Vnet1/Subnet2.

What should you do?

A. Modify the IP configurations of Nic1.

B. Add an IP configuration to Nic1.

C. Add a network interface to Server1.

D. Create a private endpoint on Subnet2.

Correct Answer: C

First add another network interface to Server1, then connect it to Subnet2.

Virtual network and subnets.

A subnet is a range of IP addresses in the virtual network. You can divide a virtual network into multiple subnets for organization and security. Each NIC in a VM is connected to one subnet in one virtual network. NICs connected to subnets

(same or different) within a virtual network can communicate with each other without any extra configuration.

Reference:

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

---

QUESTION 12

SIMULATION

You need to create a user named Admin1 in contoso.com. Admin1 must be able to back up and restore files on SRV1. The solution must use principle of the least privilege.

To complete this task, sign in the required computer or computers.

A. See explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

Step 1: Sign in to the Azure portal in the User Administrator role for the organization.

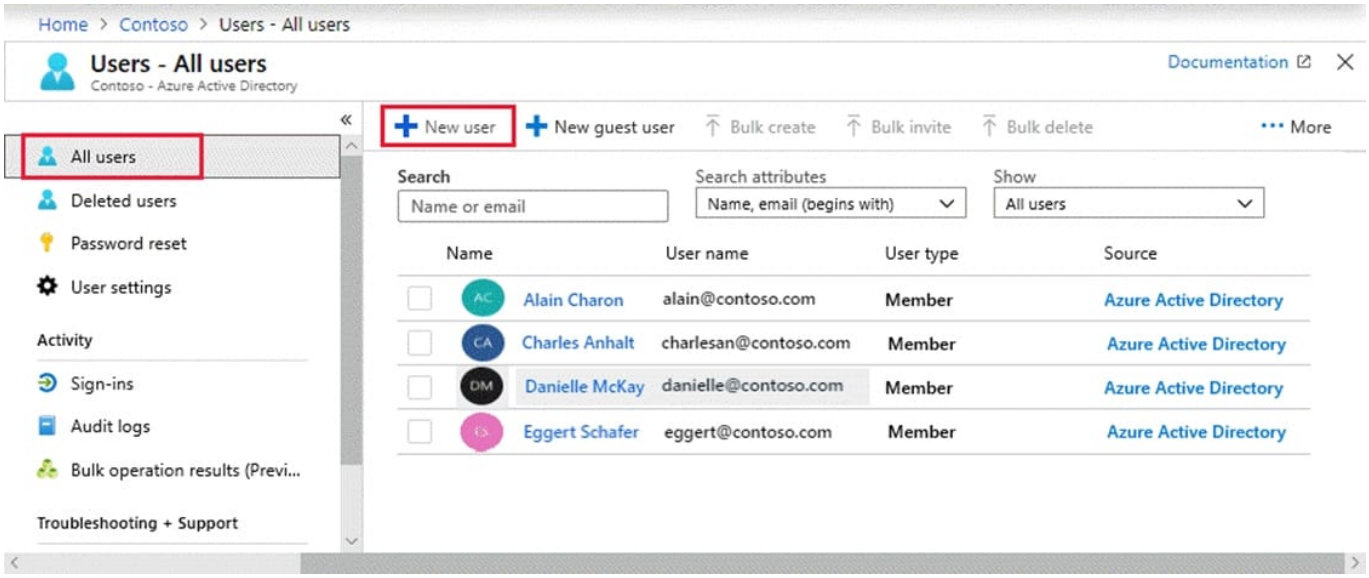
Add a new user

You can create a new user using the Azure Active Directory portal.

To add a new user, follow these steps:

Step 1. Sign in to the Azure portal in the User Administrator role for the organization.

Step 2: Search for and select Azure Active Directory from any page.



Step 3: Select Users, and then select New user.

Step 4: On the User page, enter information for this user:

Name: Admin1

User name: Admin1

Groups. Optional

Groups. Optional: Backup Operator

Step 5: Copy the autogenerated password provided in the Password box. You\\'ll need to give this password to the user to sign in for the first time.

Step 6: Select Create.

The user is created and added to your Azure AD organization.

Note:

Azure Backup provides three built-in roles to control backup management operations.

Backup Operator - This role has permissions to everything a contributor does except removing backup and managing backup policies. This role is equivalent to contributor except it can\\'t perform destructive operations such as stop backup

with delete data or remove registration of on-premises resources.

Incorrect:

Backup Contributor - This role has all permissions to create and manage backup except deleting Recovery Services vault and giving access to others. Imagine this role as admin of backup management who can do every backup management

operation.

Backup Reader - This role has permissions to view all backup management operations. Imagine this role to be a monitoring person.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

https://learn.microsoft.com/en-us/azure/backup/backup-rbac-rs-vault