

Microsoft.AZ-800J.v2026-02-16.q118

試験コード : AZ-800J
試験名称 : Administering Windows Server Hybrid Core Infrastructure (AZ-800日本語版)
認証ベンダー : Microsoft
無料問題の数 : 118
バージョン : v2026-02-16
ページの閲覧量 : 110
問題集の閲覧量 : 1365
<https://www.jpnsiken.com/shiken/Microsoft.AZ-800J.v2026-02-16.q118.html>

質問: 1

ネットワークには、contoso.com というオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。このドメインには、Windows Server を実行し、Hyper-V サーバーがインストールされている 3 つのサーバーが含まれています。各サーバーには Switch Embedded Teaming (SET) チームがあり、Remote Direct Memory Access (RDMA) と必要なすべての Windows Server 設定が各サーバーで適切に構成されていることを確認する必要があります。

何を使うべきですか？

- A. サーバー マネージャー
- B. validate-DCB コマンドレット
- C. Get-NetAdaptor コマンドレット
- D. フェールオーバー クラスタ マネージャー

正解: B ([コメントを發表する](#))

In Windows Server deployments that use Hyper-V with Switch Embedded Teaming (SET) and SMB Direct (RDMA), Microsoft's guidance in Administering Windows Server Hybrid Core Infrastructure is to validate the end-to-end Data Center Bridging (DCB) and RDMA prerequisites with Validate-DCB. The DCB validation covers the exact Windows Server settings RDMA depends on: Priority-based Flow Control (PFC), Enhanced Transmission Selection (ETS), QoS policies for SMB (priority tagging), and RDMA enablement on the relevant physical adapters. The study materials emphasize that while tools such as Server Manager, Failover Cluster Manager, or basic adapter inventory (e.g., Get-NetAdapter) can show device status or general configuration, they do not verify the complete, lossless fabric requirements for RDMA over Converged Ethernet used with Hyper-V/SET.

The prescribed approach is to run Validate-DCB against the host NICs participating in the SET team to confirm:

- * RDMA is enabled on the interfaces used for SMB Direct.
- * PFC is enabled for the SMB priority.
- * ETS bandwidth reservations are correctly applied.
- * QoS policies align across adapters so SMB traffic is lossless.

The cmdlet produces pass/fail diagnostics and remediation guidance, providing a single authoritative validation for "RDMA and all required Windows Server settings" on each server. Accordingly, the correct choice for verifying the configuration in this scenario is Validate-DCB.

質問: 2

Windows Server を実行し、次の表に示すボリュームを含む Server1 という名前のファイル サーバーがあります。

Name	File system
Microsoft C	NTFS
D	NTFS
E	REFS

BitLocker ドライブ暗号化(BitLocker)とディスククォータはどのボリュームで使用できますか？ 回答するには、回答エリアから適切なオプションを選択してください。注：正解は1つにつき1ポイントです。

Answer Area

Microsoft

BitLocker:

C only

D only

C and D only

D and E only

C, D, and E

Disk quotas:

C only

D only

C and D only

D and E only

C, D, and E

正解:

Answer Area

Microsoft

BitLocker:

C only

D only

C and D only

D and E only

C, D, and E

Disk quotas:

C only

D only

C and D only

D and E only

C, D, and E

Explanation:

BitLocker:

C only
D only
C and D only
D and E only
C, D, and E

Disk quotas:

C only
D only
C and D only
D and E only
C, D, and E

In the Administering Windows Server Hybrid Core Infrastructure materials for storage and file systems, BitLocker Drive Encryption is described as a volume-level encryption technology that operates below the file system. The guides explain that BitLocker can be applied to operating system volumes (which must be NTFS) and to fixed data volumes. For data volumes, BitLocker supports encryption regardless of whether the volume is formatted with NTFS or ReFS, because encryption occurs at the block level; only the boot/OS volume requirement mandates NTFS.

Therefore, on Server1, BitLocker can be used on C (NTFS), D (NTFS), and E (ReFS).

For quotas, the same coursework clarifies two quota mechanisms: NTFS disk quotas and FSRM quotas. The built-in NTFS disk quota feature is tied to the NTFS file system and enforces per-user limits based on file ownership on NTFS volumes only. ReFS does not implement NTFS disk quotas. (FSRM quotas, while more flexible, are also documented as being supported for NTFS volumes, and the exam objective commonly tests recognition that "NTFS disk quotas apply only to NTFS volumes.") Consequently, disk quotas can be configured on C and D (both NTFS), but not on E (ReFS).

Thus, per the Windows Server administration guidance:

* BitLocker: C, D, and E

* Disk quotas: C and D only.

質問: 3

ネットワークにはActive Directoryドメインサービス(AD DS)ドメインが含まれています。このドメインには、User1というユーザーと、次の表に示すサーバーが含まれています。

Name	Server role	DHCP scope
Server1	DHCP Server	Scope1, Scope2
Server2	DHCP Server	Scope3, Scope4

User1 が Scope1 と Scope3 のみを管理できるようにする必要があります。どうすればよいでしょうか？

A. User1 を Server1 および Server2 の DHCP 管理者グループに追加します。

B. IP アドレス管理 (IPAM) を実装します。

C. User1 を DHCP 管理者ドメイン ローカル グループに追加します。

D. Windows Admin Center を実装し、Server1 と Server2 への接続を追加します。

正解: ([正解を表示します](#))

The Windows Server hybrid core curriculum describes IPAM as follows: "IP Address Management (IPAM) provides centralized administration and role-based access control (RBAC) for DHCP and DNS." It further specifies: "IPAM enables delegation such as DHCP Scope Administrator, allowing an operator to manage specific scopes on selected DHCP servers without granting full server administration." By contrast, the built-in groups provide coarse permissions: "Adding a user to DHCP Administrators (local or domain) grants broad administrative rights over the DHCP server and all scopes." Windows Admin Center does not introduce per-scope RBAC for DHCP; it simply surfaces the existing server tools. In the scenario, the requirement is that User1 can manage only Scope1 and Scope3-that is scope-level delegation across two servers. The only option among the choices that provides granular, scope-scoped rights is IPAM, where you assign the DHCP Scope Administrator role to User1 for Scope1 on Server1 and Scope3 on Server2, leaving other scopes unmanaged by that user.

質問: 4

注: この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、指定された目標を達成できる独自のソリューションが含まれています。問題セットには、複数の正解があるものもあれば、正解がないものもあります。

このセクションの質問に回答すると、その質問に戻ることはできなくなります。そのため、これらの質問はレビュー画面に表示されません。

新しいネットワークへの DNS の展開を計画しています。

次の表に示すように、3 つの内部 DNS サーバーがあります。

Name	Location	IP address	Local DNS zone
Server1	Montreal	10.0.1.10	contoso.local
Server2	Toronto	10.0.2.10	east.contoso.local
Server3	Seattle	10.0.3.10	west.contoso.local

contoso.local ゾーンには、east.contoso.local と west.contoso.local のゾーン委任が含まれています。すべての DNS サーバーはルート ヒントを使用します。

すべての DNS サーバーがすべての内部名前空間とインターネット ホストの名前を解決できることを確認する必要があります。

解決策: Server2 で、west.contoso.local の条件付きフォワーダーを作成します。Server3

で、east.contoso.local の条件付きフォワーダーを作成します。

これは目標を満たしていますか？

A. はい

B. いいえ

正解: ([正解を表示します](#))

The DNS planning section of Administering Windows Server Hybrid Core Infrastructure states: "Private internal namespaces are not resolvable via Internet root hints. For resolution across internal DNS zones hosted on different servers, use zone delegation, stub zones, or conditional forwarders so that each server can reach the authoritative source." In the scenario, Server1 hosts contoso.local, which already contains delegations to east.contoso.local and west.contoso.local. However, Server2 (east) and Server3 (west) have no knowledge of the parent zone (contoso.local) and, because all servers use only root hints, queries for contoso.local from Server2/Server3 cannot be resolved by recursion on the public roots. The proposed fix adds a conditional forwarder on Server2 for west.contoso.local and on Server3 for east.contoso.local, which enables cross-child resolution, but does not provide a path to resolve contoso.local from Server2 or Server3.

The guidelines further note: "To ensure all servers can resolve all internal namespaces, configure forwarders (or stub zones/secondaries) to the authoritative servers for each internal zone, including the parent zone." Because the solution omits a forwarder (or stub/secondary) on Server2 and Server3 for contoso.local, it does not meet the goal.

質問: 5

contoso.com という名前の単一ドメイン Active Directory ドメイン サービス (AD DS) フォレストを展開します。

ドメインにサーバーを展開し、サービスを実行するようにサーバーを構成します。

サービスがグループ管理サービス アカウント (gMSA) を使用して認証できることを確認する必要があります。

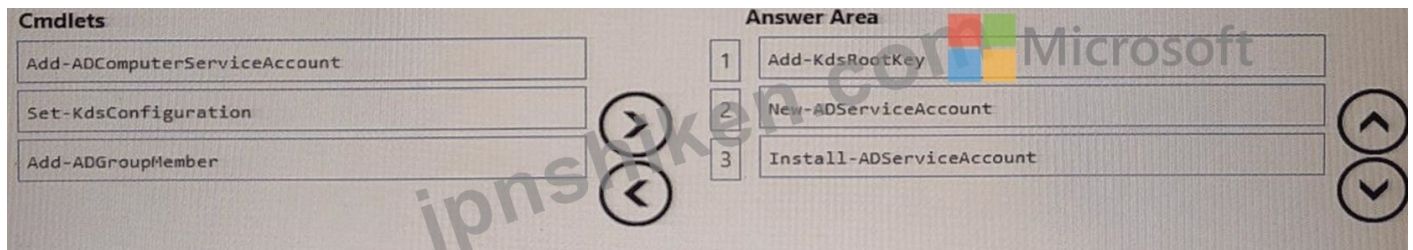
どの 3 つの PowerShell コマンドレットを順番に実行する必要がありますか? 回答するには、適切なコマンドレットをコマンドレットのリストから回答領域に移動し、正しい順序に並べます。

The screenshot shows the exam interface with a list of cmdlets on the left and an empty answer area on the right. The cmdlets are: Add-ADComputerServiceAccount, Set-KdsConfiguration, Add-ADGroupMember, Add-KdsRootKey, New-ADServiceAccount, and Install-ADServiceAccount. The answer area is empty, with navigation arrows on the right.

正解:

The screenshot shows the exam interface with the correct sequence of cmdlets in the answer area. The cmdlets are: Add-KdsRootKey, New-ADServiceAccount, and Install-ADServiceAccount. The answer area is highlighted with a red dashed box, and the cmdlets are in the correct order.

Explanation:



The Administering Windows Server Hybrid Core Infrastructure materials explain that group Managed Service Accounts (gMSAs) rely on the Key Distribution Service (KDS) to generate and distribute the managed password. Therefore, the first step in a new forest (or where no key exists yet) is to create a KDS root key:

Add-KdsRootKey. The guide states that "the KDS root key is required once per forest before any gMSA can be created or used," and without it, password material cannot be issued.

Next, you create the gMSA in Active Directory using New-ADServiceAccount. When creating the account, you specify the principals that are allowed to retrieve the managed password (for example, the computer account of Server1 or a group). The study content notes: "Use New-ADServiceAccount with - PrincipalsAllowedToRetrieveManagedPassword to authorize the host computers that will run the service." This removes the need to separately run mapping cmdlets.

Finally, on the target server, you install the gMSA locally using Install-ADServiceAccount. The documentation emphasizes: "After the account is created in AD, the host computer must install the gMSA so the Local Security Authority can obtain and maintain the password automatically."

Because authorization is granted at creation time, Add-ADComputerServiceAccount is not required in this minimal, correct sequence.

質問: 6

次の表に示すように、Windows Server 2022 を実行するサーバーがあります。

Name	Location	Description
Server1	On-premises	Hosts a Microsoft SQL Server 2019 instance
Server2	Azure	Contains the .NET SDK

Server2 には、App1 という名前の .NET アプリが含まれています。

App1からServer1上のSQL ServerインスタンスへのWebSocket接続を確立する必要があります。

ソリューションは以下の要件を満たす必要があります。

- オンボードで開く必要のあるネットワークポートの数を最小限に抑える

構内ネットワーク ファイアウォール。

- 管理上の労力を最小限に抑えます。

最初に何を作成すればよいですか？

- A. Azure Relay 名前空間
- B. Azure VPNゲートウェイ
- C. WFCリレー接続
- D. ハイブリッド接続

正解: ([正解を表示します](#))

The hybrid connectivity module details Azure Relay - Hybrid Connections for reaching on-premises services securely without inbound firewall rules. It states: "Hybrid Connections use WebSockets over outbound TCP

443 from both ends, enabling apps in Azure to connect to on-premises endpoints with no VPN and minimal firewall changes." The setup sequence is: (1) Create an Azure Relay namespace, (2) Create a Hybrid Connection inside that namespace, and **(3) install the on-premises Hybrid Connection Manager to establish the outbound listener to Azure.**" This approach meets the requirements: a WebSocket-based connection from App1 to SQL Server on Server1, minimizing open ports (only outbound 443) and administrative effort (no site-to-site VPN or complex routing). A VPN gateway would require additional configuration and more open ports; a WCF relay is a different relay type for WCF endpoints, not needed for generic TCP/WebSocket scenarios; and a hybrid connection cannot be created until a Relay namespace exists. Thus, the first object to create is an Azure Relay namespace.

質問: 7

オンプレミスの Windows デバイスがあります。

VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。

オンプレミス ネットワークと VNet1 の間にサイト間 (S2S) VPN を作成する必要があります。

作成する必要がある 3 つのリソースはどれですか。それぞれの正解はソリューションの一部を示します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

- A. ネットワーク セキュリティ グループ (NSG)
- B. ローカルネットワークゲートウェイ
- C. Azure NATゲートウェイ
- D. VPN接続
- E. 仮想ネットワークゲートウェイ
- F. Azureルートサーバー

正解: ([正解を表示します](#))

質問: 8

タスク1

DC2 が contoso.com のスキーマ マスターであることを確認する必要があります。

正解:

See the solution of this Task below.

Explanation:

Step-by-Step Guide: Seizing/Transferring the Schema Master Role to DC2

Step 1: Log in to DC2

Use an account that is a member of the Schema Admins, Enterprise Admins, and Domain Admins groups.

Step 2: Register the Schema Snap-in

The Schema snap-in is not loaded by default.

Open Command Prompt as Administrator.

Type the following command to register the schema management DLL:

```
powershell
```

```
Copy
```

```
regsvr32 schmmgmt.dll
```

Step 3: Open MMC (Microsoft Management Console)

Press Windows + R, type mmc, and hit Enter.

In MMC, go to File > Add/Remove Snap-in.

Select Active Directory Schema, then click Add > OK.

Step 4: Connect to DC2

In the Active Directory Schema console, right-click Active Directory Schema and select Change Active Directory Domain Controller.

In the dialog box, select DC2 and click OK.

This will connect the console to DC2.

Step 5: Transfer the Schema Master Role

Right-click Active Directory Schema again and select Operations Master.

In the Change Schema Master dialog box, confirm that DC2 is shown as the target.

Click the Change button to transfer the Schema Master role to DC2.

Click Yes when prompted to confirm the transfer.

Step 6: Verify the Transfer

In the same dialog box, ensure that DC2 is now listed as the Schema Master.

Optionally, run the following command in PowerShell to verify:

```
netdom query fsmo
```

The Schema Master should now be DC2.

質問: 9

ネットワークには、contoso.com という名前の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

どのサーバーがドメインの PDC エミュレーターであるかを特定する必要があります。

解決策: Active Directory ユーザーとコンピューターから、コンソール ツリーで contoso.com を右クリックし、[操作マスター] を選択します。これで目標は達成されましたか？

A. はい

B. いいえ

正解: [\(正解を表示します\)](#)

The Administering Windows Server Hybrid Core Infrastructure module covering GUI management tools states that Active Directory Users and Computers (ADUC) exposes the domain-scoped FSMO roles through the Operations Masters dialog. By right-clicking the domain node (e.g., contoso.com) and selecting Operations Masters, administrators can view the RID, PDC, and Infrastructure masters and see (or change) the current role holder. The materials clarify that these

three roles are domain-wide and are surfaced in ADUC, whereas the forest-wide roles (Schema Master and Domain Naming Master) are viewed in the Active Directory Schema and Active Directory Domains and Trusts consoles, respectively.

Therefore, using ADUC exactly as described-right-clicking the domain and choosing Operations Master- does meet the goal of identifying which server holds the PDC Emulator role in that domain. This method is especially useful in GUI-enabled admin stations and supports safe, controlled transfers when appropriate permissions are present.

質問: 10

ネットワークには、contoso.com という名前の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

どのサーバーがドメインの PDC エミュレーターであることを特定する必要があります。

解決策: Active Directory サイトとサービスから、コンソール ツリーで Default-First-Site-Name を右クリックし、[プロパティ] を選択します。

これは目標を満たしていますか？

A. はい

B. いいえ

正解: B ([コメントを发表する](#))

The course content distinguishes site management from FSMO role administration. Active Directory Sites and Services is used to manage sites, subnets, site links, replication topology, and server objects (NTDS Settings), not domain or forest operations master roles. The documentation explains that FSMO roles are either forest-wide (Schema, Domain Naming) or domain-wide (RID, PDC, Infrastructure) and are exposed via ADUC (domain roles), Active Directory Domains and Trusts (Domain Naming), and Active Directory Schema (Schema), or by command-line tools like NETDOM and NTDSUTIL. Right-clicking Default-First-Site-Name and opening Properties shows site-level configuration (e.g., inter-site transports, licensing, location metadata) but does not display FSMO role holders. Consequently, the proposed action does not meet the goal of identifying the PDC Emulator. To meet the goal, use ADUC # Operations Masters, netdom query fsmo, or ntdsutil roles as laid out in the administration guide.

質問: 11

ディスクが1つ搭載された Server1 というWindows Serverコンテナホストがあります。Server1では、次の表に示すコンテナを起動する予定です。

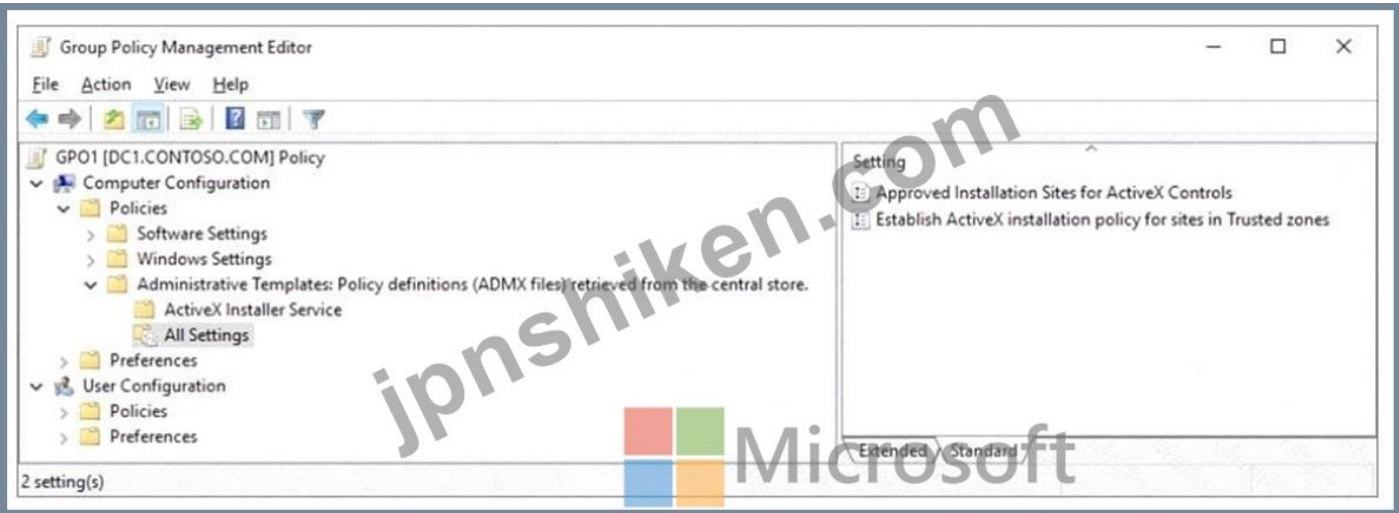
Name	Description
Container1	Container1 is a Windows container that contains a web app in development. The container must NOT share a kernel with other containers.
Container2	Container2 is a Linux container that runs a web app. The container requires two static IP addresses.
Container3	Container3 is a Windows container that runs a database. The container requires a static IP address.

各コンテナにはどの隔離モードを使用できますか？回答するには、回答エリアで適切なオプションを選択してください。注：正しい選択ごとに1ポイント獲得できます。

ネットワークには、contoso.com という Active Directory ドメイン サービス (AD DS) ドメインが含まれています。セントラル ストアを実装します。

GP01 という名前の新しいグループ ポリシー オブジェクト (GPO) を作成します。

GP01 を編集しようとする、展示に示されている設定が表示されます。(「展示」タブをクリックします。)すべての設定が利用可能であることを確認する必要があります。



解決策: \\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions フォルダを削除します。

これで目標は達成されますか？

- A. いいえ
- B. はい

正解: A ([コメントを发表する](#))

質問: 12

ネットワークには Active Directory ドメイン サービス (AD DS) ドメインが含まれています。ドメインには、次の表に示すドメイン コントローラーが含まれています。

Name	Description
DC1	PDC emulator, RID master, and global catalog server
DC2	Infrastructure master and domain naming master
DC3	Schema master
RODC1	Read-only domain controller (RODC)

攻撃者が RODC1 のコンピューター アカウントを侵害した場合に、攻撃者が従業員番号 AD DS 属性を表示できないことを確認する必要があります。どのパーティションを変更する必要がありますか？

- A. 構成
- B. グローバルカタログ
- C. ドメイン
- D. スキーマ

正解: **D** ([コメントを发表する](#))

The domain services security section describes the RODC Filtered Attribute Set (FAS), which prevents selected attributes from replicating to Read-Only Domain Controllers. The curriculum explains: "Attributes that must not be exposed on RODCs are added to the RODC filtered attribute set. This setting is defined in the schema partition; once an attribute is flagged as CONFIDENTIAL and added to FAS, it is not replicated to any RODC." Because the attacker may have compromised RODC1's computer account, protection requires ensuring sensitive attributes (e.g., employeeNumber) are never present on that RODC. Changes for FAS membership and the confidential bit are schema-level operations and apply forest-wide. Modifying the domain or configuration partitions will not change which attributes replicate to RODCs, and the global catalog is not a writable partition; it aggregates a subset of attributes but honors the schema's FAS configuration. Therefore, to ensure Employee-Number cannot be viewed if RODC1 is compromised, you modify the schema to place the attribute in the RODC filtered attribute set (and, if required, mark it confidential).

質問: 13

ネットワークにはActive Directoryドメインサービス(AD DS)ドメインが含まれています。このドメインには、次の表に示すサーバーが含まれています。

Name	Type
DC1	Domain controller
Server1	Member server
Server2	Member server

ドメインには次の表に示すユーザーが含まれます。

Name	Member of
User1	Contoso\Administrators
User2	Contoso\Remote Management Users
User3	Server2\Power Users

Server2でEnable-PSRemotingコマンドレットを実行します。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに1ポイントが加算されます。

Answer Area



Microsoft

Statements

User1 can establish a PowerShell remoting session from Server1 to Server2.

Yes

☐

No

☐

User2 can establish a PowerShell remoting session from Server2 to DC1.

☐☐

User3 can establish a PowerShell remoting session from Server1 to Server2.

☐☐

正解:

Answer Area	
Statements	
User1 can establish a PowerShell remoting session from Server1 to Server2.	Yes ☒ No ☐
User2 can establish a PowerShell remoting session from Server2 to DC1.	Yes ☐ No ☒
User3 can establish a PowerShell remoting session from Server1 to Server2.	Yes ☐ No ☒

Explanation:

User1 can establish a PowerShell remoting session from Server1 to Server2. Yes User2 can establish a PowerShell remoting session from Server2 to DC1. No User3 can establish a PowerShell remoting session from Server1 to Server2. No PowerShell Remoting (WinRM) security and connectivity are central themes in the Administering Windows Server Hybrid Core Infrastructure curriculum. The ability to establish a remote session is determined by three factors: the service state on the target, the network path, and the user's effective permissions.

* User1 (Server1 to Server2): On Server2, the Enable-PSRemoting cmdlet has been executed. By default, this configures the WinRM service to allow connections from members of the local Administrators group. Since User1 is a member of the Contoso\Administrators group, and this domain group is a member of the local Administrators group on all member servers by default, User1 has the necessary rights to establish a session to Server2.

* User2 (Server2 to DC1): While User2 is a member of the Contoso\Remote Management Users group-a group specifically designed to provide non-administrative users with remoting access-the scenario explicitly states that Enable-PSRemoting was run only on Server2. For any user to establish a remoting session to DC1, the WinRM listener must first be enabled and configured on that specific target. Because the prompt does not indicate that remoting was enabled on DC1, the connection will fail regardless of User2's group membership.

* User3 (Server1 to Server2): User3 is a member of the local Server2\Power Users group. According to official documentation, the Power Users group does not possess the default permissions required to access the WinRM endpoints (Microsoft.PowerShell or Microsoft.Windows.ServerManager). Only members of the local Administrators or Remote Management Users groups are granted these rights when Enable-PSRemoting is executed. Therefore, User3 cannot establish the session.

質問: 14

ネットワークには DHCP サーバーが含まれています。

新しいサブネットを追加し、そのサブネットに Windows Server を展開することを計画しています。

サーバーを DHCP リレー エージェントとして使用する必要があります。

どの役割をサーバーにインストールする必要がありますか？

- A. ネットワーク ポリシーとアクセス サービス
- B. リモートアクセス
- C. ネットワークコントローラー
- D. DHCP サーバー

正解: ([正解を表示します](#))

When Windows Server is used as a DHCP Relay Agent, the feature is delivered through Routing and Remote Access Service (RRAS). The AZ-800 content explains: "The DHCP Relay Agent is a component of RRAS and is installed by adding the Remote Access role and enabling the Routing role service." After installation, admins configure the relay interface(s) and specify the IP addresses of one or more DHCP servers to which broadcast DHCPDISCOVER messages are forwarded. The documentation further notes: "Network Policy and Access Services (NPS) provides RADIUS and policy evaluation, not DHCP relay; the DHCP Server role offers DHCP lease services, not relay." Thus, to prepare the server that sits on the new subnet to forward DHCP requests, you must install the Remote Access role (and within it, the Routing role service), then add the DHCP Relay Agent in the RRAS console or via PowerShell.

質問: 15

contoso.com という名前の新しい Active Directory ドメイン サービス (AD DS) フォレストを展開します。このドメインには、DC1、DC2、DC3 という 3 つのドメイン コントローラーが含まれています。

Default-First-Site-Name の名前を Site1 に変更します。

DC1、DC2、DC3 を異なる場所にあるデータセンターに発送する予定です。

次の要件を満たすには、DC1、DC2、DC3 間のレプリケーションを構成する必要があります。

各ドメイン コントローラは、独自の Active Directory サイトに存在する必要があります。

各サイト間のレプリケーション スケジュールは個別に制御する必要があります。

レプリケーションの中断は最小限に抑える必要があります。

Active Directory サイトとサービス コンソールで順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

Actions

Create a connection object between DC1 and DC2.

Create an additional site link that contains Site1 and Site2.

Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3.

Create a connection object between DC2 and DC3.

Remove Site2 from DEFAULTIPSITELINK.

Answer Area



正解:

Actions

Create a connection object between DC1 and DC2.

Create an additional site link that contains Site1 and Site2.

Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3.

Create a connection object between DC2 and DC3.

Remove Site2 from DEFAULTIPSITELINK.

Answer Area

Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3.

Create an additional site link that contains Site1 and Site2.

Remove Site2 from DEFAULTIPSITELINK.

Explanation:

Create two additional sites named Site2 and Site3. Move DC2 to Site2 and DC3 to Site3.

Create an additional site link that contains Site1 and Site2.

Remove Site2 from DEFAULTIPSITELINK.

The Administering Windows Server Hybrid Core Infrastructure guidance for AD DS site design states that each physical location should be mapped to its own Active Directory site so that replication and logon traffic can be controlled and optimized per location. The documentation explains that when you deploy new sites, domain controllers must be moved into the corresponding site containers to ensure intrasite replication uses the local site topology and intersite replication follows site links. It also emphasizes that site links define replication cost, schedule, and frequency between sites; by creating separate site links for the pairs you want to manage, you can independently control replication schedules for those paths. The guides further note that new sites are placed in DEFAULTIPSITELINK by default, and that administrators can create additional site links and then remove a site from DEFAULTIPSITELINK to prevent it from inheriting the default schedule and cost—thereby isolating schedules per site pair. Finally, the KCC/ISTG automatically generate the required connection objects, so you generally should not create manual connection objects unless you have a specific exception. Following these principles: create Site2 and Site3 and move DCs, add a dedicated link (Site1-Site2) to set its own schedule, and remove Site2 from DEFAULTIPSITELINK so Site1-Site2 and Site1-Site3 replication can be controlled independently while minimizing replication interruptions.

質問: 16

ネットワークにはActive Directoryドメインサービス(AD DS)フォレストが含まれています。フォレストには、Site1、Site2、Site3という3つのActive Directoryサイトが含まれています。各サイトには2つのドメインコントローラーが含まれています。これらのサイトはDEFAULTIPSITELINKを使用して接続されています。

クライアントコンピューターのみを含む新しいブランチ オフィスを開設します。

新しいオフィスのクライアント コンピューターが主に Site1 のドメイン コントローラーによって認証されるようにする必要があります。

解決策: Site1 に関連付けられた新しいサブネット オブジェクトを作成します。

これは目標を満たしていますか?

A. はい

B. いいえ

正解: ([正解を表示します](#))

In the Administering Windows Server Hybrid Core Infrastructure guidance for "Implement and manage AD DS sites and replication," Microsoft explains that client computers are site-aware and "select domain controllers in their own site whenever possible." A client's site membership is determined solely by the mapping of its IP subnet to an AD DS site. The material further notes that administrators should "create subnet objects and associate them to the appropriate site so that clients resolve and authenticate to DCs in that site; if a subnet is not mapped, clients may use any reachable site through site coverage." By creating a new subnet object for the branch office and associating it with Site1, all clients in that subnet will treat Site1 as their site and will therefore query and authenticate primarily against Site1's domain controllers, only failing over to other sites if necessary via DEFAULTIPSITELINK. This meets the stated goal without requiring domain controllers in the new office, because site affinity controls the preferred DC selection for Kerberos

/NTLM authentication and LDAP/GC queries.

有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/AZ-800J-mondaishu> **262**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

Windows Server を実行し、次の構成を持つ VM1 という名前の Azure 仮想マシンがあります。

サイズ: D2s_v4

オペレーティング システム ディスク: 127 GiB 標準 SSD

データ ディスク 128 GiB 標準 SSD

仮想マシン世代: Gen 2

VM1 に対して次の変更を行う予定です。

仮想マシンのサイズを D4s_v4 に変更します。

データ ディスクを取り外します。

新しい標準 SSD を追加します。

VM1 のダウンタイムが必要な変更はどれですか?

- A. データ ディスクのみを取り外し、新しい標準 SSD を追加します。
- B. データディスクのみを切り離します。
- C. 仮想マシンのサイズのみを変更します。
- D. 新しい標準 SSD のみを追加します。

正解: **C** ([コメントを发表する](#))

Within the Manage and maintain Windows Server IaaS virtual machines section, the guide notes operational impacts of common VM changes. It states: "Resizing a virtual machine changes its compute allocation; the VM is restarted and may require stop/deallocate if the target size isn't available on the current host.

Expect downtime during a size change." In contrast, the storage guidance says: "Managed data disks can be attached or removed from a running VM; these operations do not require a VM redeploy and typically do not incur downtime." Adding a new standard SSD (data disk) is supported online, and detaching a data disk can also be performed without shutting down the VM (Windows may require a rescan and clean removal in the OS, but the VM remains running). Therefore, among the proposed changes, the one that requires downtime is changing the VM size to D4s_v4, because the platform must restart (and sometimes deallocate) the VM to re-provision compute resources, whereas attaching/detaching data disks does not inherently require downtime.

質問: 18

タスク 1 で使用できる 2 つの言語はどれですか。それぞれの正解は完全な解答を示します。

注意: 正しい選択ごとに 1 ポイントが加算されます。

- A. Java
- B. 上腕二頭筋
- C. JavaScript
- D. Python
- E. PowerShell

正解: ([正解を表示します](#))

The exam materials state that Azure Automation runbooks can be authored in PowerShell and Python (along with Graphical and PowerShell Workflow where noted). The module on "Automate management in hybrid environments" specifies: "Runbooks support PowerShell for Windows-based automation and Python for cross- platform scenarios." It further explains that these languages integrate with Automation Accounts, modules /packages, credentials, and managed identities to run tasks on Azure or hybrid resources through the Hybrid Runbook Worker. Languages such as Java, JavaScript, or Bicep are not runbook languages (Bicep is used for ARM template deployments, not runbook execution). Accordingly, Task1 can be implemented in PowerShell and Python.

質問: 19

タスク9

contoso.com という名前の DNS ゾーンの読み取り専用コピーを SRV2 に複製する必要があります。

正解:

See the solution of this Task below.

Explanation:

Objective:

Create a read-only copy of the DNS zone contoso.com on SRV2.

Step-by-Step Guide: Using a Secondary Zone

Step 1: Log in to SRV2

Log in to SRV2 (where you want to host the secondary zone) using an account with local administrative privileges.

Step 2: Open DNS Manager

Press Windows + R, type dnsmgmt.msc, and press Enter.

Step 3: Create a Secondary Zone

In the DNS Manager, expand the server node for SRV2.

Right-click Forward Lookup Zones and select New Zone.

The New Zone Wizard opens.

Step 4: Configure the Secondary Zone

Zone Type:

Select Secondary zone and click Next.

Zone Name:

Type contoso.com and click Next.

Master DNS Servers:

Enter the IP address of the master DNS server that hosts the primary zone (e.g., SRV1's IP).

Click Next.

Finish:

Review the settings and click Finish.

Step 5: Allow Zone Transfers on the Primary Server

On SRV1 (or the DNS server hosting the primary zone):

Open DNS Manager.

Right-click the contoso.com zone and select Properties.

Go to the Zone Transfers tab.

Check Allow zone transfers.

Specify SRV2's IP address (or allow to any server if needed).

Step 6: Verify Zone Replication

On SRV2, refresh the Forward Lookup Zones in DNS Manager.

The contoso.com zone should now appear as a Secondary zone.

Check the Zone Transfer status to ensure it successfully replicated.

質問: 20

ネットワークにはActive Directoryドメインサービス(AD DS)ドメインが含まれています。このドメインには、次の表に示すドメインコントローラーが含まれています。

Name	Description
DC1	Has the schema master, infrastructure master, and domain naming master roles
DC2	Has the PDC emulator and RID master roles and is a global catalog server
DC3	None

DC3 をドメインの権限のあるタイム サーバーとして構成する必要があります。

どの操作マスターの役割を DC3 に転送し、どのコンソールを使用する必要がありますか？ 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Role: PDC emulator
Domain naming master
Infrastructure master
PDC emulator
RID master
Schema master

Console: Active Directory Users and Computers
Active Directory Admin
Active Directory Doma
Active Directory Sites and Services
Active Directory Users and Computers

正解:

Answer Area

Microsoft

Role: PDC emulator
Domain naming master
Infrastructure master
PDC emulator
RID master
Schema master

Console: Active Directory Users and Computers
Active Directory Admin
Active Directory Doma
Active Directory Sites and Services
Active Directory Users and Computers

Explanation:

Answer Area

Role: PDC emulator
These are the selections for Role:

Console: Active Directory Users and Computers

In the Administering Windows Server Hybrid Core Infrastructure materials for AD DS operations, the time service hierarchy is tied to FSMO roles. The guide states that "the domain controller holding the PDC Emulator role acts as the authoritative time source for the domain; other DCs in the domain synchronize time from the PDC emulator, and domain members synchronize from their logon DCs." For multi-domain forests, it further clarifies that "the PDC Emulator in the forest root domain is the authoritative source for the forest and should be configured to sync with an external, reliable NTP source." Regarding management tools, the exam guide specifies that "domain-wide FSMO roles (RID, PDC Emulator, and Infrastructure) are transferred by using Active Directory Users and Computers: right-click the domain, choose Operations Masters, and select the relevant tab." By contrast, "Schema Master is managed with the Active Directory Schema snap-in and Domain Naming Master with Active Directory Domains and Trusts." Therefore, to make DC3 the authoritative time server for the domain, you must transfer the PDC Emulator role to DC3 and perform the transfer using Active Directory Users and Computers (ADUC) via the Operations Masters dialog.

質問: 21

WindowsコンテナをホストするServer1というサーバーがあります。複数のコンテナを持つアプリケーションをデプロイする予定です。各コンテナは、アプリケーションのデプロイをサポートするDockerネットワークを作成する必要があります。どのタイプのネットワークを作成すればよいですか？

- A. transparent
- B. l2bridge
- C. NAT
- D. l2tunnel

正解: ([正解を表示します](#))

In the context of Windows Server Hybrid Core Infrastructure and container networking, choosing the correct network driver is critical for application deployment. According to official documentation, the l2bridge (Layer 2 Bridge) network mode is used when container hosts are connected to the same IP subnet. In this configuration, each container is assigned an IP address from the same prefix as the container host. All container traffic is bridged to the physical network through an external Hyper-V Virtual Switch. Because the containers share the same underlying network infrastructure as the host, they are visible to the rest of the physical network without requiring Network Address Translation (NAT).

The documentation specifies that for multi-node clusters or deployments where containers must be directly reachable on the physical network via their own IP addresses, l2bridge is the standard choice. This differs from NAT, which uses a private internal IP range and translates traffic through the host's IP, and Transparent mode, which is often used for individual hosts where the container is directly connected to the physical network but can have complexities in virtualized environments. l2tunnel is specifically used for Microsoft Cloud Stack (Azure Stack HCI) and SDN scenarios, typically involving encapsulation, which is not the standard requirement for a general multi-container application deployment on a single server unless specified.

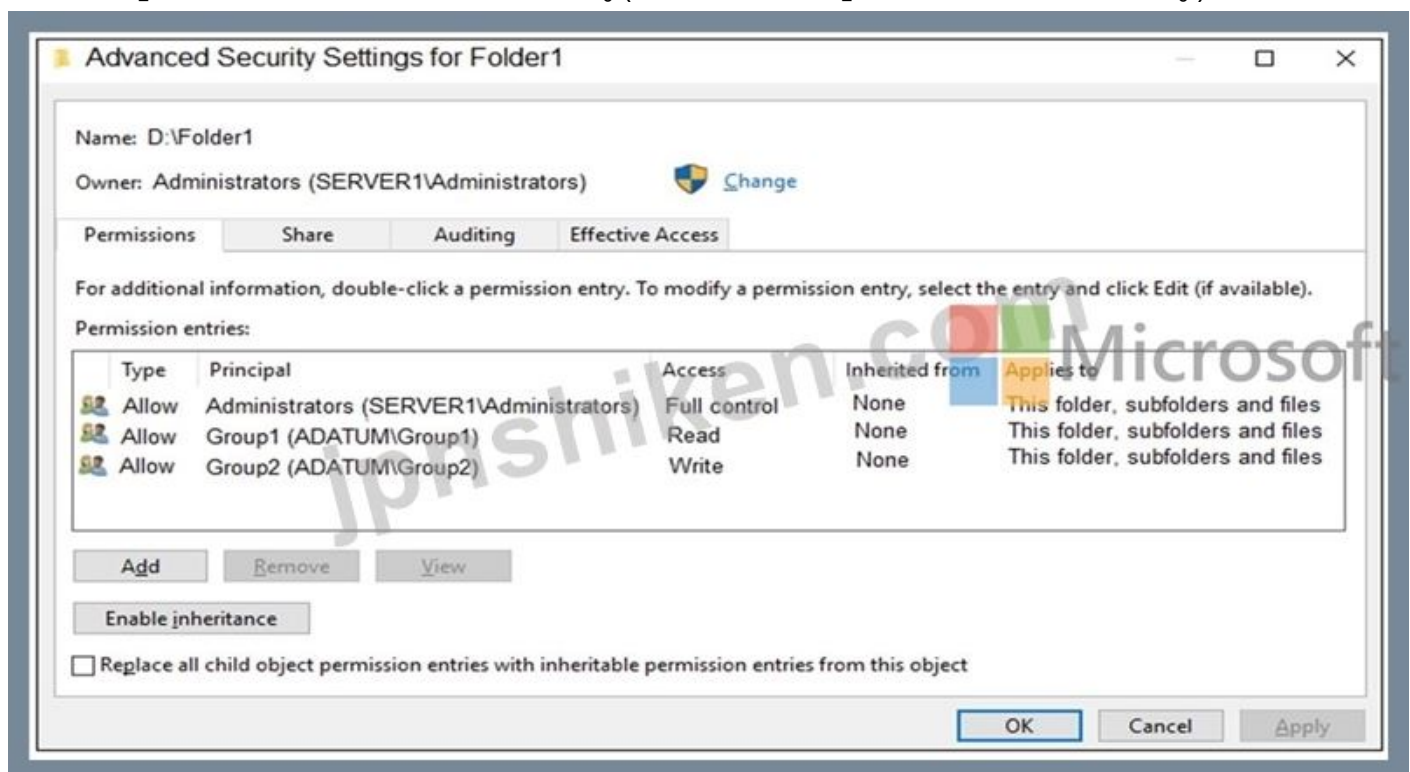
Therefore, for a high-performance, direct-access network that bridges traffic at Layer 2, l2bridge is the verified architectural choice for Windows containers.

質問: 22

ネットワークには、adatum.com という Active Directory ドメイン サービス (AD DS) ドメインが含まれています。このドメインには、Server1 というサーバーと、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Server1にはD:\Folder1というフォルダがあります。Folder1の詳細なセキュリティ設定は、「アクセス許可」の図に示されているとおりです。(「アクセス許可」タブをクリックします。)



Folder1 は次の構成を使用して共有されます。

Path : D:\Folder1
Name : Share1
ShareType : FileSystemDirectory
FolderEnumerationMode : Unrestricted

Share1 の共有権限を次の表に示します。

Group	Permission
Group1	Allow – Change
Group3	Allow – Full Control

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Statements	Yes	No
User1 can read the files in Share1.	☐	☐
User3 can delete files in Share1.	☐	☐
If User2 connects to \\Server1.adatum.com from File Explorer, Share1 will be listed.	☐	☐

正解:

Statements	Yes	No
User1 can read the files in Share1.	☒	☐
User3 can delete files in Share1.	☐	☒
If User2 connects to \\Server1.adatum.com from File Explorer, Share1 will be listed.	☒	☐

Explanation:

The course content for Administering Windows Server Hybrid Core Infrastructure explains the effective permission model for SMB shares: "Access to a shared folder is the most restrictive result of the Share permissions and the NTFS permissions. Share permissions control access over the network, while NTFS permissions control access to the file system itself. The effective

permission is the intersection-users must have permission in both places." It also clarifies typical rights: "Read includes viewing and opening; Change /Modify includes creating, changing, and deleting; Full Control adds the ability to change permissions and take ownership." Applying this: User1 is in Group1. Share1 grants Group1 = Change, and NTFS on D:\Folder1 grants Group1 = Read. The intersection is Read, so User1 can read files. User3 is in Group3. Share1 grants Group3 = Full Control, but NTFS has no entry for Group3 (and no broader Allow that would include it).

Without NTFS Modify/Delete, User3 cannot delete.

Regarding visibility, the share was created with FolderEnumerationMode = Unrestricted. The training states: "With Unrestricted enumeration, the share (and items) are not hidden based on access; users may see the share even if they lack permissions, though access will be denied when opened. Access-Based enumeration hides items from users without permission." Therefore, when User2 (member of Group2) browses \\Server1, Share1 will be listed, though opening it would rely on permissions.

質問: 23

タスク3

SRV1 上で、mcr.microsoft.com/windows/servercore/iis イメージを使用するコンテナを実行する必要があります。コンテナのポート 60 を SRV1 のポート 5001 に公開し、コンテナをバックグラウンドで実行する必要があります。

正解:

See the solution of this Task below.

Explanation:

To run a container on SRV1 using the mcr.microsoft.com/windows/servercore/iis image, publish port 60 on the container to port 5001 on SRV1, and ensure it runs in the background, you can follow these steps:

Step 1: Pull the IIS Image First, pull the IIS image from the Microsoft Container Registry:

```
docker pull mcr.microsoft.com/windows/servercore/iis
```

Step 2: Run the Container Next, run the container with the required port mapping and ensure it runs in the background using the -d flag:

```
docker run -d -p 5001:60 --name iis_container mcr.microsoft.com/windows/servercore/iis
```

This command will start a container named iis_container using the IIS image, map port 60 inside the container to port 5001 on SRV1, and run the container in detached mode.

Step 3: Verify the Container is Running To verify that the container is running and the port is published, use the following command:

```
docker ps
```

This will list all running containers and show the port mappings.

Step

4: Access the IIS Server You can now access the IIS server running in the container by navigating to http://

<SRV1_IP>:5001 in a web browser, where <SRV1_IP> is the IP address of SRV1.

Note: Ensure that Docker is installed on SRV1 and that the port 5001 is open on the firewall to allow incoming connections1.

By following these steps, you should be able to run the IIS container on SRV1 with the specified port mapping and have it running in the background.

質問: 24

Windows Server を実行し、Hyper-V サーバー ロールがインストールされている Server1 という名前のサーバーがあります。

サーバー 1 をリモートで管理するときに、ヘルプデスク ユーザーが使用できる Hyper-V モジュール コマンドレットを 10 個に制限する必要があります。

Just Enough Administration (JEA) を構成し、ロール機能とセッション構成ファイルを正常に構築します。

PowerShell コマンドをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Microsoft

Enter-PSSession

New-PSSessionConfigurationFile

Register-PSSessionConfiguration

-Path .\HyperVJeaConfig

.ps1

.psm1

.psrc

.pssc

-Name 'HyperVJeaHelpDesk' -Force

正解:

Answer Area

Microsoft

Enter-PSSession

New-PSSessionConfigurationFile

Register-PSSessionConfiguration

-Path .\HyperVJeaConfig

.ps1

.psm1

.psrc

.pssc

-Name 'HyperVJeaHelpDesk' -Force

Explanation:

Microsoft

Enter-PSSession

New-PSSessionConfigurationFile

Register-PSSessionConfiguration

-Path .\HyperVJeaConfig

.ps1

.psm1

.psrc

.pssc

-Name 'HyperVJeaHelpDesk' -Force

In Just Enough Administration (JEA), you restrict what remote users can do by publishing a PowerShell session endpoint that references a session configuration file and one or more role capability files. The AZ-

800 "Administering Windows Server Hybrid Core Infrastructure" materials explain that a JEA deployment follows this order: (1) create role capability files (.psrc) in a module's RoleCapabilities folder to enumerate allowed cmdlets, functions, and parameters; (2) author a session configuration file (.pssc)-typically with New-PSSessionConfigurationFile-that maps users or groups to the role capabilities; and (3) register the endpoint with Register-PSSessionConfiguration, supplying the .pssc path and a Name for the endpoint. Only after registration can helpdesk users connect to the constrained endpoint.

Critically, among the listed cmdlets, Register-PSSessionConfiguration is the one that accepts -Name and -Path to a .pssc file, which matches the prompt (-Path .\hypervJeaConfig __ -Name 'hypervJeaHelpDesk' -Force). Enter-PSSession is for connecting to an already published endpoint, and New-PSSessionConfigurationFile creates the .pssc but does not publish it.

Likewise, file types .ps1 (script), .psm1 (module), and .psrc (role capability) are not valid for the -Path parameter when registering an endpoint.

Therefore, the correct completion is:

Register-PSSessionConfiguration -Path .\hypervJeaConfig.pssc -Name 'hypervJeaHelpDesk' -Force.

質問: 25

Marketing OU ユーザーの storage1 へのアクセスが技術要件を満たしていることを確認する必要があります。

何を実装すべきでしょうか？

- A. Microsoft Entra Connect クラウド同期
- B. Active Directory フェデレーション サービス (AD FS)
- C. ステージングモードのMicrosoft Entra Connect
- D. Microsoft Entra Connect がアクティブ モードです

正解: ([正解を表示します](#))

The Administering Windows Server Hybrid Core Infrastructure content notes that Microsoft Entra Connect cloud sync uses lightweight agents and supports synchronizing specific OUs from multiple forests into a single tenant. The guide highlights that cloud sync "is designed for multi-forest or cross-organization scenarios and allows scoping to selected OUs and groups," enabling granular onboarding of just the identities you need. The requirement says "the users in the Marketing OU (in Fabrikam's forest) must have access to storage1." Granting access to Azure Files using Entra-based authorization requires that those users exist in the same Entra tenant. Cloud sync enables importing only the Fabrikam Marketing OU into A. Datum's tenant without establishing full trust for all users. Azure AD Connect in active or staging mode would target the A.

Datum forest and isn't intended for selectively bringing in a separate partner forest OU; AD FS is a federation solution and does not create tenant objects for ACLs on Azure resources like Azure

Files. Therefore, implement Microsoft Entra Connect cloud sync and scope it to the Marketing OU to meet the requirement.

質問: 26

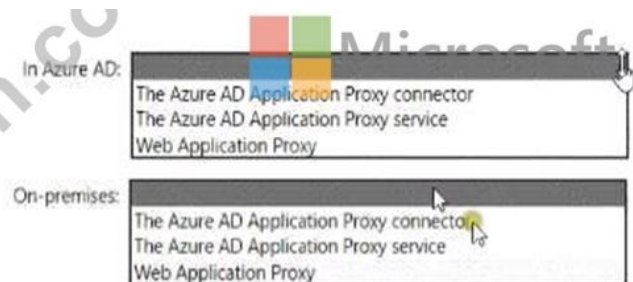
Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory Domain Services (AD DS) ドメインがあり、Kerberos 認証のみをサポートする WebApp1 という名前のオンプレミスの Web アプリがあります。

ユーザーが Azure AD アカウントを使用して WebApp1 にアクセスできるようにする必要があります。このソリューションでは、管理作業を最小限に抑える必要があります。

何を設定する必要がありますか？ 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:

Answer Area



Explanation:

Answer Area

In Azure AD: The Azure AD Application Proxy service

On-premises: The Azure AD Application Proxy connector

In the Administering Windows Server Hybrid Core Infrastructure objectives for publishing on-premises apps to cloud identities, Azure AD Application Proxy is the prescribed solution for exposing internal, Kerberos-based web apps to Azure AD users with minimal changes. The guidance explains that Application Proxy is a cloud service in Azure AD which publishes internal HTTP/HTTPS applications and supports Kerberos Constrained Delegation (KCD) so that "users authenticate with Azure AD and the service performs single sign-on to the on-premises app using Kerberos." To enable it, you turn on the Application Proxy service in the Azure AD tenant and configure the application object for passthrough/Pre-Auth and KCD. The on-premises requirement is to install the Azure AD Application Proxy connector on a domain-joined Windows Server that can reach the internal application; the connector establishes outbound-only connections to the service, avoiding inbound firewall changes and minimizing administrative effort. The materials

also contrast this with Web Application Proxy (WAP) for AD FS publishing, which requires additional infrastructure and does not leverage Azure AD cloud pre-authentication. Therefore, to let Azure AD accounts reach an on-premises Kerberos-only app with least effort, configure the Azure AD Application Proxy service (in Azure AD) and deploy the Azure AD Application Proxy connector (on-premises), then enable KCD for the published app.

質問: 27

タスク9

グループ管理サービス アカウント (gMSA) を作成する予定です。

gMSA の作成をサポートするようにドメインを構成する必要があります。

正解:

See the solution of this Task below.

Explanation:

To configure the domain to support the creation of gMSAs, you need to perform the following steps:

- * On a domain controller or a computer that has the Remote Server Administration Tools (RSAT) installed, open PowerShell as an administrator and run the following command to install the Active Directory module:

```
Install-WindowsFeature -Name RSAT-AD-PowerShell
```

- * Run the following command to create a Key Distribution Service (KDS) root key, which is required for generating passwords for gMSAs. You only need to do this once per domain:

```
Add-KdsRootKey -EffectiveImmediately
```

- * Wait for at least 10 hours for the KDS root key to replicate to all domain controllers in the domain.

- * Alternatively, you can use the -EffectiveTime parameter to specify a past date and time for the KDS root key, but this is not recommended for security reasons. For more information, see Add-KdsRootKey.

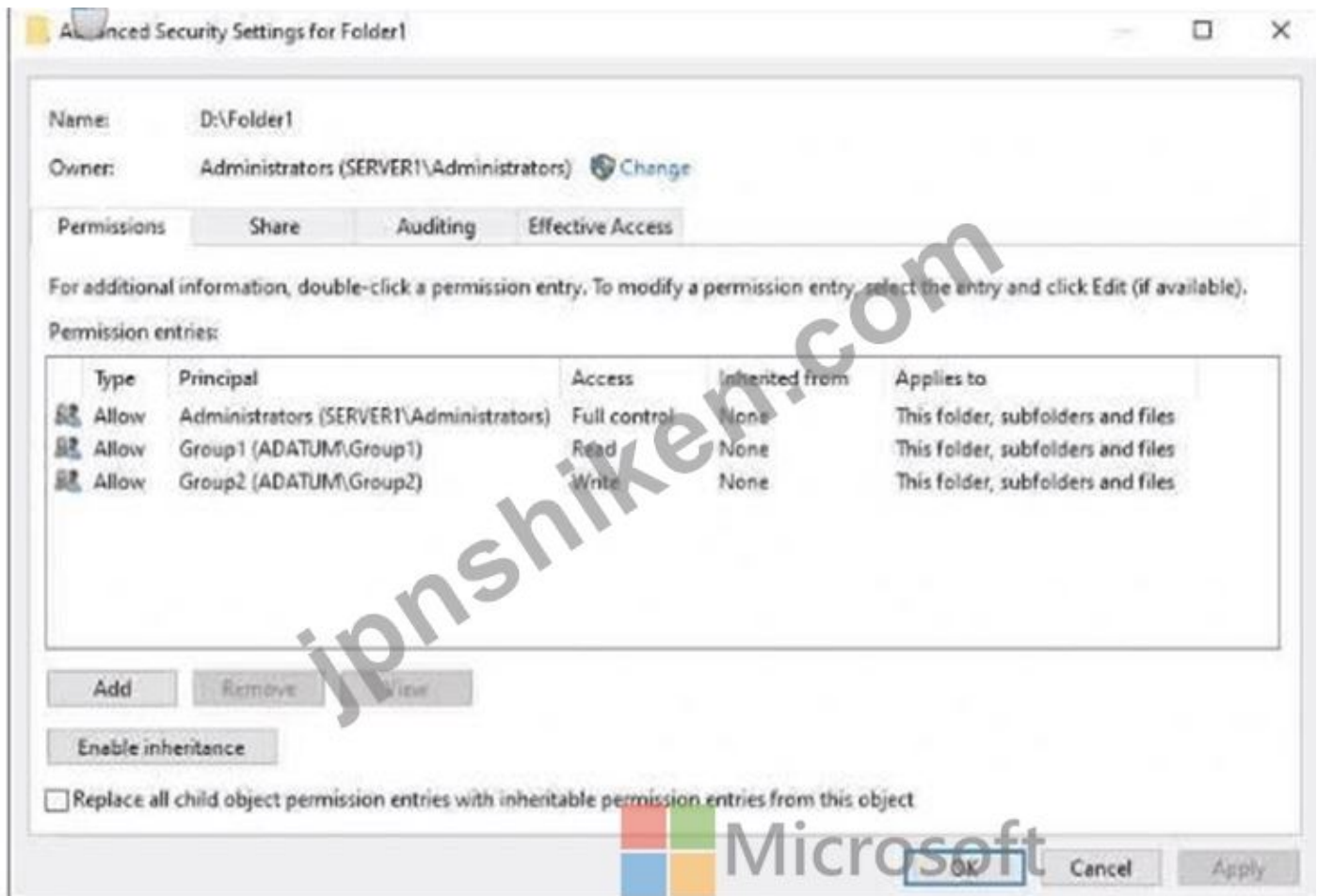
- * After the KDS root key is replicated, you can create and configure gMSAs using the New-ADServiceAccount and Set-ADServiceAccount cmdlets. For more information, see Create a gMSA and Configure a gMSA.

質問: 28

ネットワークには、adatum.com という名前の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。このドメインには、Server1 という名前のサーバーと、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Server1にはD:\Folder1というフォルダがあります。Folder1の詳細なセキュリティ設定は、「権限」の図に示されているとおりです。(「権限」ラボをクリックしてください。)



フォルダ1は次の設定で共有されます

Group	Permission
Group1	Allow - Change
Group3	Allow - Full Control

Path : D:\Folder1
 Name : Share1
 ShareType : FileSystemDirectory
 FolderEnumerationMode : Unrestricted



正解:



Explanation:

User1 can read the files in Share1. Yes

User3 can delete files in Share1. No

If User2 connects to \\Server1.adatum.com from File Explorer, (Share1 will be visible). Yes In Windows file sharing, effective access over SMB = the most restrictive result of Share permissions AND NTFS permissions. The AZ-800 materials emphasize that a user must have sufficient permission on both layers to perform an action. In Folder1, NTFS ACLs grant Group1 = Read, Group2 = Write, and no entry for Group3. The share "Share1" grants Group1 = Change and Group3 = Full Control.

* User1 (Group1): Share permission "Change" would allow modify over SMB, but NTFS grants only Read. Because the effective permission is the lower of the two, User1 is effectively Read and therefore can read the files.

* User3 (Group3): Although the share grants Full Control, there is no NTFS entry for Group3 (inheritance is disabled), so NTFS denies access. Without NTFS rights (e.g., Modify/Delete), delete is not possible.

* User2 (Group2): NTFS grants Write, but there is no share permission for Group2, so User2 cannot access content through the share. However, the share's FolderEnumerationMode = Unrestricted (i.e., Access-Based Enumeration is off). As covered in the hybrid core guide, when ABE is disabled, users can see items even if they lack permissions. Thus, when User2 browses \\Server1.adatum.com, Share1 is visible (opening it will result in Access Denied).

Therefore: Yes (User1 read), No (User3 delete), Yes (User2 sees Share1).

質問: 29

会社にはボストンとモントリオールにオフィスがあります。両オフィスは10MbpsのWANリンクで接続されていますが、このリンクはしばしば飽和状態になります。ボストンのオフィスには以下のものが含まれます。

* DC1 という名前の Active Directory ドメイン サービス (AD DS) ドメイン コントローラー。

* Windows Server を実行し、ファイル サーバー ロールがインストールされている Server1 という名前のサーバー。モントリオールのオフィスには、Windows 10 を実行するクライアント コンピューターが 20 台あります。モントリオールにはサーバーはありません。

同社は、すべてのクライアントコンピュータに新しい基幹業務(LOB)アプリケーションを導入する計画です。アプリケーションのインストールソースファイルは、\\Server\\Apps にあります。

Answer Area



On Server1:

Enable BranchCache in hosted cache mode.
Enable BranchCache in Distributed Cache mode.
Install the BranchCache for network files role service.

On the client computers:

Enable BranchCache in hosted cache mode.
Enable BranchCache in Distributed Cache mode.
Install the BranchCache for network files role service.

正解:

Answer Area

On Server1:  Microsoft

Enable BranchCache in hosted cache mode.
 Enable BranchCache in Distributed Cache mode.
 Install the BranchCache for network files role service.

On the client computers:

Enable BranchCache in hosted cache mode.
 Enable BranchCache in Distributed Cache mode.
 Install the BranchCache for network files role service.

Explanation:

Answer Area

On Server1: Install the BranchCache for network files role service.

On the client computers: Enable BranchCache in Distributed Cache mode.

 Microsoft

The Administering Windows Server Hybrid Core Infrastructure materials explain that BranchCache reduces WAN utilization by caching content that clients request from a remote content server. There are two modes: Hosted Cache and Distributed Cache. Hosted Cache "requires a server in the branch office configured as a hosted cache server," while Distributed Cache "uses a peer-to-peer cache among Windows clients and does not require any servers in the branch." For SMB shares, the content server (the file server at the main site) must have the "BranchCache for Network Files" role service installed so that it can advertise hashes and support BranchCache for file content. Client computers in the branch are then configured to Enable BranchCache in Distributed Cache mode so they can cache and retrieve content from each other, minimizing repeated downloads across the WAN.

In this scenario, Montreal has no servers, so Hosted Cache is not suitable. Installing BranchCache for Network Files on Server1 (the Boston file server hosting \\Server1\\Apps) and enabling Distributed Cache on the 20 Windows 10 clients in Montreal meets the requirement to reduce WAN saturation during the LOB app deployment and subsequent updates while requiring no additional branch infrastructure.

質問: 30

パスワードのセキュリティ要件を満たす必要があります。

Azure AD パスワード保護のコンポーネントはどこで構成すればよいですか？適切なコンポーネントを適切な場所にドラッグしてください。各コンポーネントは、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Locations	Answer Area
DC1 only All the domain controllers VM1 and VM2 The Azure AD tenant	Microsoft The Azure AD Password Protection DC agent: Location The Azure AD Password Protection proxy service: Location A custom banned password list: Location

正解:

Locations	Answer Area
DC1 only All the domain controllers VM1 and VM2 The Azure AD tenant	Microsoft The Azure AD Password Protection DC agent: All the domain controllers The Azure AD Password Protection proxy service: VM1 and VM2 A custom banned password list: The Azure AD tenant

Explanation:

Microsoft	
The Azure AD Password Protection DC agent:	All the domain controllers
The Azure AD Password Protection proxy service:	VM1 and VM2
A custom banned password list:	The Azure AD tenant

The Administering Windows Server Hybrid Core Infrastructure materials explain that Azure AD Password Protection for on-premises AD uses two components: the DC agent and the proxy service. The DC agent is installed on every domain controller because it "intercepts password set/change operations locally on the DC and evaluates them against the forbidden-password policy." The guidance further states that to ensure consistent enforcement "the DC agent should be deployed to all DCs in the forest, since password changes may occur on any DC." The proxy service is installed on member servers (not necessarily DCs) and "relays policy downloads and telemetry to Azure AD on behalf of DCs," which satisfies environments where "domain controllers must not directly contact Internet endpoints." Finally, configuration of the global and custom banned password lists is performed in Azure AD, where administrators "define tenant- wide custom banned terms; DCs obtain the policy via the proxy and cache it for local enforcement." Given Fabrikam's requirement to prevent DCs from accessing the Internet, the proxy must run on non-DC servers (VM1 and VM2). To guarantee enforcement wherever a password is changed, the DC agent must be on all domain controllers. The custom banned password list is configured in the Azure AD tenant and then distributed to on-premises DCs via the proxy.

質問: 31

Host1 という名前の Windows Server 2022 コンテナ ホストがあり、そこには Subsystem for Linux がインストールされており、次の表に示すコンテナ イメージがあります。

Name	Base image operating system
image1	Windows Server 2022
image2	Windows Server 2019
image3	Windows Server 2016
image4	Linux

イメージをHost1にデプロイする必要があります。ソリューションではコンテナの分離を最大限に高める必要があります。

プロセス分離を使用して実行できるイメージと、Hyper-V 分離を使用して実行できるイメージはどれですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Process isolation: image1, image2, and image3 only

image1 only

image1 and image2 only

image1, image2, and image3 only

image1, image2, image3, and image4

Hyper-V isolation: image1, image2, image3, and image4

image4 only

image3 and image4 only

image1, image2, and image3 only

image2, image3, and image4 only

image1, image2, image3, and image4

正解:

Answer Area

Process isolation: image1, image2, and image3 only

image1 only

image1 and image2 only

image1, image2, and image3 only

image1, image2, image3, and image4

Hyper-V isolation: image1, image2, image3, and image4

image4 only

image3 and image4 only

image1, image2, and image3 only

image2, image3, and image4 only

image1, image2, image3, and image4

Explanation:

Process isolation: image1 only

Hyper-V isolation: image1, image2, image3, and image4

The Administering Windows Server Hybrid Core Infrastructure materials explain two Windows container isolation modes. For process isolation, the guide states that Windows Server containers share the host's kernel and therefore require kernel/OS-version compatibility: "Process-isolated Windows containers run directly on the host and use the host's kernel; the container image must match the host OS version/build." Because Host1 is Windows Server 2022, only a Windows Server 2022 container image can be run with process isolation. Thus, among the images shown,

image1 (Windows Server 2022) is the only one eligible for process isolation; 2019 and 2016 images have kernel mismatches and cannot run in that mode.

The same materials describe Hyper-V isolation as running each container inside a lightweight utility VM: "Hyper-V-isolated containers get their own kernel inside a special VM, removing the kernel version dependency on the host." This mode "allows running different Windows versions than the host" and, when LCOW/WSL is present, it "enables running Linux containers on Windows" by supplying a Linux kernel within the utility VM. Since Host1 has the Subsystem for Linux installed, Hyper-V isolation can run Windows Server 2022, 2019, 2016 container images and also Linux containers. Therefore, to maximize isolation, you can run image1, image2, image3, and image4 with Hyper-V isolation, while process isolation is limited to image1 only.

有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/AZ-800J-mondaishu> **262問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 32

ネットワークには、contoso.com という名前の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

ネットワークには次の表に示すサーバーが含まれています。

Name	Role	Domain/workgroup	Operating system
DC1	Active Directory Domain Services, DNS Server	contoso.com	Windows Server
Server1	DHCP Server	contoso.com	Windows Server
Server2	None	contoso.com	Windows Server Core
Server3	None	Workgroup1	Windows Server Core

IP アドレス管理 (IPAM) を実装する予定です。

管理対象サーバーには、グループポリシーベースのプロビジョニング方法を使用する必要があります。ソリューションはサーバー検出をサポートする必要があります。

どうすればいいでしょうか？ 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Server on which to deploy the IPAM server role:

Server2
DC1
Server1
Server2
Server3

Servers that must be provisioned for IPAM:



Microsoft

DC1 and Server1
DC1 and Server1
DC1 and Server3
Server1 and Server2
Server2 and Server3

正解:

Answer Area



Explanation:

Answer Area

The Administering Windows Server Hybrid Core Infrastructure materials state the placement and provisioning requirements for IP Address Management (IPAM). Specifically:

- * "The IPAM server must be installed on a domain member computer. You cannot install the IPAM server feature on a domain controller."

- * "IPAM manages and discovers domain controllers, DHCP servers, and DNS servers in the domain.

Servers in a workgroup are not supported as managed servers."

- * "When you choose Group Policy-based provisioning, IPAM creates and links GPOs that configure the required settings on managed DC/DHCP/DNS servers so that IPAM can perform inventory, event collection, and address space management." Applying these rules:

- * Server2 is a domain-joined Windows Server Core member with no conflicting roles, satisfying the guidance to avoid installing IPAM on a DC and aligning with the recommendation to place IPAM on a dedicated member server. DC1 is a domain controller (and DNS), so it must not host IPAM. Server1 (DHCP) could host IPAM but best practice is to use a dedicated server. Server3 is in a workgroup, so it cannot host IPAM or be managed by it.

- * For GPO-based provisioning and server discovery, the managed servers that must be provisioned are the infrastructure role holders: DC1 (AD DS/DNS) and Server1 (DHCP). These are exactly the servers IPAM discovers and manages via the created GPOs.

質問: 33

タスク 10

グループポリシー設定を使用して、\\dd.contoso.com\instal1 を全ユーザーに対してドライブ H としてマッピングします。ユーザーが既に H にドライブマッピングを設定している場合は、新しいドライブマッピングが優先されます。

正解:

See the solution of this Task below.

Explanation:

To map \\dd.contoso.com\instal1 as drive H for all users using Group Policy Preferences and ensure that the new drive mapping takes precedence over any existing mappings, follow these steps:

Step 1: Open Group Policy Management Console Open the Group Policy Management Console (GPMC) on a machine that has administrative privileges over the domain.

Step 2: Create or Edit a GPO Create a new Group Policy Object (GPO) or edit an existing one that applies to the users who need the drive mapping.

Step 3: Navigate to Drive Mappings In the GPO Editor, navigate to:
User Configuration -> Preferences -> Windows Settings -> Drive Maps

Step 4: New Drive Mapping Right-click on Drive Maps and select New -> Mapped Drive.

Step 5: Configure Drive Mapping In the New Drive Properties window, configure the following settings:

Action: Select Replace. This action will overwrite any existing mappings with the same drive letter.

Location: Enter the UNC path \\dd.contoso.com\instal1.

Drive Letter: Choose H: from the drop-down menu.

Reconnect: Check this option if you want the drive mapping to persist across logon sessions.

Label As: Optionally, provide a label for the drive mapping.

Hide/Show this drive: Set according to your preference.

Hide/Show all drives: Set according to your preference.

Step 6: Common Tab Go to the Common tab and configure the following:

Run in logged-on user's security context (user policy option): Check this option.

Item-level targeting: Click on Targeting and set up any specific criteria if needed.

Step 7: Apply the GPO Click Apply and then OK to save the drive mapping configuration.

Step 8: Link the GPO Link the GPO to an Organizational Unit (OU) or domain that contains the users who should receive the drive mapping.

Step 9: Update Group Policy Instruct users to log off and log back on, or use the gpupdate /force command to refresh Group Policy on their computers.

質問: 34

Windows Server を実行し、C、D、E という 3 つのボリュームを含む Server1 というサーバーがあります。

次の表に示すように、ファイルは Server1 に保存されます。

Name	On volume	Size
File1	C	500 KB
File2	D	10 KB
File3	D	1 MB

ボリューム D では、データ重複除去が有効になっており、汎用ファイル サーバーに設定されています。

次のアクションを実行します。

* File1 をボリューム D に移動します。

* File2 をボリューム D にコピーし、コピーに File4 という名前を付けます。

* ファイル3をボリュームEに移動する

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。注：正しい選択肢は1つにつき1点です。

Statements	Yes	No
File1 is deduplicated after the deduplication job runs.	☐	☐
File3 is deduplicated after the deduplication job runs.	☐	☐
File4 is deduplicated after the deduplication job runs.	☐	☐

正解:

Statements	Yes	No
File1 is deduplicated after the deduplication job runs.	☒	☐
File3 is deduplicated after the deduplication job runs.	☐	☒
File4 is deduplicated after the deduplication job runs.	☐	☒

Explanation:

< File1 is deduplicated after the deduplication job runs. - YES

File3 is deduplicated after the deduplication job runs. - NO

File4 is deduplicated after the deduplication job runs. - NO

The Administering Windows Server Hybrid Core Infrastructure materials explain that Data Deduplication operates per-volume and only processes files on volumes where the role is enabled. The guide states that deduplication "is applied only to NTFS/ReFS volumes on which the Data Deduplication role is enabled," and that the General-purpose file server usage type applies default policies for typical data shares. It further specifies the file size limits: "Files smaller than 32 KB are not deduplicated; supported files are 32 KB up to multiple terabytes," and clarifies that optimization jobs process eligible files during scheduled runs.

Applying those rules:

* Volume D has Data Deduplication enabled (General-purpose). After moving File1 (500 KB) from C: to D:, it resides on a deduplicated volume and exceeds the minimum size threshold, so it will be deduplicated by the next optimization job.

* File3 (1 MB) is moved off the deduplicated volume (to E:), and dedup only affects enabled volumes; therefore it will not be deduplicated.

* File4 is a copy of File2 (10 KB) on D:. Because the file is smaller than the 32-KB minimum, it is not deduplicated even though it is on a deduplicated volume.

Thus the correct outcomes are YES for File1, NO for File3, and NO for File4.

質問: 35

Webapp1 のセキュリティ要件を満たすには、どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

Actions

Create a standalone managed service account (sMSA) in AD DS.

Configure the IIS application pool to run as Network Service.

Configure the IIS application pool to run as a specified user account.

Create a group managed service account (gMSA) in Active Directory.

Create a system-assigned managed identity in Azure AD.

Create a user-assigned managed identity in Azure AD.

Create the Key Distribution Services (KDS) root key in AD DS.

Answer Area



正解:

Actions	Answer Area
Create a standalone managed service account (sMSA) in AD DS.	Configure the IIS application pool to run as Network Service.
Configure the IIS application pool to run as Network Service.	
Configure the IIS application pool to run as a specified user account.	Create a group managed service account (gMSA) in Active Directory.
Create a group managed service account (gMSA) in Active Directory.	
Create a system-assigned managed identity in Azure AD.	Create the Key Distribution Services (KDS) root key in AD DS.
Create a user-assigned managed identity in Azure AD.	
Create the Key Distribution Services (KDS) root key in AD DS.	



Explanation:

Configure the IIS application pool to run as Network Service.

Create a group managed service account (gMSA) in Active Directory.



Create the Key Distribution Services (KDS) root key in AD DS.

In the Administering Windows Server Hybrid Core Infrastructure materials (AZ-800), Microsoft explains that Group Managed Service Accounts (gMSAs) are designed for services running on multiple servers and

"provide automatic password management, simplified SPN management, and the ability to delegate the management to other administrators." The guidance further states that before you can create any gMSA, "the domain must have a KDS root key so that the Key Distribution Service can generate and rotate strong, unique passwords for gMSAs on a schedule." After the KDS root key is created, "use New-ADServiceAccount to create the gMSA and grant the computers (e.g., web servers) permission to retrieve the account password." For IIS, the course notes specify that a gMSA can be used for app pools:

"Configure the IIS application pool identity to a custom account and specify the gMSA name (ending with '\$') without a password; the password is managed automatically by AD and rotates by policy (for example, every 30 days)." Mapping these requirements to the scenario: Webapp1 runs on WEB1 and WEB2 and must use the same service account with an automatic 30-day password change. Therefore, the correct sequence is: create the KDS root key, create the gMSA, and then set the IIS application pool to run under that account. This fulfills the security requirement while allowing both web servers to share the same, automatically-rotated credentials.

質問: 36

Windows Server を実行し、Hyper-V サーバー ロールがインストールされている Served という名前のサーバーがあります。

Just Enough Administration (JEA) ロール機能とセッション構成ファイルを構築します。

Server1 をリモートで管理するときに、ヘルプデスク ユーザーが使用できる Hyper-V モジュール コマンドレットを制限する必要があります。

PowerShell コマンドをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Answer Area

Register-PSSessionConfiguration -Path .\HyperVJeaConfig.pssc -Name 'HyperVJeaHelpDesk' -Force

Infrastructure documents: =

In Just Enough Administration (JEA), you restrict what remote users can do by creating two artifacts: role capability files (*.psrc) and a session configuration file (*.pssc). The role capability file defines which commands are visible/usable (for example, specific Hyper-V cmdlets via VisibleCmdlets, VisibleFunctions, or VisibleExternalCommands). The session configuration file then maps users or groups to one or more role capabilities using RoleDefinitions.

The Administering Windows Server Hybrid Core Infrastructure material explains that once those files are authored, you must expose a JEA endpoint by registering the session configuration on the target server.

This is accomplished with Register-PSSessionConfiguration, pointing to the PS session configuration file (.pssc).

Registering the endpoint enforces the role capability restrictions when helpdesk users connect (for example, Enter-PSSession -ConfigurationName HyperVJeaHelpDesk -ComputerName Server1).

New-PSSessionConfigurationFile is used earlier to create the .pssc file, but the prompt states the files are already built. Enter-PSSession only starts a session and does not publish the configuration. Therefore, the correct command to limit which Hyper-V module cmdlets helpdesk users can use is:

Register-PSSessionConfiguration -Path .\HyperVJeaConfig.pssc -Name 'HyperVJeaHelpDesk' -Force.

質問: 37

タスク6

VM1 onSRV1 という名前の仮想マシンに対してネストされた視覚化を有効にする必要があります。

正解:

See the solution of this Task below.

Explanation:

TASK 6

Objective:

Enable nested virtualization for a VM (VM1) on SRV1.

Step-by-Step Guide: Enable Nested Virtualization

Step 1: Verify Requirements

Nested virtualization requires:

SRV1 to have a processor that supports Intel VT-x or AMD-V.

Hyper-V role installed on SRV1.

VM1 must be turned off.

Step 2: Open PowerShell on SRV1

Log in to SRV1 with an account that has administrative privileges.

Open PowerShell as Administrator.

Step 3: Enable Nested Virtualization

Run the following command:

```
Set-VMProcessor -VMName "VM1" -ExposeVirtualizationExtensions $true
```

Step 4: Verify Nested Virtualization

To confirm the change, run:

```
Get-VMProcessor -VMName "VM1" | Format-List ExposeVirtualizationExtensions
```

The output should show:

```
ExposeVirtualizationExtensions : True
```

Step 5: Configure Network Adapter (Optional for Nested VMs)

Nested virtualization requires MAC address spoofing for the VM network adapter.

Run:

```
Set-VMNetworkAdapter -VMName "VM1" -MacAddressSpoofing On
```

Step 6: Start the VM

Use PowerShell:

```
Start-VM -Name "VM1"
```

Or start the VM in Hyper-V Manager.

Additional Notes

Nested virtualization allows you to run Hyper-V within a VM.

Useful for lab/test environments (e.g., running nested Hyper-V hosts in a VM).

質問: 38

ネットワークにはActive Directoryドメインサービス(AD DS)ドメインが含まれています。このドメインにはServer1という名前のサーバーが含まれています。

サーバー 1 に Windows Admin Center をインストールし、Windows Admin Center を使用して、許可されたグループから BUILTIN\Users を削除します。

すべてのユーザーが引き続き Windows Admin Center にサインインできることがわかります。

権限のないユーザーが Windows Admin Center にサインインできないようにする必要があります。

Windows Admin Center では何をすればよいですか？

- A. パフォーマンスプロファイルをオンに設定する
- B. 管理者セッションの再認証を要求するをオンに設定
- C. プロキシ設定からバイパス リストを構成します。
- D. 許可されたグループにセキュリティ グループを追加します。

正解: ([正解を表示します](#))

In Windows Admin Center (WAC), "gateway access" is controlled by the Allowed groups list on the gateway. The AZ-800 materials explain that membership in the local Administrators group on the WAC gateway still permits sign-in unless you explicitly scope access to specific groups in the Allowed groups list.

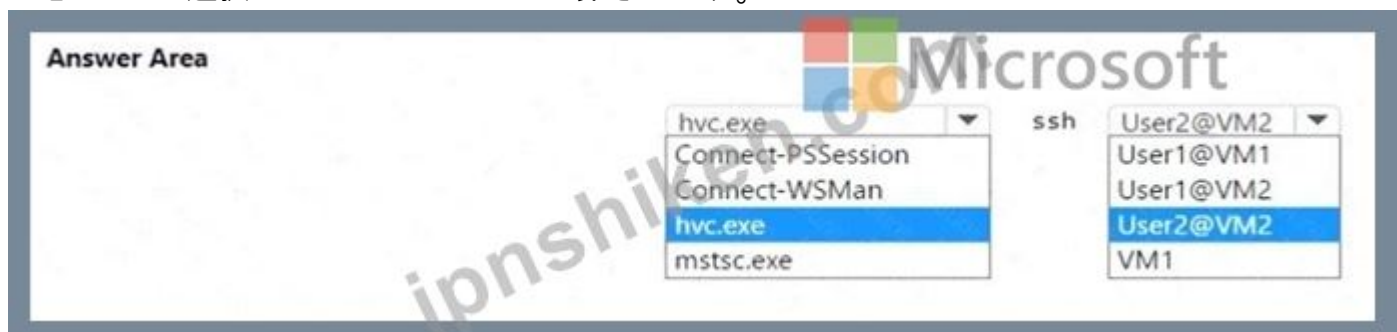
The guidance further states that to restrict who can sign in to the WAC gateway, you must populate Allowed groups with one or more security groups (for example, a domain group) and remove broad principals (like BUILTIN\Users). Until you add at least one explicit group, existing administrators can continue to authenticate, which is why "everyone" appears able to sign in after only removing BUILTIN\Users. By adding a dedicated security group to Allowed groups, only members of that group can authenticate to the gateway UI; non-members are denied. Settings such as Performance profile or Require manage-as sessions to re-authenticate affect performance and remote management prompts, not gateway sign-in. Proxy bypass lists control outbound connectivity, not access control. Therefore, to prevent unauthorized sign-ins, configure Allowed groups with a specific security group and manage membership there.

質問: 39

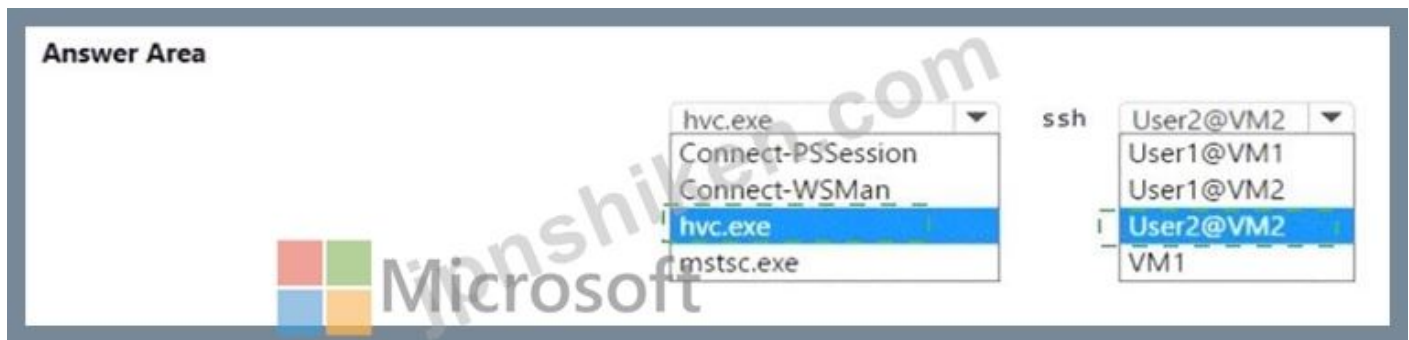
HyperV1 の技術要件を満たす必要があります。

どのコマンドを実行する必要がありますか？ 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:



質問: 40

Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory Domain Services (AD DS) ドメインがあります。ドメインには、Server1 と Server2 という名前の 2 つのサーバーが含まれています。

Admin1 という名前のユーザーは、Server1 と Server2 のローカルの Administrators グループのメンバーです。

Azure Arc を使用して Server1 と Server2 を管理する予定です。Azure Arc オブジェクトは、RG1 という名前のリソース グループに追加されます。

Admin1 が Azure Arc を使用して Server1 と Server2 を管理するように構成できることを確認する必要があります。

最初に何をすべきですか？

- A. Azure portal から、新しいオンボーディング スクリプトを生成します。
- B. Admin1 に RG1 の Azure Connected Machine Onboarding ロールを割り当てます。
- C. ハイブリッド Azure AD は、Server1 と Server2 に参加します。
- D. Admin1 の Azure クラウド専用アカウントを作成します。

正解: ([正解を表示します](#))

Reference:

In the Administering Windows Server Hybrid Core Infrastructure content for Azure Arc-enabled servers, the onboarding script (interactive or service-principal based) requires that the identity used to connect a machine has the least-privilege built-in role at the intended scope. The guide states that for scripted or portal onboarding you should "grant the Azure RBAC role Azure Connected Machine Onboarding at the subscription or resource-group scope to the identity that will run the connect process; this role includes only the permissions necessary to register and connect the server resource." It also notes that no hybrid Azure AD join is required just to onboard Arc, and that local admin on the target server is sufficient for installing the Connected Machine agent. Therefore, before Admin1 runs the onboarding script for Server1 and Server2 into RG1, you must first assign Admin1 the Azure Connected Machine Onboarding role at RG1.

This satisfies least privilege and enables the script to create the Microsoft.HybridCompute/machines resource entries and related artifacts while avoiding broader roles like Contributor or Owner.

質問: 41

Server4 の技術要件を満たす必要があります。

Server1 と Server4 で実行する必要があるコマンドレットはどれですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Server1:	
	Enable-PSRemoting
	Enable-ServerManagerStandardUserRemoting
	Set-Item
	Start-Service

Server4:	
	Enable-PSRemoting
	Enable-ServerManagerStandardUserRemoting
	Set-Item
	Start-Service

正解:

Server1:	
	Enable-PSRemoting
	Enable-ServerManagerStandardUserRemoting
	Set-Item
	Start-Service

Server4:	
	Enable-PSRemoting
	Enable-ServerManagerStandardUserRemoting
	Set-Item
	Start-Service

Explanation:

Server1 - Set-Item

Server4 - Enable-PSRemoting

質問: 42

オンプレミス ネットワークには、Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

Microsoft Entra Connect クラウド同期を使用して、ドメインを Microsoft Entra テナントと同期する予定です。

次の要件を満たす必要があります。

* ドメインと Microsoft Entra ID を同期するために必要なソフトウェアをインストールします。

* パスワード ハッシュの同期を有効にします。

パスワード ハッシュ同期を有効にするには、何をインストールし、何を使用すればよいですか？

回答するには、回答領域で適切なオプションを選択してください。

Answer Area

Install: Microsoft Entra Connect
Active Directory Administrative Center
Microsoft Entra Connect
The AD FS Management console
The Microsoft Entra Connect provisioning agent

Use: The Azure portal
Active Directory Administrative Center
Microsoft Entra Connect
The AD FS Management console
The Azure portal

正解:

Answer Area

Install: Microsoft Entra Connect
Active Directory Administrative Center
Microsoft Entra Connect
The AD FS Management console
The Microsoft Entra Connect provisioning agent

Use: The Azure portal
Active Directory Administrative Center
Microsoft Entra Connect
The AD FS Management console
The Azure portal

Explanation:



Install: Microsoft Entra Connect
Active Directory Administrative Center
The AD FS Management console
The Microsoft Entra Connect provisioning agent

Use: The Azure portal
Active Directory Administrative Center
Microsoft Entra Connect
The AD FS Management console
The Azure portal

In a cloud-sync deployment, Microsoft's hybrid identity guidance for Administering Windows Server Hybrid Core Infrastructure specifies that you do not install the full Microsoft Entra (Azure AD) Connect server.

Instead, cloud sync "uses a lightweight agent-called the Microsoft Entra Connect provisioning agent- installed on one or more Windows Server computers that can reach your AD DS domain controllers." The agent handles directory read operations and securely communicates with the cloud provisioning service.

The study material further states that all configuration-including creating sync configurations, scoping filters, and enabling features such as Password Hash Synchronization (PHS)-is performed in the Microsoft Entra admin experience: "Cloud sync is configured in the Azure portal; you create a cloud sync configuration, select the on-premises AD forest, and enable password hash synchronization so password hashes are synchronized to Microsoft Entra ID." Because you are using Microsoft Entra Connect cloud sync, the correct software to install on-premises is the Microsoft Entra Connect provisioning agent (not the full Microsoft Entra Connect server or ADFS tools). And to enable PHS for cloud sync, you use the Azure portal (Microsoft Entra admin center) to turn on Password hash synchronization within the cloud sync configuration. This meets both requirements:

installing the proper agent for cloud sync and enabling PHS centrally in the portal.

質問: 43

ネットワークには Active Domain Services (AD DS) フォレストが含まれています。フォレストには 3 つのドメインが含まれています。各ドメインには 10 個のドメイン コントローラーが含まれます。

カスタム Active Directory パーティションに DNS ゾーンを格納する予定です。

ゾーンの Active Directory パーティションを作成する必要があります。パーティションは、4 つのドメイン コントローラーのみにレプリケートされます。

何を使うべきですか？

- A. Active Directory サイトとサービス
- B. Active Directory 管理者センター
- C. dnscmd.exe
- D. DNS マネージャー

正解: ([正解を表示します](#))

In the Windows Server hybrid administration guidance for DNS, Microsoft describes that DNS zones stored in Active Directory can use application directory partitions to customize replication scope beyond the default domain- or forest-wide options. The study materials state that "custom application directory partitions allow DNS data to replicate only to the DNS servers that are explicitly enlisted in that partition." They further emphasize that while DNS Manager lets you pick among built-in scopes or select an existing application partition, "creating a new application directory partition is performed with command-line tools (dnscmd) or Windows PowerShell." The documented procedure is: "Use dnscmd /CreateDirectoryPartition <FQDN-of-partition> to create the custom partition, then dnscmd /EnlistDirectoryPartition on each DNS server that should host and replicate the data." Because you must have the partition replicate to only four of the domain controllers, you first create the partition, and then enlist only those four DNS servers. Tools such

as Active Directory Sites and Services or Active Directory Administrative Center do not create DNS application directory partitions, and DNS Manager cannot create a new custom partition; it can only use an existing one. Therefore, the correct tool to meet the requirement is dnscmd.exe, after which you enlist just the selected four DNS servers into that partition.

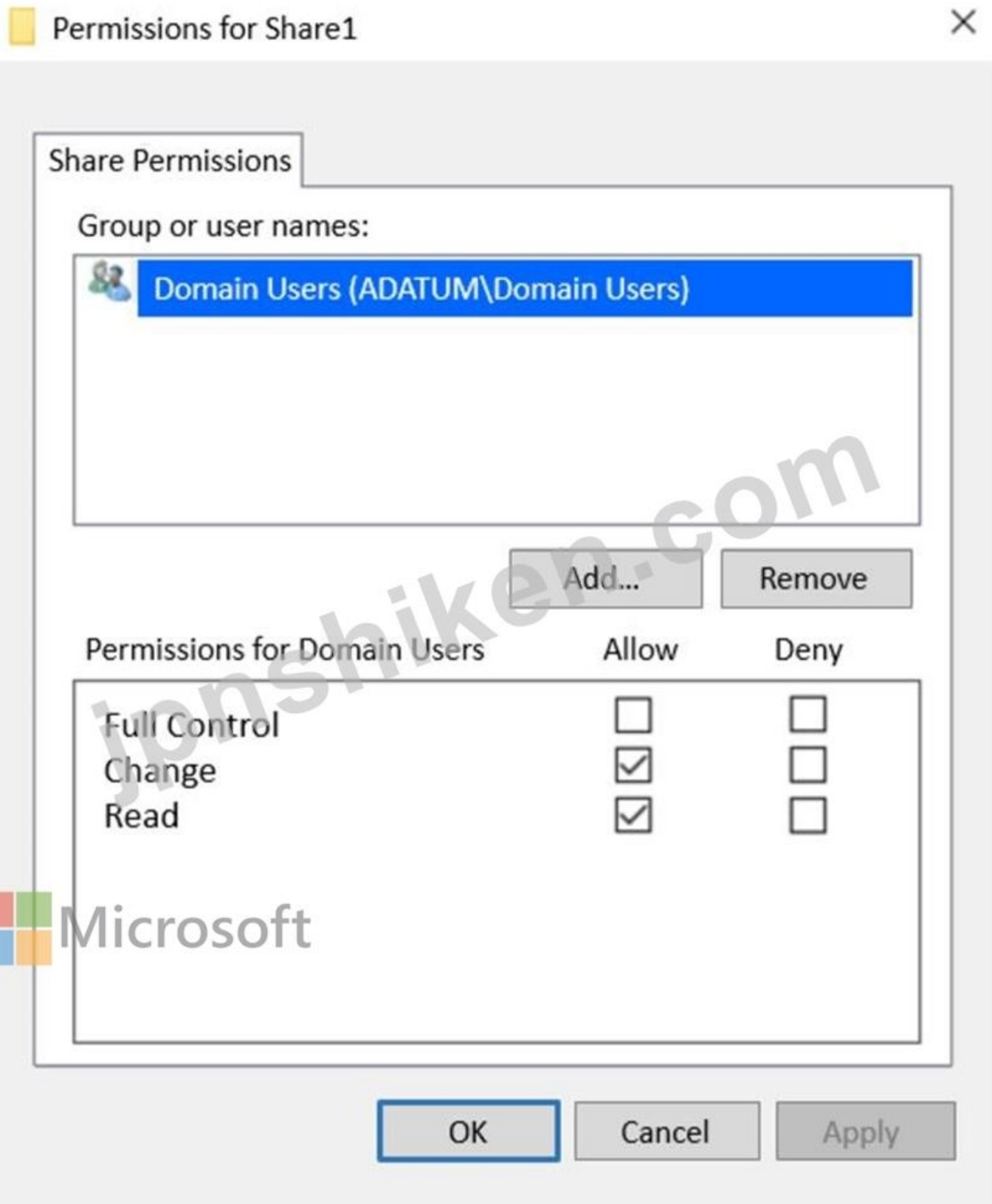
質問: 44

ネットワークには、adatum.com という Active Directory ドメイン サービス (AD DS) ドメインが含まれています。このドメインには、Server1 というファイル サーバーと、User1、User2、User3 という 3 人のユーザーが含まれています。

Server1 には、次の構成を持つ Share1 という名前の共有フォルダーが含まれています。

ShareState	:	Online
AvailabilityType	:	NonClustered
FolderEnumerationMode	:	AccessBased
CachingMode	:	Manual
LeasingMode	:	Full
SmbInstance	:	Default
CompressData	:	False
ContinuouslyAvailable	:	False
EncryptData	:	False
Name	:	Share1
Path	:	E:\Share1
ShadowCopy	:	False

Share1 の共有アクセス許可は、「共有アクセス許可」の図に示すように構成されています。



Share1にはFile1.bxtというファイルが含まれています。File1.txtの共有設定は、ファイル権限の図に示されているとおりです。

Advanced Security Settings for File1.txt

Name: E:\Share1\File1.txt

Owner: Administrators (SERVER1\Administrators) [Change](#)

Permissions Share Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	Domain Admins (ADATUM\Domain Admins)	Full control	None
Allow	User1 (User1@Adatum.com)	Full control	None
Allow	User2 (User2@Adatum.com)	Read	None
Allow	User3 (User3@Adatum.com)	Write	None

Add Remove View

Enable inheritance

OK Cancel Apply

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Statements

	Yes	No
When User1 connects to \\Server1.adatum.com\Share1\, the user can take ownership of File1.txt.	☐	☐
When User2 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☐	☐
When User3 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☐	☐

正解:

Statements

	Yes	No
When User1 connects to \\Server1.adatum.com\Share1\, the user can take ownership of File1.txt.	☒	☐
When User2 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☒	☐
When User3 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☐	☒

Explanation:

When User1 connects to \https://www.google.com/search?q=Server1.adatum.com\Share1, the user can take ownership of File1.txt.: Yes When User2 connects to \https://www.google.com/search?q=Server1.adatum.com\Share1, File1.txt is visible.: Yes When User3 connects to \https://www.google.com/search?q=Server1.adatum.com\Share1, File1.txt is visible.: No In Windows Server Hybrid environments, access to files over a network is governed by the intersection of Share Permissions, NTFS (File) Permissions, and Access-Based Enumeration (ABE).

* Ownership Rights: User1 has Full Control in the NTFS permissions for File1.txt. In Windows security, the Full Control right inherently includes the "Take Ownership" and "Change Permissions" rights. While the Share permission for "Domain Users" is set to Change, which normally restricts permission changes over the wire, a user with NTFS Full Control can still perform ownership operations if they have sufficient effective rights. Therefore, User1 can take ownership.

* File Visibility and ABE: The exhibit for Share1 shows that FolderEnumerationMode is set to AccessBased. Access-Based Enumeration (ABE) ensures that users only see the files and folders for which they have at least Read (or equivalent) NTFS permissions.

* User2: The NTFS permissions grant User2 Read access to File1.txt. Since User2 has read access, ABE will allow the file to be visible when the user browses the share.

* User3: The NTFS permissions grant User3 Write access but not Read access. ABE specifically requires the "Read" permission for a file to be visible in a directory listing. Because User3 lacks the Read permission, File1.txt will be hidden from their view, even though they have Write rights to the underlying file.

質問: 45

タスク 8

DC1にfabrikam.comという新しいプライマリDNSゾーンを展開する必要があります。このゾーンは署名されている必要があります。

正解:

See the solution of this Task below.

Explanation:

To deploy a new primary DNS zone named fabrikam.com to DC1 and sign the zone, you can follow these steps:

Step 1: Create the Primary DNS Zone Use the Add-DnsServerPrimaryZone PowerShell command to create the primary zone:

```
Add-DnsServerPrimaryZone -Name "fabrikam.com" -ZoneFile "fabrikam.com.dns" -
```

DynamicUpdate Secure This command creates a primary zone for fabrikam.com with a DNS file named fabrikam.com.dns and allows secure dynamic updates.

Step 2: Sign the Zone To sign the zone, you can use the DNS Manager or Windows PowerShell. Here's how to sign the zone using PowerShell:

```
Add-DnsServerSigningKey -ZoneName "fabrikam.com" -Type KeySigningKey -CryptoAlgorithm RsaSha256 Set-DnsServerDnsSecZoneSetting -ZoneName "fabrikam.com" -DenialOfExistence
```

NSEC3 - NSEC3Parameters 1,0,10,"" These commands add a signing key to the zone and set DNSSEC settings with NSEC3 parameters.

Step 3: Publish the Signed Zone After signing the zone, ensure that it is published and available for DNS queries. You can verify the zone signing status using the following command:

Get-DnsServerZone -Name "fabrikam.com"

Note: Ensure that you have the appropriate permissions to perform these actions on DC1 and that the DNS Server role is installed and properly configured. Also, replace "fabrikam.com.dns" with the actual path to your DNS file if it's different¹².

By following these steps, you should be able to deploy and sign the new primary DNS zone fabrikam.com on DC1.

質問: 46

Azure File Sync を使用して、Server1 という名前のオンプレミス サーバーから Azure にファイルを同期する必要があります。

30 パーセントの空き領域と 70 日間に構成されたクラウド階層化ポリシーがあります。

Server1 のボリューム E は 500 GB です。

1年前、Azure File Syncを使用してServer1上のE:\Dataを同期するように構成しました。E:\Dataで表示されるファイルは、次の表のとおりです。

Name	Size	Last accessed
File1	200 GB	2 days ago
File2	100 GB	10 days ago
File3	200 GB	60 days ago
File4	50 GB	100 days ago

ボリューム E には他のファイルは含まれていません。

File1 と File3 はどこにありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

File1:	Microsoft
	Server1 only
	The Azure file share only
	Server1 and the Azure file share

File3:	
	Server1 only
	The Azure file share only
	Server1 and the Azure file share

正解:

File1:	Microsoft
	Server1 only
	The Azure file share only
	Server1 and the Azure file share

File3:	
	Server1 only
	The Azure file share only
	Server1 and the Azure file share

Explanation:

File1: Server1 and the Azure file share

File3: The Azure file share only

Azure File Sync cloud tiering manages local storage by balancing two specific policies: the Volume Free Space Policy and the Date Policy. According to the official documentation for Administering Windows Server Hybrid Core Infrastructure, the Volume Free Space policy is the primary governing factor for tiering decisions.

* Storage Calculations: Volume E is 500 GB. With a 30 percent free space requirement, the server must maintain 150 GB of free space ($500 \times 0.30 = 150$). This means only 350 GB ($500 - 150$) of file content can be cached locally on Server1.

* Date Policy Application: The date policy is set to 70 days. Any file not accessed within this window is automatically tiered regardless of free space.

* File4 (Last accessed 100 days ago) is older than 70 days, so it is tiered to The Azure file share only.

- * Volume Free Space Application: The remaining files (File1, File2, and File3) were all accessed within the last 70 days. Their total size is 500 GB (\$200 + 100 + 200 = 500\$). Since the maximum allowed local storage is 350 GB, Azure File Sync must tier additional files to satisfy the 30% free space requirement.
- * Tiering Priority: Files are tiered based on their "coldness" (last access time). File3 (60 days ago) is significantly older than File1 (2 days) and File2 (10 days). By tiering File3, the remaining local data (File1 + File2) totals 300 GB, which fits within the 350 GB limit.
- * Conclusion: Consequently, File1 remains cached on Server1 and the Azure file share, while File3 is tiered to The Azure file share only.

有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/AZ-800J-mondaishu> **262**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 47

次の表に示すように、Windows Server を実行するオンプレミスのファイル サーバーがあります。

Name	Relevant folder
Server1	D:\Folder1, E:\Folder2
Server2	D:\Data

次の表に示す Azure ファイル共有があります。

Name	Location
share1	East US
share2	East US

Sync1 という名前のストレージ同期サービスと、Group1 という名前の Azure File Sync 同期グループを追加します。Group1 は、クラウド エンドポイントとして share1 を使用します。Server1とServer2をSync1に登録します。Server1のD:\Folder1をGroup1のサーバーエンドポイントとして追加します。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Statements	Yes	No
You can add share2 as a cloud endpoint in Group1.	☐	☐
You can add E:\Folder2 from Server1 as a server endpoint in Group1.	☐	☐
You can add D:\Data from Server2 as a server endpoint in Group1.	☐	☐

正解:

Statements	Yes	No
You can add share2 as a cloud endpoint in Group1.	☐	☒
You can add E:\Folder2 from Server1 as a server endpoint in Group1.	☒	☐
You can add D:\Data from Server2 as a server endpoint in Group1.	☒	☐

Explanation:

Statements	Yes	No
You can add share2 as a cloud endpoint in Group1.	☐	☒
You can add E:\Folder2 from Server1 as a server endpoint in Group1.	☒	☐
You can add D:\Data from Server2 as a server endpoint in Group1.	☒	☐

The Azure File Sync design guidance in Administering Windows Server Hybrid Core Infrastructure explains that a sync group defines one sync topology and is anchored by exactly one cloud endpoint (an Azure file share). The material states: "Each sync group contains a single cloud endpoint... Additional Azure file shares must be placed in separate sync groups." Consequently, after Group1 uses share1 as its cloud endpoint, share2 cannot be added to the same sync group, which makes the first statement No.

For server endpoints, the guide notes: "A server endpoint represents a specific path on a registered Windows Server... A server can host multiple server endpoints, including in the same sync group, provided paths don't overlap (no parent/child or identical paths)." Because D:\Folder1 is already in Group1, adding E:\Folder2 from the same Server1 is supported and non-overlapping, so the second statement is Yes.

Finally, multi-server synchronization is a core capability: "Multiple servers can be added as server endpoints to the same sync group to enable branch-to-branch and server-to-cloud sync; contents are merged in the Azure file share namespace." Therefore, adding D:\Data from Server2 as another server endpoint in Group1 is fully supported, making the third statement Yes.

These rules satisfy the scenario: one cloud endpoint per sync group, multiple non-overlapping server endpoints (including multiple from the same server), and multi-server participation in the same group.

質問: 48

オンプレミスの Active Directory Domain Services (AD DS) ドメインが Azure Active Directory (Azure AD) テナントと同期しており、オンプレミス ネットワークはサイト間 VPN を使用して Azure に接続されています。DNS ゾーンは、次の表のとおりです。

Name	Location	Description
contoso.com	A domain controller named DC1 on the on-premises network	Provides name resolution on-premises
fabrikam.com	An Azure private DNS zone	Provides name resolution for all Azure virtual networks

fabrikam.com の名前がオンプレミスネットワークから解決できることを確認する必要があります。どの 2 つのアクションを実行する必要がありますか？ 正解はソリューションの一部を示します。注: 正解は 1 点です。

- A. DC1 上の fabrikam.com に対して条件付きフォワーダーを作成します。
- B. DC1 に fabrikam.com のスタブ ゾーンを作成します。
- C. DO に fabrikam.com のセカンダリ ゾーンを作成します。
- D. Windows Server を実行する Azure 仮想マシンをデプロイします。仮想ネットワークの DNS サーバー設定を変更します。
- E. Windows Server を実行する Azure 仮想マシンをデプロイします。仮想マシンに DNS フォワーダーを構成します。

正解: **A,E** ([コメントを发表する](#))

In hybrid name-resolution designs covered in Administering Windows Server Hybrid Core Infrastructure, Azure Private DNS does not support zone transfers and therefore you cannot host it on, or pull it into, on-premises DNS by using stub or secondary zones. The guidance states that when on-premises clients must resolve names that live in an Azure Private DNS zone, the recommended pattern is to place a DNS forwarder in Azure (typically a Windows Server VM running the DNS role) that can directly query the Azure resolver from inside the virtual network. Then, on-premises Windows DNS servers are configured with a conditional forwarder that forwards queries for the private zone's suffix to the Azure DNS forwarder over the VPN/ExpressRoute connection.

This achieves the following:

- * Keeps the authoritative zone in Azure Private DNS while making it reachable from on-premises.
- * Avoids unsupported mechanisms (no AXFR/IXFR available from Azure Private DNS, so stub and secondary zones won't work).
- * Uses least privilege and minimal change on both sides: add a DNS VM in Azure (E) and create a conditional forwarder on DC1 for fabrikam.com pointing to that VM's private IP (A).

Options B and C require zone transfers, which are not available from Azure Private DNS, and D (changing VNet DNS servers) affects Azure VMs' resolver settings but does not enable on-premises resolution of the Azure-hosted private zone.

質問: 49

オンプレミス ネットワークには、単一ドメインの Active Directory Domain Services (AD DS) フォレストが含まれています。contoso.com という Azure AD テナントがあり、AD DS フォレストは Azure AD Connect を使用して Azure AD テナントと同期しています。フォレスト内の NoSync カスタム属性を持つユーザーが同期から除外されるようにする必要があります。

Azure AD Connect の cloudFiltered 属性はどのように構成すればよいですか。また、どのツールを使用する必要がありますか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Attribute:

Tool:

ipnshiken.com Microsoft

正解:

Answer Area

Attribute:

Tool:

ipnshiken.com Microsoft

Explanation:

Answer Area

Attribute:

Tool:

ipnshiken.com Microsoft

In Azure AD Connect-based hybrid identity, object filtering can be enforced with the built-in cloudFiltered metaverse flag. The Administering Windows Server Hybrid Core Infrastructure materials explain that

"cloudFiltered is a Boolean in the metaverse that determines whether an object is eligible for export to Azure AD; when set to True, the connector space object is excluded from synchronization to Azure AD." The recommended approach for attribute-based filtering is to create a custom inbound synchronization rule that scopes the users you want to exclude and flows a constant value of True into cloudFiltered. The guide states: "Use the Synchronization Rules Editor to define an inbound rule from Active Directory to the metaverse. Add a scoping filter (for example, a custom attribute equals 'NoSync') and configure an attribute flow mapping cloudFiltered # Constant(True). Objects matching the scope will not be exported." Because you need to exclude any user whose custom attribute equals NoSync, you create an inbound rule targeting user objects, add the scoping filter on that custom attribute, and then set cloudFiltered = True (constant). This is done with the Synchronization Rules Editor, not ADSI Edit or the Azure AD Connect wizard, since the wizard doesn't author custom attribute flows and ADSI Edit doesn't manage sync rules.

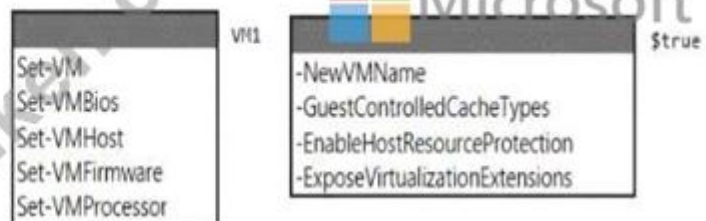
質問: 50

VM1 の技術要件を満たす必要があります。

最初にどのコマンドレットを実行する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

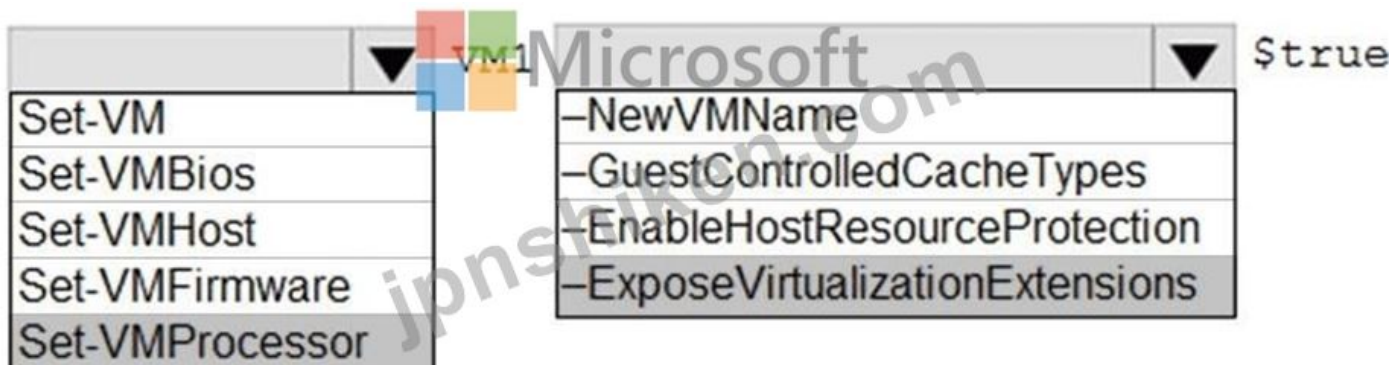
Answer Area



正解:



Explanation:



In the Administering Windows Server Hybrid Core Infrastructure objectives for managing Hyper-V, enabling nested virtualization is the required step when you must "run virtual machines inside a virtual machine." The referenced guidance states that Hyper-V on a VM is supported only when the host exposes hardware virtualization features to the guest. The prescriptive step is: "Turn off the VM and run Set-VMProcessor - VMName <VMName> -ExposeVirtualizationExtensions \$true to enable nested virtualization." The module further notes that this action "passes through Intel VT-x/AMD-V to the guest so the guest OS can install the Hyper-V role and create VMs." It also clarifies that "the setting is applied on the parent host for the target VM and requires the VM to be powered off before the change is committed." Because the technical requirement says "Ensure that you can run virtual machines on VM1", VM1 must be able to host Hyper-V while itself running as a VM on Server2. The first and essential cmdlet is therefore Set- VMProcessor with the - ExposeVirtualizationExtensions switch set to \$true against VM1. Other optional settings (for example, MAC spoofing on the vNIC or static memory) may be configured later if needed, but exposing virtualization extensions is the enabling prerequisite that satisfies the requirement.

質問: 51

Windows Server を実行し、DHCP サーバーの役割がインストールされたサーバーがあります。このサーバーには、Scope! というスコープがあり、以下の構成になっています。

* アドレス範囲: 192.168.0.2 ~ 192.168.1.2M 。マスク 255.255.254.0

* ルーター: 192.168.0.1

* リース期間: 3日間

* DNSサーバー 172.16.0.254

同じベンダーのMicrosoft Teams Phoneデバイスが50台あります。すべてのデバイスのMACアドレスは同じ範囲内にあります。

スコープ1からリースを受け取るすべてのTeams Phoneデバイスが、192.168.1.100から192.168.1.200の範囲のIPアドレスを持つようにする必要があります。このソリューションは、スコープ1からIP構成を受け取る他のDHCPクライアントに影響を与えてはなりません。

何を創造すべきでしょうか？

- A. ポリシー
- B. スコープ
- C. フィッター
- D. スコープオプション

正解: [\(正解を表示します\)](#)

Reference:

In Windows Server DHCP, policies let you "assign different options or even different IP address ranges to clients that meet specified conditions." The AZ-800 study guide explains that scope-level policies can target clients by MAC address (Client Identifier), vendor class, user class, relay agent, or other fields, and when a lease is requested, "the DHCP server evaluates policies in order; if a client matches a policy, the server can allocate an address from the policy's configured IP range and apply policy-specific options, without affecting other clients in the scope." This is distinct from filters, which only allow or deny clients based on MAC and do not select an address pool; scope options merely set option values (DNS, router, etc.) and cannot constrain the lease address range; creating another scope would require a different subnet or superscope and would change allocation behavior for the entire network.

Given Scope1 (192.168.0.0/23) already serves all clients, and only the Teams Phone devices (all MACs in a common range) must receive addresses 192.168.1.100-192.168.1.200 without impacting others, the correct solution is to create a DHCP policy on Scope1 with a condition matching that MAC address range and configure the policy's IP address range to 192.168.1.100-192.168.1.200. This fulfills the requirement while leaving all other clients to receive addresses from the normal Scope1 pool.

質問: 52

オンプレミス ネットワークには、contoso.com という名前の Active Directory ドメインが含まれています。Azure AD テナントがあります。Azure AD Connect クラウド同期を使用し、contoso.com を Azure AD テナントと同期する予定です。Azure AD Connect クラウド同期で使用するアカウントを作成する必要があります。どの種類のアカウントを作成する必要がありますか？

- A. システム割り当てマネージド ID
- B. グループ管理サービス アカウント (gMSA)
- C. ユーザー
- D. InetOrgPerson

正解: **B** ([コメントを发表する](#))

In the AZ-800/"Administering Windows Server Hybrid Core Infrastructure" content, Azure AD Connect cloud sync uses a lightweight provisioning agent that reads from on-premises AD DS. The agent runs under a Group Managed Service Account (gMSA) so it can securely obtain and rotate credentials automatically. The implementation guidance states that during agent installation you provide domain admin credentials once so the installer can create and delegate a gMSA for the agent; alternatively, you can pre-create the gMSA and assign it. The documentation emphasizes that cloud sync does not rely on user or computer accounts with static passwords; instead it "deploys a gMSA for the agent service to ensure secure, automatic password management and least-privilege directory access." System-assigned managed identities apply to Azure resources only (not on-prem AD DS), and InetOrgPerson is an object class for users, not a service identity. A regular user account would introduce password management and rotation

issues and is not the recommended nor required identity type for the cloud sync agent. Therefore, to satisfy Azure AD Connect cloud sync prerequisites, you create and use a gMSA.

質問: 53

注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。

このセクションで質問に回答した後は、そのセクションに戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。

Windows Server を実行し、DHCP サーバーの役割を持つ Server1 というサーバーがあります。Server1 には、Scope 1 という 1 つの DHCP スコープが含まれています。

5 台のプリンターをネットワークに展開します。

プリンタに常に同じ IP アドレスが割り当てられていることを確認する必要があります。

解決策: ネットワークに DHCP リレー エージェントを展開します。

これは要件を満たしていますか?

A. はい

B. いいえ

正解: B ([コメントを发表する](#))

質問: 54

ネットワークには、contoso.com という名前の Active Directory Domain Services (AD DS) フォレストが含まれています。ルート ドメインには、次の表に示すドメイン コントローラが含まれています。

Name	FSMO role
DC1	Domain naming master
DC2	RID master
DC3	PDC emulator
DC4	Schema master
DC5	Infrastructure master

アプリケーション パーティションの作成を妨げるドメイン コントローラはどれですか?

A. DC1

B. DC2

C. DC3

D. DC4

E. DC5

正解: (正解を表示します)

In Administering Windows Server Hybrid Core Infrastructure, the operations that affect forest-wide naming contexts are tied to specific FSMO roles. The material explains that AD DS contains five FSMO roles-Schema Master, Domain Naming Master, RID Master, PDC Emulator, and Infrastructure Master-and each governs a unique set of authoritative changes. The course notes state:

"The Domain Naming Master is responsible for all changes to the forest namespace. This includes adding and removing domains and application directory partitions (also called application naming contexts). Because these operations change the forest-wide naming structure, the Domain Naming Master must be online and reachable to perform them." It further emphasizes: "Creation or deletion of application partitions is a forest-scoped operation. Only the Domain Naming Master can process these updates to ensure single-master consistency of the forest's name context metadata." By contrast, the Schema Master controls schema updates, the RID Master allocates RID pools, the PDC Emulator provides time sync and password update precedence, and the Infrastructure Master maintains cross-domain reference updates. None of these roles can substitute for the Domain Naming Master when creating application partitions. Therefore, if DC1 (which holds the Domain naming master role) fails, you cannot create new application partitions until that role holder is restored or the role is transferred/seized to another domain controller.

質問: 55

ネットワークには、contoso.com と fabrikam.com という 2 つの Active Directory ドメイン サービス (AD DS) フォレストがあります。これらのフォレスト間には双方向のフォレスト信頼が確立されています。各フォレストには 1 つのドメインが含まれています。これらのドメインには、次の表に示すサーバーが含まれています。

Name	Domain	Description
Server1	contoso.com	Hosts a Windows Admin Center gateway
Server2	fabrikam.com	Hosts resources that will be managed remotely by using Windows Admin Center on Server1

contoso.com のユーザーがサーバー上の Windows Admin Center を使用してサーバーに接続できるように、リソーススペースの制約付き委任を構成する必要があります。コマンドはどのように実行すればよいですか？回答するには、回答領域で適切なオプションを選択してください。注：正しい選択ごとに1ポイントが加算されます。

Answer Area

Set-ADComputer -Identity (Get-ADComputer server1.contoso.com) (Get-ADComputer server2.fabrikam.com) (Get-ADGroup 'Contoso\Domain Users') (Get-ADGroup 'Fabrikam\Domain Users')

-PrincipalsAllowedToDelegateToAccount (Get-ADComputer server1.contoso.com) (Get-ADComputer server2.fabrikam.com) (Get-ADGroup 'Contoso\Domain Users') (Get-ADGroup 'Fabrikam\Domain Users')

正解:

Answer Area

Set-ADComputer -Identity (Get-ADComputer server1.contoso.com) (Get-ADComputer server2.fabrikam.com) (Get-ADGroup 'Contoso\Domain Users') (Get-ADGroup 'Fabrikam\Domain Users')

-PrincipalsAllowedToDelegateToAccount (Get-ADComputer server1.contoso.com) (Get-ADComputer server2.fabrikam.com) (Get-ADGroup 'Contoso\Domain Users') (Get-ADGroup 'Fabrikam\Domain Users')

Explanation:

Set-ADComputer -Identity

(Get-ADComputer server1.contoso.com)
(Get-ADComputer server2.fabrikam.com)
(Get-ADGroup 'Contoso\Domain Users')
(Get-ADGroup 'Fabrikam\Domain Users')

-PrincipalsAllowedToDelegateToAccount

(Get-ADComputer server1.contoso.com)
(Get-ADComputer server2.fabrikam.com)
(Get-ADGroup 'Contoso\Domain Users')
(Get-ADGroup 'Fabrikam\Domain Users')

In the Administering Windows Server Hybrid Core Infrastructure guidance for Windows Admin Center (WAC) and Kerberos delegation, resource-based constrained delegation (RBCD) is configured on the resource's computer account, not on the client/gateway. The documentation explains that "resource-based constrained delegation is applied to the target service account; the target's msDS- AllowedToActOnBehalfOfOtherIdentity attribute contains the security principals (computers or service accounts) that are permitted to act on behalf of users." It further clarifies that "this model supports cross- domain and cross-forest scenarios when a trust exists; you specify the front-end computer (for example, a WAC gateway) from the trusted forest as an allowed principal on the resource computer in its own domain." For WAC, the gateway (Server1 in contoso.com) must be allowed to delegate to the managed node (Server2 in fabrikam.com). The study materials show the exact PowerShell interface: "Use Set-ADComputer with - PrincipalsAllowedToDelegateToAccount to populate the resource's allowed-to-act list." Therefore, the Identity parameter must reference the resource computer account (Server2 in fabrikam.com), and the PrincipalsAllowedToDelegateToAccount parameter must reference the gateway computer account (Server1 in contoso.com).

Hence the correct command is:

```
Set-ADComputer -Identity (Get-ADComputer server2.fabrikam.com) -  
PrincipalsAllowedToDelegateToAccount (Get-ADComputer server1.contoso.com)
```

質問: 56

Windows Server 2022 を実行し、コンテナホストとして構成された Host1 というサーバーがあります。Host1 には、Windows Server 2019 をベースにした image1 というコンテナイメージが格納されています。

Host1 上の image1 からコンテナを起動する必要があります。

コマンドをどのように完了すればよいですか？ 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

Answer Area



Explanation:

Answer Area



In Windows Server container deployments, the isolation mode determines kernel compatibility between the host and the container image. The Administering Windows Server Hybrid Core Infrastructure materials explain that Windows Server containers using process isolation share the host kernel and therefore require the container image to match the host's OS version/build. The guide contrasts this with Hyper-V isolation, stating that each container runs inside a lightweight utility VM: "Hyper-V isolated containers do not share the host kernel; they provide a separate kernel instance, allowing containers built on a different Windows build (or earlier Windows Server version) to run on a newer host." Because Host1 is Windows Server 2022 and image1 is based on Windows Server 2019, process isolation would fail due to the version mismatch. The documented remediation is to start the container with Hyper-V isolation, which decouples the container from the host's kernel requirements. The study guide shows this operationally with Docker: "Use docker run ... --isolation=hyperv when the container base image version differs from the host." Therefore, to successfully start the container on Host1, you must use the Docker CLI with Hyper-V isolation:

Docker run -d --isolation=hyperv image1.

質問: 57

Windows Server を実行し、Share1 という名前のファイル共有を含む Server1 という名前のサーバーがあります。

Share1 でユーザーが MP4 ファイルを保存できないようにする必要があります。このソリューションでは、ユーザーが他の種類のファイルを共有に保存できるようにする必要があります。

Server1 で何を構成する必要がありますか？

- A. ファイル管理タスク
- B. NTFSクォータ
- C. NTFS アクセス許可
- D. ファイルスクリーン

正解: [\(正解を表示します\)](#)

In the Administering Windows Server Hybrid Core Infrastructure content for File Services, Microsoft describes File Server Resource Manager (FSRM) as the feature used to control the types of files that users can store on file servers. The guide explains that a file screen "prevents users from saving unauthorized file types on a volume or in a folder by applying a file group (such as Audio and Video) or custom file name patterns (for example, *.mp4)." It further clarifies that file screening "does not affect access permissions to other files and folders and allows permitted file types to be stored without restriction." By contrast, NTFS permissions govern access (read/write/modify) and "cannot filter by file extension," and NTFS quotas and File Management Tasks address capacity and automated tasks, not content blocking. Therefore, to stop users from storing .MP4 while allowing all other files, you create a File Screen on the path to Share1 and block either the built-in Audio and Video file group or a custom pattern *.mp4. This aligns precisely with the exam guide's directive that FSRM File Screening is the supported and intended method to restrict file types on Windows file shares while leaving other file operations unaffected.

質問: 58

ネットワークには、contoso.com と adatum.com という 2 つの Active Directory ドメイン サービス (AD DS) フォレストがあります。contoso.com と adatum.com の間には双方向の外部信頼が確立されています。これらのフォレストには、次の表に示すサーバーが含まれています。

Name	In domain	Description
DC1	contoso.com	Hosts all FSMO roles
DC2	adatum.com	Hosts all FSMO roles
SRV1	adatum.com	File server
SRV2	adatum.com	File server

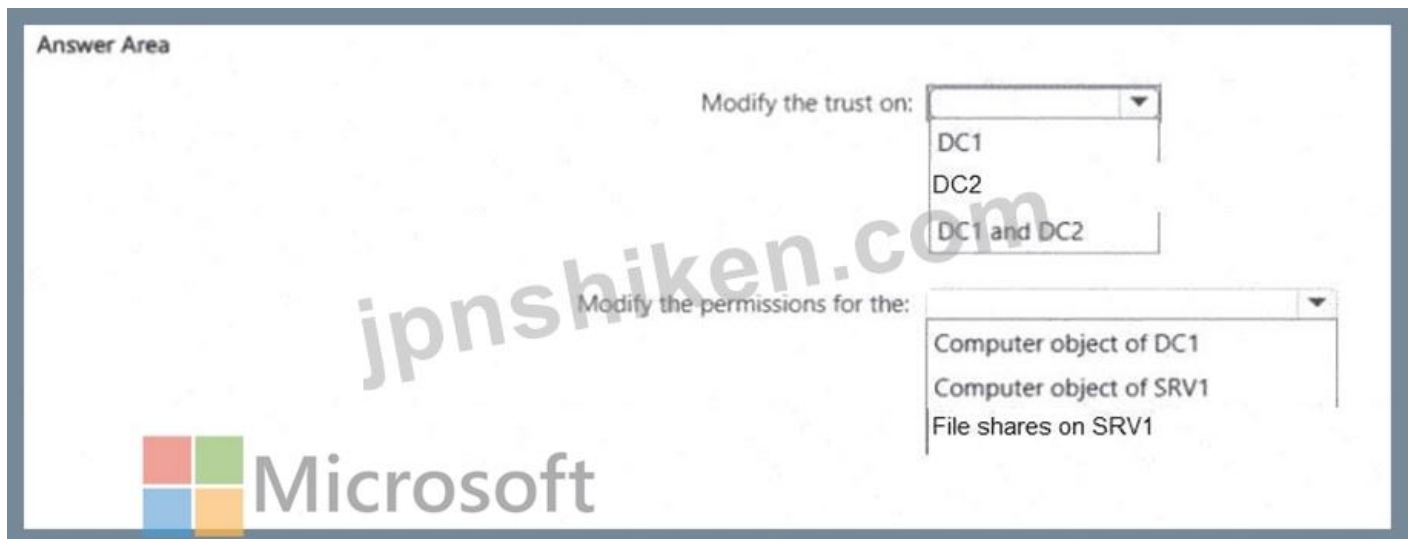
contoso.com のユーザーが SRV1 でホストされている共有リソースにのみアクセスできるようにする必要があります。ソリューションは以下の要件を満たす必要があります。

* adatum.com のユーザーが contoso.com でホストされているリソースにアクセスできることを確認します。

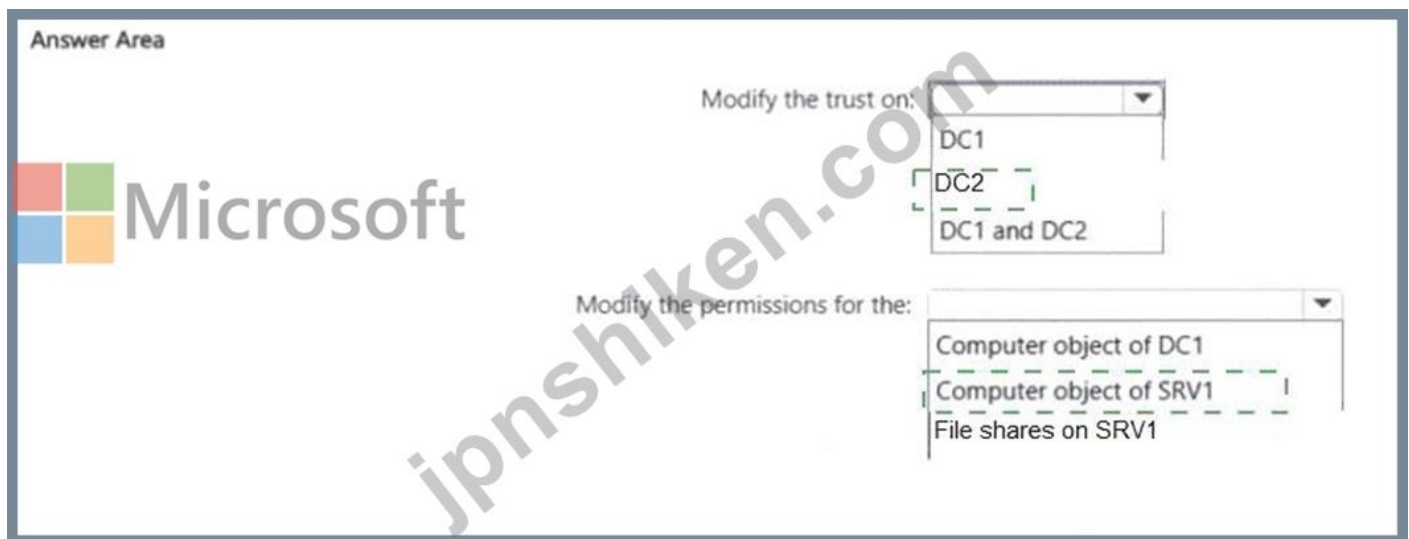
* contoso.com ユーザーが adatum.com 内の他のリソースにアクセスできないようにします。

どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Modify the trust on: DC2

* Modify the permissions for the: Computer object of SRV1

In an Active Directory Domain Services (AD DS) environment involving multiple forests and external trusts, managing granular access across domain boundaries is achieved through Selective Authentication.

According to official documents for Administering Windows Server Hybrid Core Infrastructure, there are two primary authentication settings for a trust: Domain-wide authentication and Selective authentication.

When you need to restrict users from a trusted forest (contoso.com) so they can only access specific resources in the trusting forest (adatum.com), you must configure the trust to use Selective Authentication. This configuration must be performed in the resource domain (the trusting domain). Based on the provided table, DC2 is the domain controller for adatum.com, which is where the shared resources (SRV1) reside.

Therefore, you must modify the trust properties on DC2 to enable Selective Authentication for the incoming trust from contoso.com.

Once Selective Authentication is enabled, Windows does not automatically grant the "Authenticated Users" SID to the user's access token for resources in the local domain. Instead, administrators must explicitly grant the Allowed to Authenticate permission on the specific resource's computer object. In this scenario, since the requirement is to restrict access specifically to resources on SRV1, you must modify the security permissions on the Computer object of SRV1 in Active Directory Users and Computers. By granting the contoso.com users (or a group containing them) this permission, they can successfully authenticate against SRV1 while being blocked from all other servers in the adatum.com forest. This satisfies the requirement to prevent access to any other resources while maintaining the ability of adatum.com users to access contoso.com (as the 2-way trust remains intact).

質問: 59

タスク5

SRV1 の C:\app というフォルダにコピーされたアプリケーションがあります。C:\app には、アプリ用の Dockerfile も含まれています。

SRV1では、Dockerfileを使用してアプリケーションのコンテナイメージを作成する必要があります。コンテナイメージの名前はapp1にする必要があります。

正解:

See the solution of this Task below.

Explanation:



Explore

To create a container image named app1 for your application using the Dockerfile in the C:\app directory on SRV1, follow these steps:

Step 1: Open PowerShell or Command Prompt First, open PowerShell or Command Prompt on SRV1.

Step 2: Navigate to the Application Directory Change to the directory where your application and Dockerfile are located:

```
cd C:\app
```

Step 3: Build the Container Image Use the docker build command to create the container image. The -t flag tags the image with the name app1:

```
docker build -t app1 .
```

The period . at the end of the command tells Docker to use the Dockerfile in the current directory.

Step 4: Verify the Image Creation After the build process completes, verify that the image app1 has been created successfully by listing all images:

docker images

You should see app1 in the list of images.

Step 5: Use the Image Now, you can use the image app1 to run containers or push it to a container registry if needed.

By following these steps, you'll have created a Docker container image named app1 using the Dockerfile located in C:\app on SRV11. Ensure that Docker is installed on SRV1 and that you have the necessary permissions to execute these commands.

質問: 60

ネットワークには、次の表に示すセグメントが含まれています。

Name	IPv4 address space	Gateway
Segment1	172.16.1.0/24	172.16.1.1
Segment2	172.16.2.0/24	172.16.2.1

Windows Server を実行し、次の表のように構成されているサーバーがあります。

Name	IPv4 address	Connected to	Windows Defender Firewall configuration
Server1	172.16.1.10	Segment1	Allow ICMP traffic
Server2	172.16.2.2	Segment1	Allow ICMP traffic
Server3	172.16.2.20	Segment2	Allow ICMP traffic

Windows Serverを実行し、静的IPアドレス172.16.1.1を持つServer4というサーバーを展開します。Server4をSegment1に接続します。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Microsoft

ipnshiken.com

Statements	Yes	No
Server1 can successfully ping Server2 by using the name of Server2.	☐	☐
Server2 can successfully ping Server3 by using the IP address of Server3.	☐	☐
Running <code>ipconfig /all</code> on Server4 will display an IP address from the 169.254.0.0/16 IPv4 address space.	☐	☐

正解:

Answer Area

Microsoft

ipnshiken.com

Statements	Yes	No
Server1 can successfully ping Server2 by using the name of Server2.	☐	☒
Server2 can successfully ping Server3 by using the IP address of Server3.	☐	☒
Running <code>ipconfig /all</code> on Server4 will display an IP address from the 169.254.0.0/16 IPv4 address space.	☐	☒

Explanation:

< Server1 can successfully ping Server2 by using the name of Server2. No Server2 can successfully ping Server3 by using the IP address of Server3. No Running ipconfig /all on Server4 will display an IP address from the 169.254.0.0/16 IPv4 address space.

No

The Windows Server networking objectives explain that hosts determine whether a destination is local by comparing the destination IP to their own subnet and mask. If the destination is outside the local subnet, traffic is sent to the default gateway; if it is within the local subnet, the host uses ARP to resolve the destination MAC on the local segment. In this scenario, Server1 (172.16.1.10/24) and Server2 (172.16.2.2/24) are on different subnets. Even though Server2 is physically attached to Segment1, its IP places it in the 172.16.2.0/24 network. When Server1 pings Server2 (by name or IP), name resolution returns 172.16.2.2, which Server1 treats as remote and forwards to the gateway 172.16.1.1. The router will forward toward Segment2 (172.16.2.0/24), where Server2 is not physically present, so communication fails. Similarly, Server2 # Server3: Server2 believes 172.16.2.20 is local and issues an ARP on Segment1; ARP cannot cross to Segment2, so no reply-ping fails. The materials also note that APIPA (169.254.0.0/16) is assigned only when DHCP fails on DHCP-configured interfaces. Because Server4 was configured with a static address (172.16.1.1), ipconfig /all will show that static IP, not an APIPA address. Additionally, assigning 172.16.1.1 to Server4 conflicts with the listed gateway, further preventing routed communication but does not change the fact that Server4 uses its configured static IP.

質問: 61

タスク7

Microsoft Defender for Cloud を使用して DC1 のセキュリティ構成を監視する必要があります。
必要なソース ファイルは、\\dc1.contoso.com\install という名前のフォルダーにあります。

正解:

See the solution of this Task below.

Explanation:

One possible solution to monitor the security configuration of DC1 by using Microsoft Defender for Cloud is to use the Guest Configuration feature. Guest Configuration is a service that audits settings inside Linux and Windows virtual machines (VMs) to assess their compliance with your organization's security policies. You can use Guest Configuration to monitor the security baseline settings for Windows Server in the Microsoft Defender for Cloud portal by following these steps: On DC1, open a web browser and go to the folder named \\dc1.contoso.com\install. Download the Guest Configuration extension file (GuestConfiguration.msi) and save it to a local folder, such as C:\Temp.

Run the Guest Configuration extension file and follow the installation wizard. You can choose to install the extension for all users or only for the current user. For more information on how to install the Guest Configuration extension, see Install the Guest Configuration extension.

After the installation is complete, sign in to the Microsoft Defender for Cloud portal (2).

In the left pane, select Security Center and then Recommendations.

In the recommendations list, find and select Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration).

In the Remediate Security Configurations page, you can see the compliance status of your Windows VMs, including DC1, based on the Azure Compute Benchmark. The Azure Compute Benchmark is a set of rules that define the desired configuration state of your VMs. You can also see the number of failed, passed, and skipped rules for each VM. For more information on the Azure Compute Benchmark, see Microsoft cloud security benchmark: Azure compute benchmark is now available.

To view the details of the security configuration of DC1, click on the VM name and then select View details.

You can see the list of rules that apply to DC1 and their compliance status. You can also see the severity, description, and remediation steps for each rule. For example, you can see if DC1 has the latest security updates installed, if the firewall is enabled, if the password policy is enforced, and so on.

To monitor the security configuration of DC1 over time, you can use the Compliance over time chart, which shows the trend of compliance status for DC1 in the past 30 days. You can also use the Compliance breakdown chart, which shows the distribution of compliance status for DC1 by rule severity.

By using Guest Configuration, you can monitor the security configuration of DC1 by using Microsoft Defender for Cloud and ensure that it meets your organization's security standards. You can also use Guest Configuration to monitor the security configuration of other Windows and Linux VMs in your Azure environment.

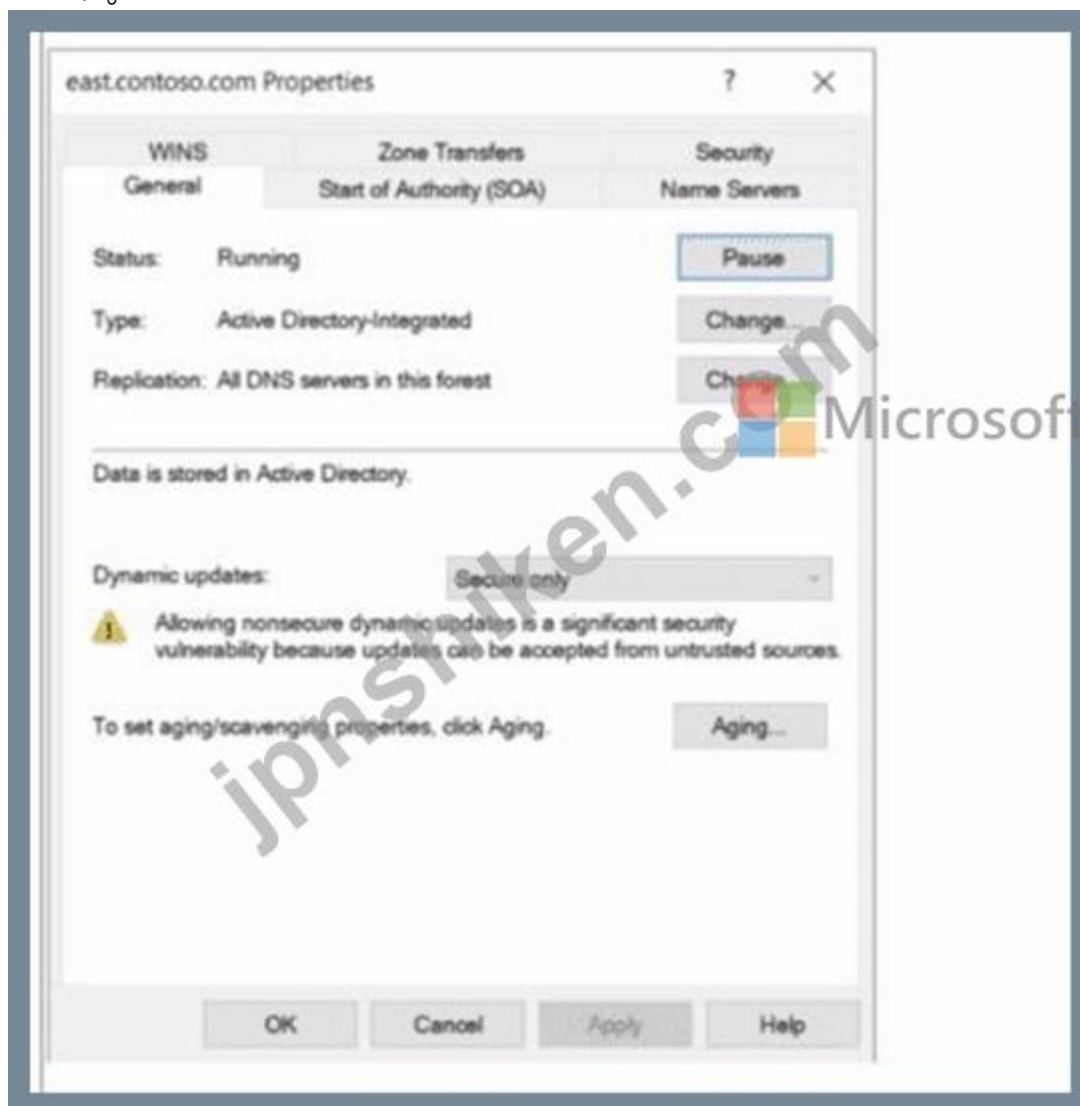
有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/AZ-800J-mondaishu> **262**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 62

ネットワークには、contoso.com という名前の Active Directory ドメイン サービス (AD DS) フォレストが含まれています。このフォレストには、次の表に示すサーバーが含まれています。サーバー1はcontoso.comのDNSゾーンをホストしています。contoso.comのプロパティの 全般」タブは、次の図に示すように構成されています。



Server3 は east.contoso.com の DNS ゾーンをホストしており、次の図に示すように構成されています。



以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Statements	Yes	No
A secondary DNS zone for contoso.com can be added to Server3.	☐	☐
If you add a DNS record to contoso.com, the record will replicate to Server2.	☐	☐
If you add a DNS record to east.contoso.com, the record will replicate to Server1.	☐	☐

正解:

Statements	Yes	No
A secondary DNS zone for contoso.com can be added to Server3.	☒	☐
If you add a DNS record to contoso.com, the record will replicate to Server2.	☒	☐
If you add a DNS record to east.contoso.com, the record will replicate to Server1.	☒	☐

Explanation:

A secondary DNS zone for contoso.com can be added to Server3.: Yes

If you add a DNS record to contoso.com, the record will replicate to Server2.: Yes

If you add a DNS record to east.contoso.com, the record will replicate to Server1.: Yes
The replication and availability of DNS data in a Windows Server environment are dictated by the zone type and its replication scope. According to official documentation, Active Directory-integrated zones provide high availability and multi-master replication.

* Secondary Zone Availability: A secondary zone is a read-only copy of a DNS zone hosted on another server (the master). Standard DNS protocol allows any DNS server, regardless of its role as a Domain Controller, to host a secondary zone for any reachable primary zone. Since Server3 is a member server, it can host a secondary zone for contoso.com to provide local name resolution.

* Replication of contoso.com: The properties for the contoso.com zone on Server1 show the replication scope is set to "All DNS servers in this domain". Since Server1 and Server2 are both domain controllers in the contoso.com domain, any record added to this zone will automatically replicate between them through the Active Directory replication process.

* Replication of east.contoso.com: The properties for the east.contoso.com zone on Server3 show the replication scope is set to "All DNS servers in this forest". In Active Directory, the forest-wide replication scope stores the DNS zone in the ForestDnsZones partition. This partition is replicated to every domain controller that runs the DNS Server service throughout the entire forest. Because Server1 is a domain controller within the same forest (contoso.com root), it will receive the replicated records from the east.contoso.com zone.

質問: 63

タスク 4

SRV1 上で mcr.microsoft.com/windows/servercore/iis イメージを使用するコンテナを実行する必要があります。コンテナのポート 80 を SRV1 のポート 5001 に公開し、コンテナをバックグラウンドで実行する必要があります。このタスクの解決策については、以下を参照してください。

正解:

To run a container on SRV1 using the mcr.microsoft.com/windows/servercore/iis image, publish port 80 on the container to port 5001 on SRV1, and ensure it runs in the background, you can follow these steps:

Step 1: Pull the IIS Image First, pull the correct IIS image from the Microsoft Container Registry:
`docker pull mcr.microsoft.com/windows/servercore/iis`

Step 2: Run the Container Next, run the container with the required port mapping and ensure it runs in the background using the -d flag:

`docker run -d -p 5001:80 --name iis_container mcr.microsoft.com/windows/servercore/iis` This command will start a container named iis_container using the IIS image, map port 80 inside the container to port 5001 on SRV1, and run the container in detached mode.

Step 3: Verify the Container is Running To verify that the container is running and the port is published, use the following command:

`docker ps`

This will list all running containers and show the port mappings.

Step

4: Access the IIS Server You can now access the IIS server running in the container by navigating to `http://`

`<SRV1_IP>:5001` in a web browser, where `<SRV1_IP>` is the IP address of SRV1.

Note: Ensure that Docker is installed on SRV1 and that the port 5001 is open on the firewall to allow incoming connections¹.

By following these steps, you should be able to run the IIS container on SRV1 with the specified port mapping and have it running in the background. Please replace `mcr.microsoft.com/windows/servercore/iis` with the correct image name `mcr.microsoft.com/windows/servercore/iis` as shown in the commands above.

質問: 64

sub1 という名前の Azure サブスクリプションと、Windows Server を実行する 500 台のオンプレミス仮想マシンがあります。

Azure Arc デプロイ スクリプトを実行して、オンプレミスの仮想マシンを Azure Arc にオンボードする予定です。スクリプトでサブ 1 へのアクセスを認証するために使用する ID を作成する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。

コマンドをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

New-AzADAppCredential New-AzADServicePrincipal New-AzUserAssignedIdentity	-DisplayName 'Arc-for-servers' -Role	Azure Connected Machine Onboarding' 'Virtual Machine Contributor' 'Virtual Machine User Login'
---	--------------------------------------	--

正解:

Answer Area

New-AzADAppCredential New-AzADServicePrincipal New-AzUserAssignedIdentity	-DisplayName 'Arc-for-servers' -Role	Azure Connected Machine Onboarding' 'Virtual Machine Contributor' 'Virtual Machine User Login'
---	--------------------------------------	--

Explanation:

New-AzADAppCredential New-AzADServicePrincipal New-AzUserAssignedIdentity	-DisplayName 'Arc-for-servers' -Role	Azure Connected Machine Onboarding' 'Virtual Machine Contributor' 'Virtual Machine User Login'
---	--------------------------------------	--

Reference:

In the Administering Windows Server Hybrid Core Infrastructure objectives for managing Azure Arc-enabled servers, Microsoft specifies that onboarding non-Azure machines with the scripted onboarding method requires an Azure AD application/service principal with the least-privileged built-in role expressly created for Arc onboarding. The study guide states that: "For scripted onboarding at scale, create an Azure AD service principal and assign the Azure Connected Machine Onboarding role at the required scope (subscription or resource group). This role grants only the permissions necessary for the connect operation and agent registration; it does not confer general virtual machine management rights." The PowerShell guidance in the same module explains that a service principal can be created and granted a role in one step using New-AzADServicePrincipal, providing a display name and a role assignment: "Use New-AzADServicePrincipal with the -DisplayName parameter to create the application identity and the -Role (and optionally -Scope) parameters to assign the built-in role needed for onboarding." It also contrasts other cmdlets: "New-AzADAppCredential updates credentials for an existing application only; New-AzUserAssignedIdentity creates a managed identity resource and is not used for Arc scripted onboarding." Because the question asks for an identity used by the Azure Arc deployment script and to follow the principle of least privilege, the correct command is to create a service principal and assign the minimal role: New-AzADServicePrincipal -DisplayName 'arc-for-servers' -Role 'Azure Connected Machine Onboarding'. Other roles such as Virtual Machine Contributor or Virtual Machine User Login exceed what Arc onboarding requires and therefore violate least-privilege guidance.

質問: 65

VM2 の技術要件を満たす必要があります。

何をすべきでしょうか？

- A. シールドされた仮想マシンを実装します。
- B. ゲスト サービス統合サービスを有効にします。
- C. Credential Guard を実装します。

D. 拡張セッション モードを有効にします。

正解: ([正解を表示します](#))

In the Administering Windows Server Hybrid Core Infrastructure materials under Hyper-V management, Microsoft specifies that Enhanced Session Mode changes VMConnect from a raw console attach to a connection that uses Remote Desktop Protocol (RDP) to the guest. The guide states that Enhanced Session Mode "uses RDP to establish the VMConnect session so the user must supply credentials for a logon to the guest operating system," and further that it "prevents a second administrator from inheriting an already signed-in console session" because the connection is treated as a new interactive sign-in. In contrast, the default basic console session "attaches directly to the active console without prompting for credentials," which is exactly the current problem described for VM2.

The same objective area clarifies that other options do not meet the requirement: Guest Services integration only enables file copy and certain host-guest interactions; Credential Guard protects secrets inside Windows by isolating LSASS but does not affect Hyper-V console connection behavior; Shielded VMs provide fabric-level protections and encryption but are not required merely to force credential prompts for VMConnect.

Therefore, to force users to provide credentials when they connect to VM2 and to eliminate inherited console sessions, you should enable Enhanced Session Mode on the Hyper-V host (and ensure the guest supports RDP).

質問: 66

オンプレミス ネットワークの IP アドレス範囲は 10.0.0.0/23 です。

VNet1 という名前の Azure 仮想ネットワークがあり、そこには VM1 という名前の仮想マシンが含まれています。VNet1 の IP アドレス範囲は 10.0.1.0/24 です。

オンプレミス ネットワークを VNet1 に接続するには、サイト間 (S2S) VPN をデプロイする必要があります。

まず何をすべきでしょうか？

A. VNet1 を IP アドレス範囲 10.0.1.128/25 を使用するように構成します。

B. Azure Bastion を VNet1 にデプロイします。

C. VNet1 を IP アドレス範囲 10.0.2.0/24 を使用するように構成します。

D. Azure 拡張ネットワークをデプロイします。

正解: ([正解を表示します](#))

For Site-to-Site VPNs, the exam guide states that "the on-premises address spaces and the Azure virtual network address spaces must not overlap." Overlapping prefixes prevent route advertisement and creation of connections. Your on-premises network uses 10.0.0.0/23, which spans 10.0.0.0-10.0.1.255. The current VNet1 space is 10.0.1.0/24, which sits inside the on-premises supernet and therefore overlaps. The guidance instructs: "Before configuring gateways and connections, ensure VNet address ranges are unique and non-overlapping with any local networks." Options like deploying Bastion or Azure Extended Network don't change IP topology and won't resolve the overlap. Subnetting VNet1 to 10.0.1.128/25 also still overlaps the

10.0.0.0/23 range. The correct first step is to change VNet1's address space to a non-overlapping range, such as 10.0.2.0/24, and then proceed to deploy the virtual network gateway and the S2S connection. This aligns with the required prerequisite in the study material that unique address spaces are mandatory for successful S2S VPN routing.

質問: 67

タスク5

SRV1 上の scope1 という名前の DHCP スコープがクライアント要求を処理できることを確認する必要があります。

正解:

See the solution of this Task below.

Explanation:

One possible solution to ensure that a DHCP scope named scope1 on SRV1 can service client requests is to activate the scope on the DHCP server. A scope must be activated before it can assign IP addresses to DHCP clients. To activate a DHCP scope on SRV1, perform the following steps:

On SRV1, open DNS Manager from the Administrative Tools menu or by typing dnsmgmt.msc in the Run box.

In the left pane, expand your DHCP server and click on IPv4.

In the right pane, right-click on the scope that you want to activate, such as scope1, and select Activate.

Wait for the scope to be activated. You can verify the activation status by checking the icon next to the scope name. A green arrow indicates that the scope is active, while a red arrow indicates that the scope is inactive.

Now, the DHCP scope named scope1 on SRV1 can service client requests and lease IP addresses to DHCP clients. You can test the DHCP service by using the `ipconfig /renew` command on a DHCP client computer that is connected to the same subnet as the scope.

質問: 68

Windows Server を実行する Server1 という名前のサーバーがあり、Server1 には JBOD (Just-A-Bunch-Of-Disks) エンクロージャが接続されています。

Server1 にストレージ プールと、ミラー レイアウトを使用する仮想ディスクを作成する予定です。

2 方向ミラー レイアウトを使用するか、3 方向ミラー レイアウトを使用するかを検討しています。

各タイプのマイナー レイアウトに必要なディスクの最小数はいくつですか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Two-way mirror:

1
2
3
4
5
6

Three-way mirror:

1
2
3
4
5
6



正解:

ANSWER AREA



Two-way mirror:

1
2
3
4
5
6

Three-way mirror:

1
2
3
4
5
6

Explanation:

Two-way mirror: 2

Three-way mirror: 5

In the Administering Windows Server Hybrid Core Infrastructure materials, the Storage Spaces guidance explains that mirror layouts keep multiple copies of each slab of data across different physical drives in a pool. A two-way mirror maintains two copies, so the pool must contain at least two physical disks to place each copy on a separate disk. This provides protection from a single disk failure with continuous availability.

For higher resiliency, a three-way mirror maintains three copies of every write. The Windows Server implementation requires a minimum of five physical disks in the pool to create a three-way mirror virtual disk. The extra drives beyond the three copies are needed to satisfy the layout/columning rules used by Storage Spaces for performance striping and to ensure there is sufficient distribution to sustain a failure and still have capacity and parallelism for repair operations. The curriculum emphasizes that mirror spaces are recommended for workloads

needing fast writes and quick recovery, while parity spaces trade performance for capacity efficiency. Therefore, when planning a JBOD-backed storage pool on a single Windows Server, you must allocate at least 2 disks for a two-way mirror and at least 5 disks for a three-way mirror to meet the platform's resiliency and layout requirements.

質問: 69

ネットワークには Active Directory ドメイン サービス (AD DS) ドメインが含まれています。ドメインには次の表に示すリソースが含まれています。

Name	Description
CLIENT1	Client computer that runs Windows
DC1	Domain controller
Server1	File server
Server2	File server

ストレージレプリカを使用して、Server1 から Server2 にボリュームをレプリケートする予定です。

ストレージレプリカを構成する必要があります。

Windows Admin Center はどこにインストールすればよいですか？

- A. Server 1
- B. CLIENT1
- C. DC1
- D. Server2

正解: B ([コメントを发表する](#))

The AZ-800 materials emphasize Windows Admin Center (WAC) as the unified, browser-based management tool for Windows Server features including Storage Replica. The guidance explains two common installation modes: desktop mode (install WAC on a management workstation) and gateway mode (install on a management server). In either case, WAC remotely manages target servers (Server1/Server2) over WinRM

/PowerShell-WAC does not need to be installed on the source or destination file servers to configure replication partnerships, volumes, or test failover. Best practice in the study content is to install WAC on a management computer and add the servers as managed nodes, then use the Storage Replica tool in WAC to create a partnership, select source/target volumes, and monitor replication health. Installing WAC on a domain controller is discouraged, and installing it directly on the file servers is unnecessary. Consequently, to configure Storage Replica between Server1 and Server2, you should install Windows Admin Center on the client management computer (CLIENT1) and use it to manage and configure the replication on both servers remotely.

質問: 70

ネットワークには、contoso.com と fabrikam.com という 2 つの Active Directory ドメイン サービス (AD DS) フォレストが含まれています。Contoso.com には、amer.contoso.com、apac.contoso.com、emea.contoso.com という 3 つの子ドメインが含まれています。Fabrikam.com には、apac.fabrikam.com という子ドメインが含まれています。contoso.com と fabrikam.com の間には、双方向のフォレスト信頼が確立されています。contoso.com フォレスト内のユーザーに、fabrikam.com フォレスト内のリソースへのアクセス権を付与する必要があります。

ソリューションは次の要件を満たす必要があります。

- * contoso.com 内のユーザーは、contoso.com フォレスト内のグループにのみ直接追加する必要があります。

- * fabrikam.com 内のリソースにアクセスするための権限は、fabrikam 内のグループにのみ直接付与する必要があります。

com フォレスト。

- * グループの数は最小限に抑える必要があります。

ユーザーを整理し、権限を割り当てるには、どの種類のグループを使用すべきでしょうか？ 適切なグループの種類を適切な要件に合わせてドラッグしてください。各グループの種類は、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

The Windows Server hybrid core administration guidance describes the classic cross-forest/group nesting model as AGUDLP: "Accounts # Global (or Universal) # Domain Local # Permissions." For resource access that spans forests, the documentation stresses two points: (1) Put user accounts into groups that exist only in their own forest, and (2) Grant ACL permissions only to

groups that exist in the resource forest. It further explains that Universal groups are forest-wide and "can contain users and global groups from any domain in the same forest and can be used across forest trusts," which minimizes the number of groups when users come from multiple child domains. By contrast, Domain Global groups are limited to membership from a single domain, which would require separate globals per child domain and thus more groups. For assigning permissions at the resource side, the guidance states that Domain Local groups are intended to "receive permissions on resources within their own domain and can contain members from trusted forests," which satisfies the requirement that permissions in fabrikam.com be granted only to groups in that forest. Therefore, to meet all constraints and minimize group count: place contoso.com users in a Universal group (in contoso.com) and add that group to a Domain Local group (in fabrikam.com) that is granted the required permissions.

質問: 71

Server1 という名前の Windows Server コンテナ ホストがあります。

df1 という名前の Dockerfile を作成します。

dt1 を使用してコンテナ イメージを生成する必要があります。

どのコマンドを実行する必要がありますか？

- A. docker create
- B. docker build
- C. docker exec
- D. docker images

正解: **B** ([コメントを发表する](#))

Infrastructure documents: =

In the Windows Server container objectives of Administering Windows Server Hybrid Core Infrastructure, image creation is performed from a Dockerfile by using the build workflow. The guide explains that a Dockerfile is a "text manifest of instructions that define how to assemble an image." To produce the actual image, you run docker build against a build context, optionally specifying the Dockerfile name and the image tag. The study text notes: "Use docker build to compile a container image from a Dockerfile; the command processes each instruction (FROM, COPY, RUN, EXPOSE, etc.) and writes the resulting layers to a new image." Other commands serve different purposes: docker exec runs a command inside an existing container; docker create prepares a container from an already-built image without starting it; docker images merely lists images. Therefore, to generate an image from df1, you would run a command such as docker build -f df1 -t contoso/app:1.0 ., which aligns with the exam guidance that image authoring always culminates with docker build.

質問: 72

タスク3

contoso.com に Admin1 という名前のユーザーを 3 人作成する必要があります。Admin1 は SRV1 上のファイルのバックアップと復元を実行できる必要があります。このソリューションでは、最小権限の原則を適用する必要があります。

正解:

See the solution of this Task below.

Explanation:

TASK 3

Objective:

Create a user named Admin1 in contoso.com.

Admin1 must be able to back up and restore files on SRV1.

Follow the principle of least privilege.

Step-by-Step Guide

Step 1: Create the User Account

Log in to a Domain Controller (e.g., DC1) with appropriate admin rights.

Open Active Directory Users and Computers (dsa.msc).

In the contoso.com domain:

Right-click the Users container or another OU where you want to create the account.

Select New > User.

Enter the following:

First name: Admin1

User logon name: Admin1

Click Next and set a password (ensure it meets the domain's password policy).

Configure password options (e.g., User must change password at next logon, if required).

Click Finish.

Step 2: Grant Backup and Restore Rights on SRV1

By default, Backup Operators have the ability to back up and restore files (without giving full admin rights).

Log in to SRV1 (the target server).

Open Computer Management (compmgmt.msc).

In the left pane, expand:

System Tools > Local Users and Groups > Groups.

Find and double-click the Backup Operators group.

Click Add.

In the Select Users, Computers, Service Accounts, or Groups window:

Type Admin1.

Click Check Names to resolve the user.

Click OK to add Admin1 to the group.

Click OK again to close the Backup Operators group properties.

Step 3: Verify Access

Log in as Admin1 on SRV1 and test performing backup and restore operations using tools like Windows Server Backup.

Since Backup Operators can back up and restore data but do not have full administrative privileges, this follows the least privilege principle.

Additional Notes

If you prefer using PowerShell, you can add the user to the group like this on SRV1:

```
Add-LocalGroupMember -Group "Backup Operators" -Member "contoso\Admin1"
```

質問: 73

Server1の技術要件を満たす必要があります。現在、必要なタスクを実行できるユーザーは誰ですか？

- A. 管理者1のみ
- B. 管理者3のみ
- C. Admin1とAdmin3のみ
- D. Admin1 Admin2. および Admm3

正解: ([正解を表示します](#))

In the AZ-800 "Administering Windows Server Hybrid Core Infrastructure" objectives for Active Directory, server promotion is governed by forest/domain administrative roles. The materials state that promoting a member server to a domain controller in a given domain requires membership in either the Enterprise Admins group or the Domain Admins group of the target domain. The Configuration and Domain naming contexts that DCPromo touches (NTDS settings, SYSVOL/DFS-R readiness, DC computer account, and associated service SPNs) are protected so that "Enterprise Admins have full rights forest-wide, and Domain Admins have full rights within their respective domain." In this case, the requirement is to promote Server1 to a domain controller in canada.contoso.com. From the identities table:

- * Contoso\Admin1 is a member of Enterprise Admins (forest-wide authority).
- * Canada\Admin3 is a member of Canada\Domain Admins (authority within canada.contoso.com).
- * Contoso\Admin2 is Domain Admins (contoso.com) only, which does not grant administrative authority in the canada.contoso.com child domain.

Therefore, the users who can currently perform the required task for Server1 are Admin1 and Admin3.

質問: 74

Azure Virtual Desktop セッションホストがセキュリティ要件を満たすように、グループポリシー設定を構成する必要があります。何を構成すればよいですか？

- A. GP04のリンクのセキュリティフィルタリング
- B. GPO1のリンクのセキュリティフィルタリング
- C. GPO4におけるループバック処理
- D. GP01のリンクの強制プロパティ
- E. GPO1でのループバック処理
- F. GP04のリンクの強制プロパティ

正解: C ([コメントを发表する](#))

The exam content for Group Policy processing stresses User Group Policy loopback processing for session hosts (RDS/AVD): "In environments like Remote Desktop Session Host (or Azure Virtual Desktop), enable loopback processing on the OU that contains the session host computers so that user settings from that GPO apply when users log on to those computers, regardless of the user's own OU." The requirement states:

"Apply GPO4 to the Azure Virtual Desktop session hosts. Ensure that Azure Virtual Desktop user sessions lock after being idle for 10 minutes. Users must be able to control the lockout time manually from their client computer." The idle-lock is a user configuration setting that must apply when users sign in to the session hosts, not to their personal devices. Therefore, enable loopback processing (Merge/Replace) in GPO4, which is linked to the VirtualDesktops OU containing the session hosts. Using security filtering or Enforced cannot make user settings in GPO4 override the user's own OU without loopback. Loopback ensures the AVD hosts impose the 10-minute lock for sessions, while leaving users free to set their own client device policies independently-fulfilling least-impact design.

質問: 75

Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory Domain Services (AD DS) ドメインがある Azure AD ハイブリッドに参加している Windows 10 デバイスがいくつかあります。

ユーザーがデバイスにサインインするときに、Windows Hello for Business を使用できるようにする必要があります。

Azure AD Connect でどのオプション機能を選択する必要がありますか？

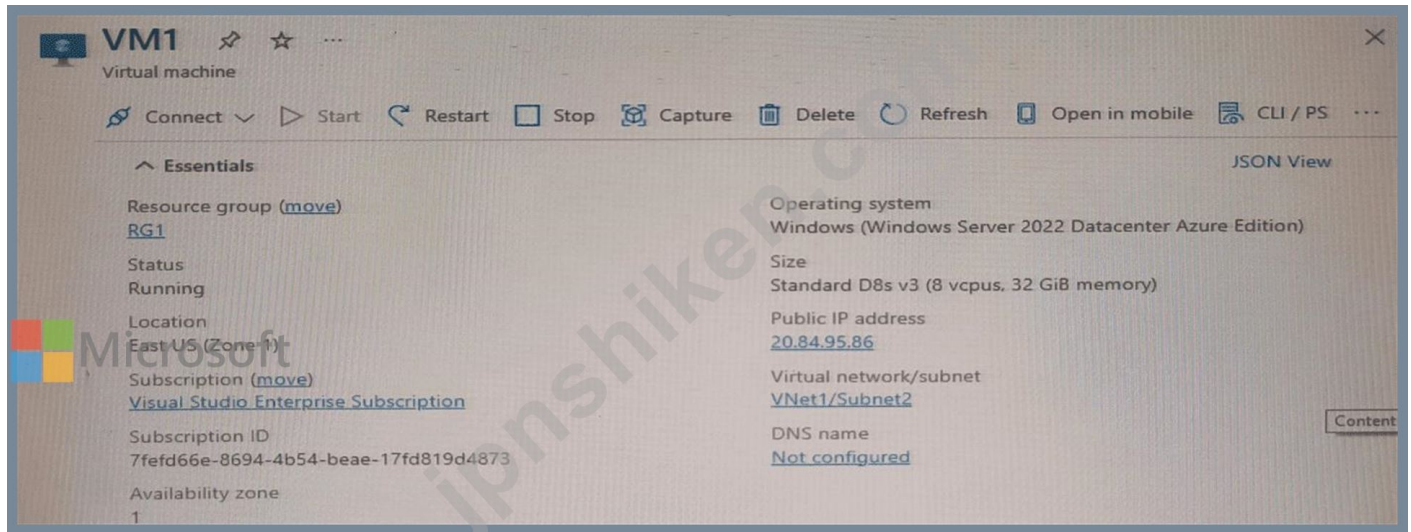
- A. デバイスの書き戻し
- B. グループの書き戻し
- C. パスワード ライトバック
- D. ディレクトリ拡張属性の同期
- E. Azure AD アプリと属性のフィルタリング

正解: ([正解を表示します](#))

The Windows Server Hybrid Core Infrastructure materials explain that Windows Hello for Business (WHfB) in a hybrid environment relies on Azure AD registration and corresponding device objects in on-premises AD DS. Azure AD Connect provides the Device writeback optional feature, which "writes Azure AD device objects back to AD DS as msDS-Device objects so on-premises domain controllers and policies can recognize and evaluate the device during authentication." The guide further notes that for hybrid-joined Windows 10/11 devices, enabling Device writeback "allows on-premises authentication stacks and Conditional Access decisions to use the registered device and its key material (key trust or certificate trust), enabling WHfB sign-in on domain-joined devices." Other options do not meet the requirement: Password writeback is used for self-service password reset, Group writeback returns Microsoft 365 groups to AD DS, and Directory extension attribute sync simply synchronizes custom attributes. Therefore, to ensure users can sign in with Windows Hello for Business on Azure AD hybrid-joined devices, select Device writeback in Azure AD Connect.

質問: 76

次の資料に示すように、VM1 という名前の仮想マシンを含む Azure サブスクリプションがあります。



サブスクリプションには、次の表に示すディスクがあります。

Name	Resource group	Location	Availability zone
Disk1	RG1	East US	None
Disk2	RG2	East US	1
Disk3	RG1	Central US	None
Disk4	RG1	Central US	1

データ ディスクとして VM1 に接続できるディスクはどれですか？

- A. ディスク 2 のみ
- B. Disk4のみ
- C. Disk1 と Disk2 のみ
- D. Disk2 と Disk4 のみ
- E. Disk1、Disk3、Disk4 のみ
- F. ディスク 1、ディスク 2、ディスク 3。とDisk4

正解: ([正解を表示します](#))

In Azure infrastructure management, attaching data disks to a virtual machine (VM) is governed by two primary constraints: Geographic Location and Availability Zone alignment. According to the official documentation for Administering Windows Server Hybrid Core Infrastructure, a data disk must reside in the same physical region as the virtual machine it is being attached to.

Reviewing the provided exhibits:

* VM1 Location: The VM essentials exhibit shows that VM1 is located in the East US region and specifically within Availability Zone 1.

* Disk Analysis:

* Disk1: Located in East US. Although its Availability Zone is set to "None" (meaning it is a regional/non-zonal managed disk), regional disks can be attached to zonal VMs within the same region.

* Disk2: Located in East US and specifically in Availability Zone 1. This is a perfect match for VM1, as it shares both the region and the specific zone.

* Disk3: Located in Central US. This disk cannot be attached because it is in a different geographical region than the VM.

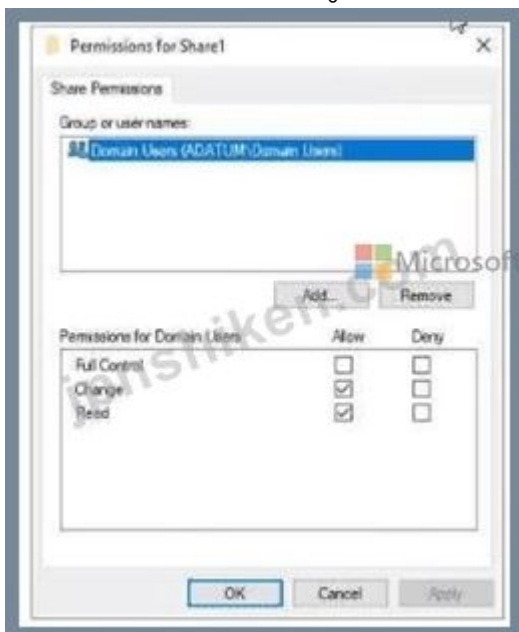
* Disk4: Located in Central US. Similar to Disk3, the regional mismatch prevents it from being attached to a VM in East US, regardless of its zonal configuration.

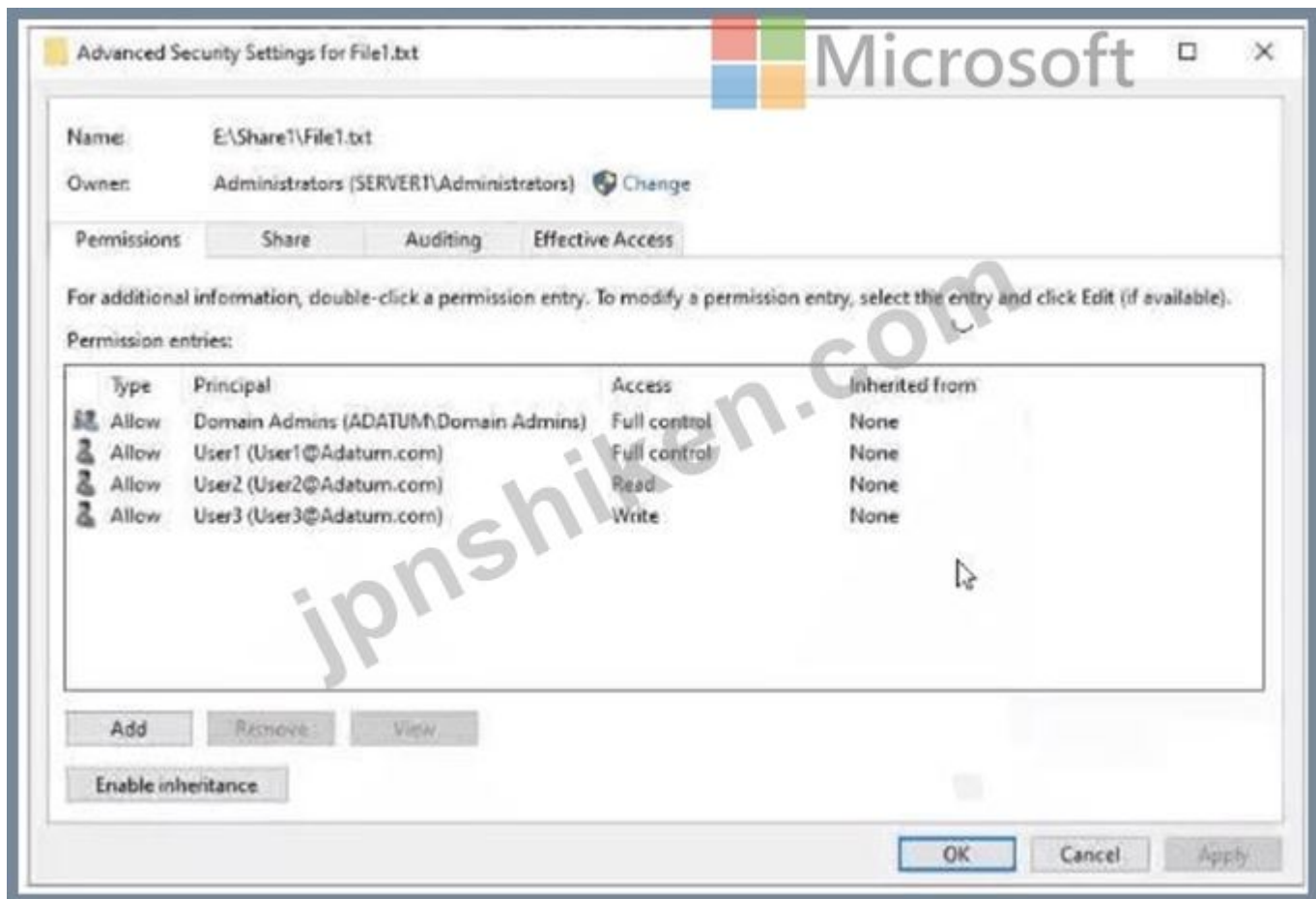
Therefore, only disks residing in the East US region (Disk1 and Disk2) are eligible to be attached as data disks to VM1. While a zonal VM can use a non-zonal disk (Disk1) in the same region, it cannot use disks from a different region (Disk3 and Disk4) or disks from a different availability zone within the same region (though in this case, Disk2 matches the zone).

有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/AZ-800J-mondaishu> **262問**、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 77

ネットワークには、adatum.com という名前の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。





ドメインには、Server1 という名前のサーバーと、User1、User2、User3 という名前の 3 人のユーザーが含まれています (Server1 には、次の構成を持つ Share1 という名前の共有フォルダーが含まれています)。

```

ShareState      : Online
AvailabilityType : NonClustered
FolderEnumerationMode : AccessBased
CachingMode     : Manual
LeasingMode     : Full
SmbInstance     : Default
CompressData    : False
ContinuouslyAvailable : False
EncryptData     : False
Name            : Share1
Path            : E:\Share1
ShadowCopy      : False
  
```

Share1 の共有権限は、「共有権限」の図に示されているとおりに設定されています。(「共有権限」タブをクリックしてください。)Share1 には File1.txt というファイルが含まれています。File1.txt の詳細なセキュリティ設定は、「ファイル権限」の図に示されているとおりに設定されています。(「ファイル権限」タブをクリックしてください。)以下の各文について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area		Microsoft	
Statements	Yes	No	
When User1 connects to \\Server1.adatum.com\Share1\, the user can take ownership of File1.txt.	☐	☐	
When User2 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☐	☐	
When User3 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☐	☐	

正解:

Answer Area

Statements	Yes	No
When User1 connects to \\Server1.adatum.com\Share1\, the user can take ownership of File1.txt.	☐	☒
When User2 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☒	☐
When User3 connects to \\Server1.adatum.com\Share1\, File1.txt is visible.	☐	☒

Explanation:

When User1 connects to \\Server1\Share1\, the user can take ownership of File1.txt. No When User2 connects to \\Server1\Share1\, File1.txt is visible. Yes When User3 connects to \\Server1\Share1\, File1.txt is visible. No In Windows file sharing, the effective permission over SMB is the most restrictive result of share and NTFS permissions. The study guides emphasize that "share permissions cap what NTFS can allow when access is via the share" and that Access-Based Enumeration (ABE) hides items that the user cannot read. In the exhibit, the share permission grants Domain Users = Change, Read (no Full Control). NTFS on File1.txt grants User1 = Full control, User2 = Read, User3 = Write.

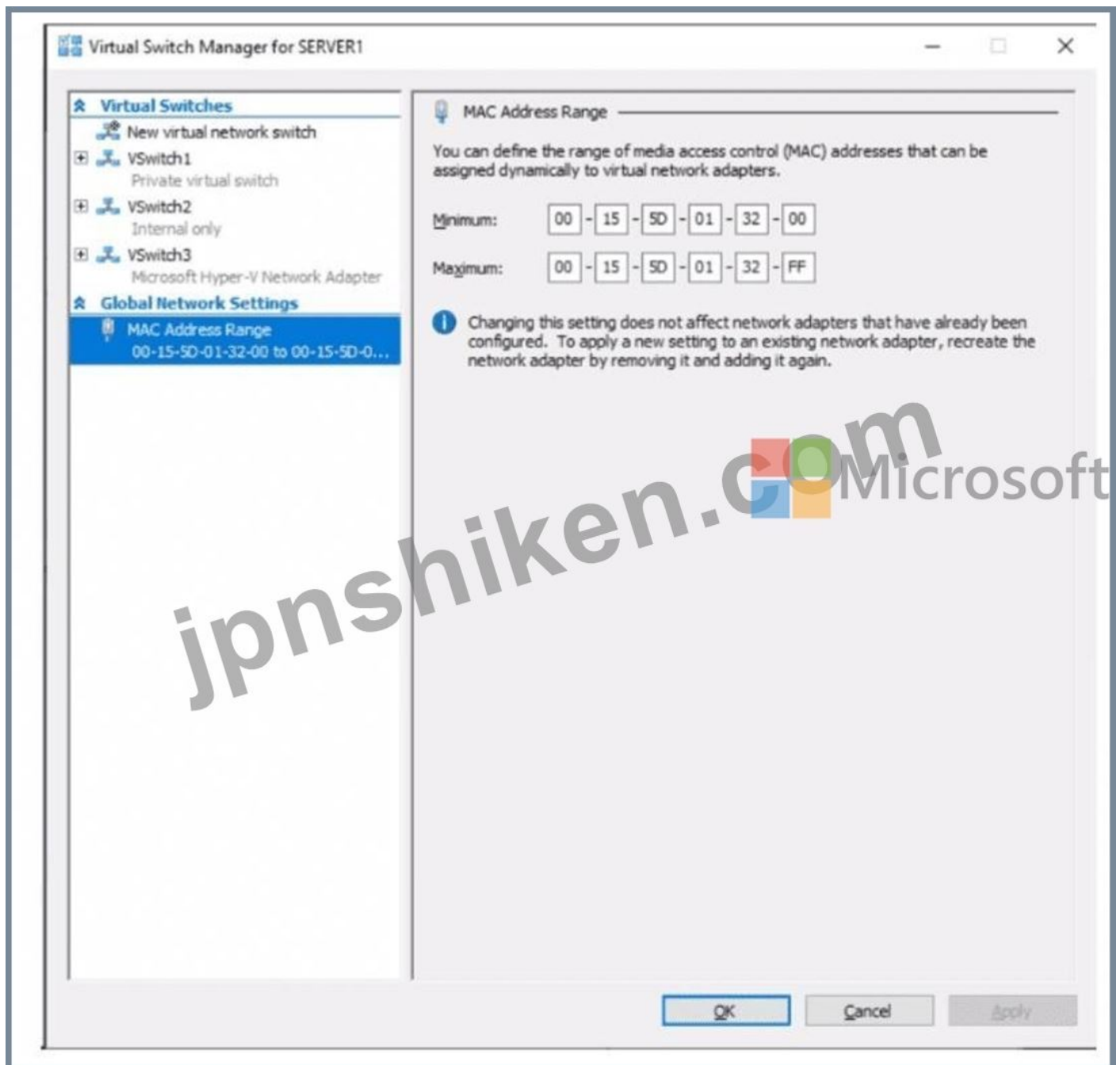
* User1: Although NTFS grants Full control (which includes Change permissions/Take ownership), the share grants only Change, which does not include taking ownership. Because share permissions limit SMB access, User1 cannot take ownership when connecting through \\Server1\Share1\.

* User2: Has Read on the file and the share allows Read; with ABE enabled on the share, items for which the user has at least read access remain visible. Therefore File1.txt is visible to User2.

* User3: Has Write (no Read) on the file; with ABE, objects without read permission are hidden during enumeration. Even though the share allows Change/Read in general, the absence of NTFS Read on the file means File1.txt will not be visible to User3.

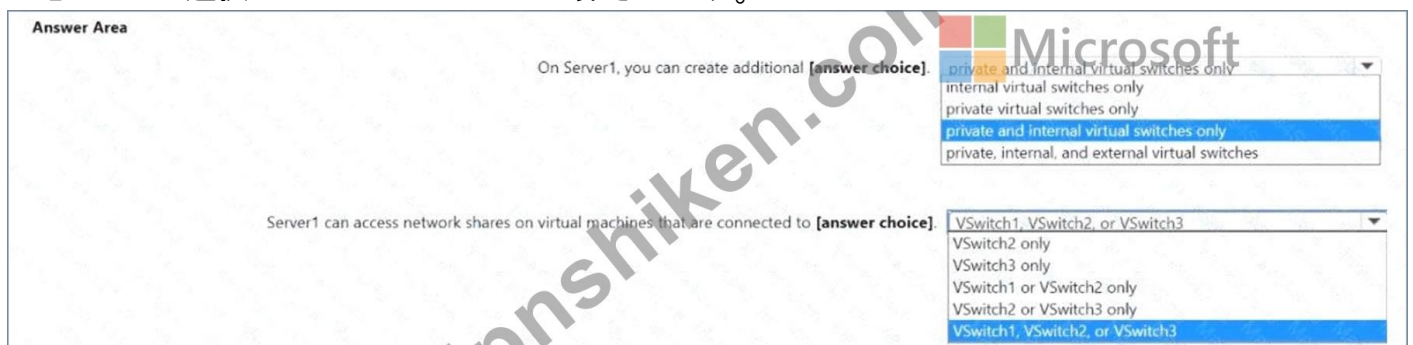
質問: 78

Windows Server を実行する Server1 というサーバーがあります。Server1 には、次の図に示す単一のネットワーク インターフェイスと Hyper-V 仮想スイッチがあります。



ドロップダウンメニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

Answer Area

On Server1, you can create additional [answer choice].

- private and internal virtual switches only
- internal virtual switches only
- private virtual switches only
- private and internal virtual switches only
- private, internal, and external virtual switches

Server1 can access network shares on virtual machines that are connected to [answer choice].

- VSwitch1, VSwitch2, or VSwitch3
- VSwitch2 only
- VSwitch3 only
- VSwitch1 or VSwitch2 only
- VSwitch2 or VSwitch3 only
- VSwitch1, VSwitch2, or VSwitch3

Explanation:

Answer Area

On Server1, you can create additional [answer choice].

- private and internal virtual switches only

Server1 can access network shares on virtual machines that are connected to [answer choice].

- VSwitch1, VSwitch2, or VSwitch3

The Hyper-V networking section of the Administering Windows Server Hybrid Core Infrastructure material explains that Hyper-V provides three virtual switch types: External, Internal, and Private. It states:

"An External switch is bound to a physical NIC and can optionally connect the management OS; an Internal switch connects VMs to each other and to the host only; a Private switch connects VMs to each other only (no host access)." The guide further clarifies limits on external switches: "A single physical adapter can be bound to only one External virtual switch at a time (unless using NIC Teaming). Additional External switches require additional physical adapters." In the exhibit, Server1 has a single NIC already bound to vSwitch3, and the tree shows 'Microsoft Hyper-V Network Adapter', indicating the management OS shares the adapter. Therefore, you cannot add another External switch with the lone NIC; you can still create Internal and Private switches. Regarding host connectivity, the guide specifies: "The management OS can communicate with VMs attached to an Internal switch and to an External switch (when the management OS is connected). The host cannot communicate with VMs on a Private switch." Consequently, Server1 can access network shares only from VMs on vSwitch2 (Internal) or vSwitch3 (External with management OS), but not from VMs on vSwitch1 (Private).

質問: 79

Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory Domain Services (AD DS) ドメインがあります。Windows Server を実行する 100 個の新しい Azure 仮想マシンをデプロイする予定です。新しい各仮想マシンが AD DS ドメインに参加していることを確認する必要があります。何をすべきですか？

- A. Azure AD Connect
- B. a Group Policy Object (GPO)
- C. an Azure Resource Manager (ARM) template
- D. an Azure management group

正解: C ([コメントを发表する](#))

Reference:

In Administering Windows Server Hybrid Core Infrastructure (AZ-800) guidance on deploying and managing Windows Server IaaS VMs, Microsoft emphasizes automating domain join during provisioning by using Azure VM extensions within an Azure Resource Manager (ARM) template. The supported method for joining Azure VMs to an on-premises AD DS domain is the `JsonADDomainExtension` (Microsoft.Compute/virtualMachines/extensions). In the ARM template, you provide parameters such as the AD DS domain name, `OUPath` (optional), `User` (a domain account with join rights), `Password` (as a secure parameter), `Restart` (true/false), and `Options`. When the VM is created, the extension executes on first boot and performs the classic AD DS domain join, ensuring every newly deployed VM is joined consistently and at scale.

By contrast, Azure AD Connect (A) only synchronizes identities between AD DS and Azure AD; it does not join Windows Server computers to AD DS. A GPO (B) can configure domain-joined computers after they are in the domain, but it cannot join non-domain systems. Azure management groups (D) provide governance and hierarchy for subscriptions and policies, not machine domain-join operations. Therefore, to ensure that 100 newly deployed Windows Server VMs are automatically joined to the on-premises AD DS domain during deployment, the verified and supported approach is to use an ARM template with the `JsonADDomainExtension`.

質問: 80

Windows Server 2022 を実行し、次の表に示すネットワーク アダプターを備えたサーバーがあります。

Name	Vendor	Interface	Link speed	Remote Direct Memory Access (RDMA) support
LAN1	Vendor1	Network Adapter #1	1 Gbps	No
LAN2	Vendor2	Network Adapter #2	25 Gbps	Yes
LAN3	Vendor3	Network Adapter #3	25 Gbps	Yes
LAN4	Vendor4	Network Adapter #4	10 Gbps	No

LAN2とLAN3のNICラーニングを設定する必要があります。ソリューションはDynamic Virtual Machine Multi-Queue (d.VMMQ)をサポートしている必要があります。

何をすべきでしょうか？

- A. 静的チームングモード
- B. スイッチ埋め込みチームング (SET)
- C. 負荷分散とフェイルオーバー (LBFO)
- D. LACPチームングモード

正解: [\(正解を表示します\)](#)

The networking section of the AZ-800 material specifies that Switch Embedded Teaming (SET) is the teaming technology for Hyper-V hosts introduced in Windows Server 2016 and enhanced in later versions.

The guide highlights that SET "integrates teaming into the Hyper-V virtual switch," and supports advanced offloads including RDMA, VMMQ/d.VMMQ, SR-IOV, and RSS when the NICs support

them. Conversely, the legacy LBFO (Load Balancing/Failover) teaming is described as "not supported with RDMA or VMMQ on Hyper-V hosts" and is deprecated for Hyper-V scenarios. Static or LACP teaming modes refer to LBFO team modes and thus inherit those limitations. Because LAN2 and LAN3 are 25-Gbps adapters that support RDMA and the requirement explicitly calls for NIC learning with Dynamic VMMQ, the prescribed and supported solution is to create a SET team using those two adapters and bind it to the Hyper-V switch. The documentation emphasizes that SET "enables RDMA with SMB Direct and Dynamic VMMQ on teamed NICs," meeting the performance and capability requirements.

質問: 81

次の表に示すように、Windows Server を実行するオンプレミス サーバーがあります。

Name	Type
Server1	Physical server
VM2	Hyper-V virtual machine

VMV という仮想マシンを含む Azure サブスクリプションがあります。Azure Arc を使用してすべてのサーバーを管理できるようにする必要があります。ソリューションでは、管理の労力を最小限に抑える必要があります。

Azure Connected Machine エージェントはどのサーバーにインストールすればよいですか？

- A. サーバー1のみ
- B. VM1のみ
- C. VM2のみ
- D. VM1とVM2のみ
- E. Server1とVM2のみ
- F. Server1、VM1、VM2

正解: **E** ([コメントを发表する](#))

Azure Arc-enabled servers use the Azure Connected Machine agent to onboard non-Azure machines (on- premises or other clouds) so they appear in Azure for inventory, policy, Update Management, Defender, etc.

The AZ-800 study guide emphasizes: "Install the Connected Machine agent on Windows or Linux servers that are outside of Azure. Native Azure VMs are already Azure resources and can be managed without Arc; onboarding Azure VMs to Arc is optional and not required for basic management." In the scenario, Server1 (a physical on-premises server) and VM2 (a Hyper-V VM on-premises) are non-Azure; both require the Connected Machine agent to be projected into Azure via Arc. VM1 is already an Azure VM and can be managed through Azure natively (Azure VM resource model, extensions, policies) without installing the Arc agent. Because the requirement is to manage all servers via Azure Arc while minimizing administrative effort, you install the agent only where it's needed-on Server1 and VM2. This provides Arc governance and management for on-prem systems without redundant configuration on the Azure VM.

質問: 82

Windows Server を実行するタイル サーバーが 5 台あります。

ファイルサーバーの共有フォルダへの.mov拡張子の動画ファイルのアップロードをブロックする必要があります。その他のファイル形式はすべて許可する必要があります。このソリューションは、管理作業を最小限に抑える必要があります。

何を創造すべきでしょうか？

- A. ダイナミックアクセス制御の集中アクセスポリシー
- B. ファイルスクリーン
- C. ダイナミックアクセス制御の中央アクセスルール
- D. データ損失防止 (DLP) ポリシー

正解: ([正解を表示します](#))

In the Administering Windows Server Hybrid Core Infrastructure materials for file services, Microsoft emphasizes using File Server Resource Manager (FSRM) to control which file types users can store on shares.

FSRM provides File Screening Management that "controls the types of files that users can save" on a path by matching file groups (extensions) and applying either active screening (block) or passive screening (allow but report). The guides further note that you can "create file screen templates to standardize settings and apply them to multiple folders or servers," minimizing repeated administration across many file servers.

To meet the requirement "block users from uploading video files that have the .mov extension... All other types of files must be allowed," you create a File Screen with Active screening on the shared folders (or their parent paths) using a File Group that contains *.mov. This directly prevents writes of the specified extension while permitting other files.

By contrast, Dynamic Access Control (DAC) central access policies/rules govern authorization based on claims and resource properties, not file extensions. A DLP policy targets Microsoft 365 workloads and sensitive information types rather than enforcing extension-based blocking on Windows Server SMB shares.

Therefore, the least-effort and purpose-built solution is an FSRM file screen.

質問: 83

タスク8192.168.2.0 ~ 192.168.2.255 の IP アドレス範囲に関連付けられた、Site2 という名前の Active Directory ドメイン サービス (AD DS) サイトを作成する必要があります

。

正解:

See the solution of this Task below.

Explanation:

To create an AD DS site named Site2 that is associated to an IP address range of 192.168.2.0 to 192.168.2.255, you can follow these steps:

On a domain controller or a computer that has the Remote Server Administration Tools (RSAT) installed, open Active Directory Sites and Services from the Administrative Tools menu or by typing dssite.msc in the Run box.

In the left pane, right-click on Sites and select New Site.

In the New Object - Site dialog box, enter Site2 as the Name of the new site. Select a site link to associate the new site with, such as DEFAULTIPSITELINK, and click OK. You can also create a new site link if you want to customize the replication frequency and schedule between the sites. For more information on how to create a site link, see Create a Site Link.

In the left pane, right-click on Subnets and select New Subnet.

In the New Object - Subnet dialog box, enter 192.168.2.0/24 as the Prefix of the subnet. This notation represents the IP address range of 192.168.2.0 to 192.168.2.255 with a subnet mask of 255.255.255.0.

Select Site2 as the Site object to associate the subnet with, and click OK.

Wait for the changes to replicate to other domain controllers. You can verify the site and subnet creation by checking the Sites and Subnets containers in Active Directory Sites and Services.

Now, you have created an AD DS site named Site2 that is associated to an IP address range of 192.168.2.0 to

192.168.2.255. You can add domain controllers to the new site and configure the site links and site link bridges to optimize the replication topology.

質問: 84

Windows Server を実行し、Active Directory フェデレーション サービスの役割がインストールされている Server1 という名前のサーバーがあります。

Server2 という名前のサーバーに Web アプリケーション プロキシを展開する予定です。

Server1 から Active Directory フェデレーション サービス (AD FS) 証明書をエクスポートします。

Server2 でどのアクションを順番に実行する必要がありますか？ 適切なアクションを正しい順序にドラッグして教えてください。各アクションは 1 回だけ、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要があります。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Actions

- Install the Remote Access role.
- Install the Active Directory Federation Services role.
- Run the Web Application Proxy Configuration Wizard.
- Install Microsoft Application Request Routing (ARR) for IIS.
- Run the Active Directory Federation Services Configuration Wizard.

Answer Area

Step 1:

Step 2: Import the AD FS certificate to Server2.

Step 3:

Microsoft

正解:

Actions

- Install the Remote Access role.
- Install the Active Directory Federation Services role.
- Run the Web Application Proxy Configuration Wizard.
- Install Microsoft Application Request Routing (ARR) for IIS.
- Run the Active Directory Federation Services Configuration Wizard.

Answer Area

Step 1: Install the Remote Access role.

Step 2: Import the AD FS certificate to Server2.

Step 3: Run the Web Application Proxy Configuration Wizard.

Microsoft

Explanation:

<Step 1: Install the Remote Access role.

Step 2: Import the AD FS certificate to Server2.

Step 3: Run the Web Application Proxy Configuration Wizard.

In Administering Windows Server Hybrid Core Infrastructure, the Web Application Proxy (WAP) component is documented as a role service of the Remote Access role and is deployed on an edge or perimeter server to publish AD FS and other web apps. The guide states that before configuring WAP, you must install the Remote Access role with the Web Application Proxy role service on the proxy server. It further explains that WAP must establish trust with the existing AD FS farm by using the AD FS service communications certificate: "Import the federation service SSL certificate (with private key) on the proxy server and place it in the local computer's personal store." After the certificate is present, you run the Web Application Proxy Configuration Wizard to "specify the Federation Service name, provide AD FS credentials, and complete the trust and configuration." The materials also clarify that you do not install the AD FS role on the proxy and Microsoft Application Request Routing (ARR) is not required for WAP. The AD FS Configuration Wizard applies to federation servers, not proxies. Therefore, the minimal and correct sequence on Server2 is: Install Remote Access (WAP) # Import the AD FS cert # Run the Web Application Proxy Configuration Wizard, which configures the trust and enables publishing of the AD FS endpoint.

質問: 85

DC1 が失敗します。

スキーマ マスターの技術要件を満たす必要があります。

ntdsutil.exe を実行します。

どの 5 つのコマンドを順番に実行する必要がありますか? 回答するには、コマンドのリストから適切なコマンドを回答領域に移動し、正しい順序に並べます。

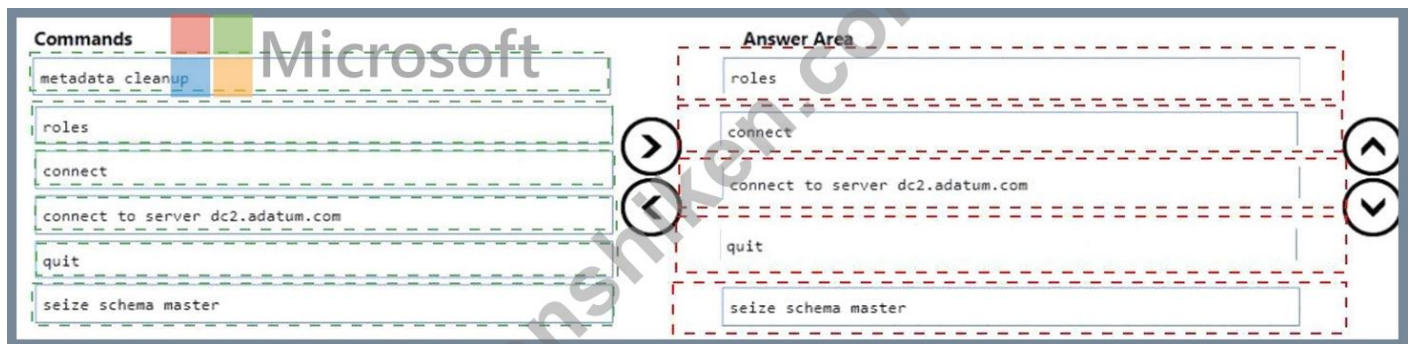
Commands

metadata cleanup
roles
connect
connect to server dc2.adatum.com
quit
seize schema master

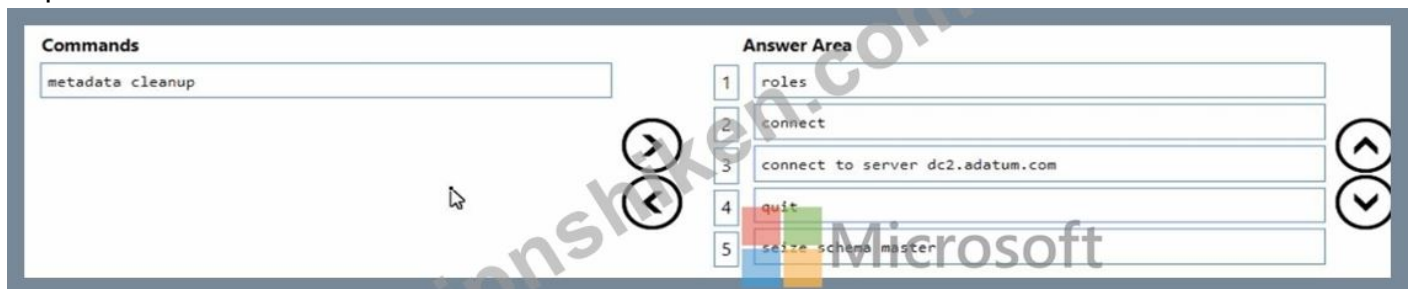
Answer Area



正解:



Explanation:



質問: 86

ネットワークにはオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。このドメインには、User1 というユーザーと、次の表に示すサーバーが含まれています。

Name	Operating system
Server1	Windows Server 2016
Server2	Windows Server 2022
Backup1	Windows Server 2019

User1 は、Protected Users セキュリティ グループのメンバーです。

ユーザー1は次のアクションを実行します。

* Server1からServer2にリモートPowerShellセッションを確立します

* Server2 の PowerShell セッションから、Backup1 上のリソースにアクセスしようとし
ます。Backup1 上のリソースへのアクセス要求は拒否されます。

User1 が Server2 の PowerShell セッションを使用して Backup1 のリソースにアクセスできるようにする必要があります。このソリューションは、最小権限の原則に従い、管理作業を最小限に抑える必要があります。

何を設定すればよいでしょうか？

- A. Kerberos 委任 (制約なし)
- B. クレドSSP
- C. RunAs を使用した PSSessionConfiguration
- D. リソースベースのKerberos制約委任

正解: D ([コメントを发表する](#))

In Windows remoting, hopping from one server to another (Server1 # Server2 # Backup1) triggers the

"second-hop" problem because the user's TGT is not forwarded. The AZ-800 material explains that members of Protected Users cannot use NTLM, DES/RC4, or unconstrained delegation, and their credentials cannot be cached or delegated. Therefore, CredSSP or unconstrained delegation cannot be used. The guide prescribes Kerberos constrained delegation to allow a middle-tier server to act on the user's behalf, and specifically recommends resource-based constrained delegation (RBCD) because it is configured on the resource (Backup1) by setting msDS-AllowedToActOnBehalfOfOtherIdentity to allow the front-end computer account (Server2\$) to delegate to the service SPN on the resource. This model follows least privilege, avoids broad domain-wide delegation, works with Protected Users, and requires minimal administration because you touch only the destination resource. In short: configure RBCD on Backup1 to permit Server2 to obtain S4U2Proxy tickets to the share service, enabling User1's PowerShell session on Server2 to access Backup1 while remaining compliant with Protected Users restrictions and Kerberos-only authentication.

質問: 87

Windows Server を実行できる Azure 仮想マシンをデプロイする計画です。この仮想マシンは、Active Directory ドメイン サービス (AD DS) ドメイン コントローラーと、新しい仮想ディスク上の f: というドライブをホストします。

仮想マシンのストレージを構成する必要があります。ソリューションは以下の要件を満たす必要があります。

- * AD DS の回復力を最大化します。
- * 偶発的なデータ損失を防ぎます。

ストレージをどのように構成すればよいですか？ 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Microsoft

Volume for the AD DS database:

C
D
F

Caching configuration for the volume that hosts the database:

NONE
READ
READ/WRITE

正解:

Answer Area

Microsoft

Volume for the AD DS database:

C
D
F

Caching configuration for the volume that hosts the database:

NONE
READ
READ/WRITE

Explanation:

Volume for the AD DS database: F

Caching configuration for the volume that hosts the database: NONE

The Administering Windows Server Hybrid Core Infrastructure guidance for deploying AD DS on Azure IaaS VMs is explicit about storage placement and disk caching. The study materials state that you must not use the temporary disk and should place the AD DS database and logs on a persistent data disk:

"Do not place the Active Directory database, logs, or SYSVOL on the temporary disk (typically D: in Azure).

Data on the temporary disk is not persistent and can be lost at any time." They also direct disabling host caching on the disk that holds the AD DS database and logs to maximize resiliency and avoid write-caching data loss:

"For disks that store NTDS.dit and the AD DS log files, configure Host caching = None to prevent stale or unflushed writes and to ensure directory integrity during failures." And, for drive layout:

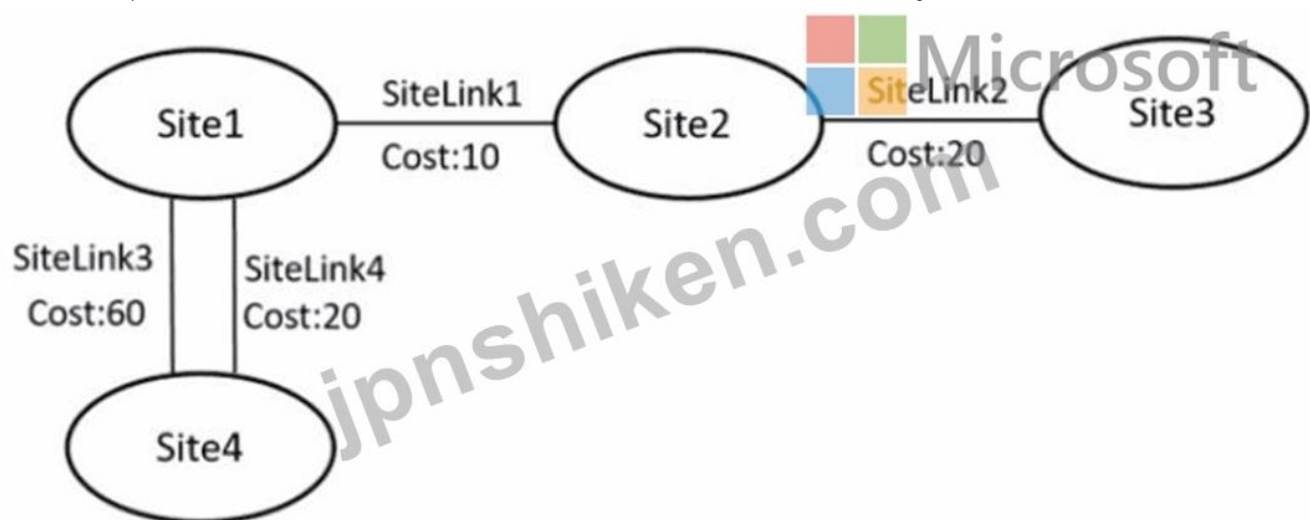
"Install the operating system on C: and create a separate data disk/volume for AD DS database and logs to improve reliability and recoverability." Applying these verified practices:

- * Selecting F: (the new persistent data disk) meets the requirement to avoid the non-persistent D: drive and to separate AD DS from the OS volume (C:).

- * Setting host caching to NONE on that disk maximizes resiliency and prevents accidental data loss by disabling volatile write caching for critical AD DS data.

質問: 88

ネットワークにはActive Directoryドメインサービス(AD DS)フォレストが含まれています。フォレストには、次の図に示すサイトとサイトリンクが含まれています。



サイトには、次の表に示すブリッジヘッドドメインコントローラーが含まれています。

Name	Site
DC1	Site1
DC2	Site2
DC3	Site3
DC4	Site4

IP サイト間トランスポート コンテナーは、次の図に示すように構成されます。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Statements	Yes	No
DC1 can replicate directly to DC3.	☐	☐
DC1 will load balance replication traffic to DC4 via SiteLink3 and SiteLink4.	☐	☐
To ensure that replication between DC4 and DC2 is routed via DC1, the configuration of the IP intersite transport container must be modified.	☐	☐

正解:

Answer Area

Statements	Yes	No
DC1 can replicate directly to DC3.	☒	☐
DC1 will load balance replication traffic to DC4 via SiteLink3 and SiteLink4.	☐	☒
To ensure that replication between DC4 and DC2 is routed via DC1, the configuration of the IP intersite transport container must be modified.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
DC1 can replicate directly to DC3.	☒	☐
DC1 will load balance replication traffic to DC4 via SiteLink3 and SiteLink4.	☐	☒
To ensure that replication between DC4 and DC2 is routed via DC1, the configuration of the IP intersite transport container must be modified.	☒	☐

質問: 89

ネットワークに Active Directory Domain Services (AD DS) ドメインが含まれている - ドメインには、Windows Server を実行する 10 台のサーバーが含まれています。サーバーには静的 IP アドレスがあります。

DHCP を使用して IP アドレスをサーバーに割り当てる予定です。

各サーバーが常に同じ IP アドレスを受け取るようにする必要があります。

各サーバーの DHCP 予約を作成するには、どの種類の識別子を使用する必要がありますか？

- A. ユニバーサル意識別子 (UUID)
- B. 完全修飾ドメイン名 (FQDN)
- C. NetBIOS名
- D. MAC アドレス

正解: **D** ([コメントを發表する](#))

Reference:

In the Administering Windows Server Hybrid Core Infrastructure materials for DHCP, reservations are defined as mappings that "bind a specific hardware (MAC) address to a single, permanent IPv4 address from a scope." The guide emphasizes that DHCP reservations ensure devices-such as servers using DHCP rather than static addressing-"always receive the same address whenever they request a lease," and that the required inputs when creating a reservation are the IP address, MAC address (also called hardware address), and a descriptive name. The exam prep further notes that while DHCPv4 supports an optional "Client Identifier," Windows Server hosts typically use the MAC address by default unless explicitly configured otherwise. Because your 10 Windows Server machines currently use static IPs and you want DHCP to always assign them the same IP, the correct identifier for each reservation is the MAC address. FQDNs and NetBIOS names are not valid unique identifiers for DHCP reservations, and UUIDs are unrelated to DHCP addressing.

Therefore, selecting MAC address meets the reservation requirement and aligns with the documented DHCP best practices in the hybrid core infrastructure objectives.

質問: **90**

Windows Server を実行する Server1 という名前のサーバーがあります。

Windows コンテナでアプリケーションをホストする予定です。

コンテナを実行するには Server1 を構成する必要があります。何をインストールすればよいですか？

- A. Windows 管理センター
- B. Linux用Windowsサブシステム
- C. ドクター
- D. ハイパーV

正解: **C** ([コメントを發表する](#))

In the Windows Server hybrid curriculum for AZ-800, running Windows containers on a Windows Server host requires enabling the Containers feature and installing a container runtime, specifically the Docker (Moby) engine. The guide explains that Windows Server supports two isolation modes-process and Hyper- V isolation-but in both cases you still need a Docker-compatible runtime to pull images, create, and manage containers. The materials emphasize: container functionality isn't provided by Windows Admin Center or WSL; Admin Center is only a management tool and WSL targets Linux user-space scenarios, not Windows container runtime

services. Likewise, the Hyper-V role is optional and only needed if you choose Hyper-V isolation for containers; it is not, by itself, sufficient to run containers. Therefore, the required installation to "configure Server1 to run containers" is the Docker engine (often referred to in Microsoft's docs as Docker

/Moby), after which you can pull Windows base images and run Windows containers on the host. This aligns with the prescribed steps: enable Containers feature # install Docker # configure isolation as needed # deploy containerized apps.

質問: 91

User1 の技術要件を満たす必要があります。ソリューションでは、最小権限の原則を適用する必要があります。

何をすべきでしょうか？

- A. contoso.com の Server Operators グループに Users1 を追加します。
- B. contoso.com に委任を作成します。
- C. contoso.com の Account Operators グループに Users1 を追加します。
- D. OU3 に委任を作成します。

正解: ([正解を表示します](#))

In the Administering Windows Server Hybrid Core Infrastructure guidance for managing AD DS, Microsoft emphasizes using OU-level delegation to satisfy administrative needs while adhering to the principle of least privilege. The documentation explains that the Delegate Control wizard on an OU lets you grant a user or group only the specific permissions required for common tasks, including "Modify the membership of a group". This grants the write permission to the member attribute on group objects contained in that OU, without giving broader account-management rights across the domain.

By contrast, placing a user in Account Operators or Server Operators provides elevated, domain-wide capabilities far beyond what is required. Account Operators can create, delete, and modify many account types across the domain (except for protected admin accounts), which violates least-privilege for a task that only needs to change group membership in one OU. Server Operators is unrelated to group membership and is intended for server administration tasks. Creating a delegation at the domain root would similarly be excessive because it applies broadly to all containers and OUs.

Therefore, to meet the requirement "Ensure that User1 can manage the membership of all the groups in Contoso\OU3," you should delegate control on OU3 and assign the built-in task "Modify the membership of a group" to User1, achieving the minimal permissions necessary.

有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版の

質問: 92

単一のディスクを持つ Server1 という名前の Windows Server コンテナ ホストがあります。Server1 では、次の表に示すコンテナを起動する予定です。

Name	Description
Container1	Container1 is a Windows container that contains a web app in development. The container must NOT share a kernel with other containers.
Container2	Container2 is a Linux container that runs a web app. The container requires two static IP addresses.
Container3	Container3 is a Windows container that runs a database. The container requires a static IP address.

各コンテナに使用できる分離モードはどれですか？ 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Container1:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container2:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container3:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

正解:

Container1:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container2:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Container3:

Hyper-V isolation only
Process isolation only
Hyper-V isolation or process isolation

Explanation:

Container1:	
	Hyper-V isolation only
	Process isolation only
	Hyper-V isolation or process isolation
Container2:	
	Hyper-V isolation only
	Process isolation only
	Hyper-V isolation or process isolation
Container3:	
	Hyper-V isolation only
	Process isolation only
	Hyper-V isolation or process isolation

The Administering Windows Server Hybrid Core Infrastructure guidance explains two Windows container isolation modes: process isolation (Windows Server containers) and Hyper-V isolation. With process isolation, containers share the host's kernel, so they run as ordinary processes on the host. With Hyper-V isolation, each container runs inside a lightweight VM with its own kernel; this provides a hard isolation boundary and prevents kernel sharing with other containers. The curriculum further notes that Linux containers on Windows require Hyper-V isolation because they cannot share the Windows kernel.

Applying these rules:

- * Container1 "must NOT share a kernel with other containers." The only mode that prevents kernel sharing is Hyper-V isolation, so Container1 must use Hyper-V isolation.
- * Container2 is a Linux container. On a Windows Server container host, Linux containers are run via a utility VM and therefore require Hyper-V isolation.
- * Container3 is a Windows container that needs a static IP address. The networking modules describe that Windows containers can obtain static IPs when you use supported networks (for example, I2bridge /transparent) regardless of isolation mode; therefore a Windows workload like a database can run in either process or Hyper-V isolation, depending on the isolation/security you want.

Thus, the correct selections are: Hyper-V isolation only for Container1 and Container2, and Hyper-V isolation or process isolation for Container3.

質問: 93

Windows Server を実行する Server1 と Server2 という 2 つのオンプレミス サーバーがあります。

storage1 という名前の Azure ストレージ アカウントがあり、このアカウントには share1 という名前のファイル共有が含まれています。Server1 は、Azure File Sync を使用して share1 と同期します。share1 と同期するように Server2 を構成する必要があります。

順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



In the Administering Windows Server Hybrid Core Infrastructure guidance for Azure File Sync, the workflow to onboard an additional Windows Server to an existing sync topology is explicit. Once a Storage Sync Service, sync group, and cloud endpoint (the Azure file share) already exist and are syncing with another server (Server1 in this case), you only need to prepare and join the new server (Server2) to that configuration.

The documented sequence is: (1) install the Azure File Sync agent on the Windows Server you want to add; (2) use the agent to register the server with the correct Storage Sync Service resource; and (3) in the existing sync group, add a server endpoint that points to the local path on

the newly registered server. The materials emphasize that creating a new Storage Sync Service or adding another cloud endpoint is unnecessary when the Azure file share is already in the sync group. The "server endpoint" binds the on-premises path to the already defined cloud endpoint in the sync group, enabling bi-directional sync. Therefore, the correct order is:
Install agent on Server2 # Register Server2 with the Storage Sync Service # Add a server endpoint to the sync group.

質問: 94

タスク2

シアトルのサイトで DC3 という名前のドメイン コントローラーを昇格する予定です。
DC3 が午後 8 時から午前 6 時の間だけ DC1 および DC2 と複製されるようにする必要があります。

正解:

See the solution of this Task below.

Explanation:

TASK 2

Objective: Configure DC3 to replicate with DC1 and DC2 only between 8:00 PM and 6:00 AM.

Step-by-Step Guide: Replication Scheduling for DC3

Step 1: Promote DC3 to a Domain Controller (if not already done)

Use Server Manager or PowerShell to install the Active Directory Domain Services role and promote the server as a domain controller.

Example PowerShell command to install the AD DS role:

powershell

Copy

Install-WindowsFeature AD-Domain-Services

To promote:

powershell

Copy

Install-ADDSDomainController -DomainName "contoso.com"

Step 2: Open Active Directory Sites and Services

Log in to DC3 or another DC with administrative tools.

Open Active Directory Sites and Services (dssite.msc).

Step 3: Locate the Site

In the left pane, expand the Sites container and find the site that contains DC3.

Expand the site to find Servers.

Under Servers, select DC3.

Step 4: Configure Replication Connection Objects

Expand DC3 and click on NTDS Settings.

In the right pane, you'll see connection objects to other domain controllers (these represent replication partners).

Step 5: Adjust the Replication Schedule for Each Connection

For each connection object to DC1 and DC2:

Right-click the connection object and select Properties.

Click the Change Schedule button.

Step 6: Set the Replication Schedule

In the schedule window, you'll see a grid of hours.

Clear all hours except the time window of 8 PM to 6 AM (in 1-hour blocks).

Select 8 PM to 6 AM (10 hours total) for all days.

Click OK to save.

Step 7: Verify and Document

Ensure that both connection objects (to DC1 and DC2) have the updated schedule.

Document your configuration as part of your environment's change control.

質問: 95

Windows Server を実行し、UserData という名前の共有フォルダーを含むサーバーがあります。

各ユーザーが UserData で消費できるストレージ容量を制限する必要があります。

何を使うべきですか？

A. 収納スペース

B. 作業フォルダー

C. 分散ファイル システム (DFS) 名前空間

D. ファイル サーバー リソース マネージャー (FSRM)

正解: D ([コメントを發表する](#))

In the Administering Windows Server Hybrid Core Infrastructure materials for file services, Microsoft specifies that FSRM is the component designed to enforce space usage limits on shared data: "File Server Resource Manager provides quota management, file screening, and storage reports. You can assign quotas to volumes or specific folders and use templates to standardize limits and notifications." The guide further notes that you can "configure hard or soft quotas per folder, generate warning e-mails or events as thresholds are reached, and apply automatic quota templates for user home directories." Because your requirement is to limit the amount of storage space that each user can consume in the UserData share, the supported and least-privilege approach is to apply an FSRM quota on the UserData folder (or on each user's home subfolder via auto-apply templates). Other options listed do not meet the goal: Storage Spaces manages physical capacity and resiliency, not per-user limits; Work Folders synchronizes user data but does not enforce quotas on a share; DFS Namespaces provides a unified namespace and referrals, not storage consumption control.

Therefore, FSRM is the correct tool to enforce per-user or per-folder storage limits on UserData.

質問: 96

Windows Server を実行する Server1 という名前のオンプレミス サーバーがあります。

VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。

Azure ネットワーク アダプターを使用して、Server1 を VNet1 に接続する必要があります。

何を使うべきでしょうか？

- A. Azure AD コネクト
- B. デバイス マネージャー
- C. Azureポータル
- D. Windows 管理センター

正解: **D** ([コメントを发表する](#))

The Administering Windows Server Hybrid Core Infrastructure study guides describe Azure Network Adapter (ANA) as "a Windows Admin Center (WAC) workflow that creates a point-to-site VPN from an on-premises Windows Server to an Azure virtual network." The guidance emphasizes: "ANA is initiated and configured exclusively from Windows Admin Center; it automates creation of the Azure VPN gateway side and the client configuration on the server." The Azure portal does not expose an "ANA" button for a standalone server, Device Manager has no role, and Azure AD Connect is for directory synchronization, not networking. The steps include registering WAC with Azure, selecting Add > Azure Network Adapter on the target server, choosing the subscription/resource group/VNet (e.g., VNet1), and letting WAC provision the P2S configuration and Windows VPN client profile. Therefore, to connect Server1 to VNet1 using Azure Network Adapter, you must use Windows Admin Center.

質問: 97

注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす独自の解決策が含まれています。質問セットによっては、正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。

このセクションで質問に答えた後は、そのセクションに戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。

Windows Server 2022 を実行し、DHCP サーバーの役割を持つ Server1 という名前のサーバーがあります。Server1 には、Scope1 という名前の単一の DHCP スコープが含まれています。

5 台のプリンターをネットワークに展開します。

プリンタに常に同じ IP アドレスが割り当てられていることを確認する必要があります。

解決策: Scope1 の DHCP スコープ オプションを構成します。

これは要件を満たしていますか？

- A. はい
- B. いいえ

正解: ([正解を表示します](#))

In Windows Server DHCP, scope options define configuration parameters (for example, default gateway, DNS servers, DNS domain suffix, WINS/NBNS) that are handed to clients as part of a lease, but they do not determine which IP address a client receives. The AZ-800/"Administering Windows Server Hybrid Core Infrastructure" content explains that DHCP scope options are used to "provide TCP/IP configuration values (router, DNS, and other option fields) to clients in a scope," whereas address assignment control is handled by the lease process and reservations. The guide stresses that if you must ensure a device "always obtains the same IPv4 address from

DHCP," you must "create a reservation that binds a client identifier (usually the MAC address) to a specific IP in the scope." Therefore, simply configuring or changing Scope1's scope options will not pin the printers to fixed addresses; the printers will continue to draw any free address from the scope's pool. Because the requirement is to always assign the same IPs, scope options alone cannot meet the goal; reservations are required for deterministic address assignment.

質問: 98

分散型クラスター展開を使用しています。この展開には、Windows Server を実行するスケールアウト ファイル サーバー (SOFS) クラスターと、Hyper-V ロールが有効になっているコンピューティング クラスターが含まれています。

ストレージのサービス品質(QoS)を実装する必要があります。ソリューションでは、SOFSクラスターとHyper-Vクラスター間の帯域幅使用量を制御する必要があります。

各クラスターでどのコマンドレットを実行する必要がありますか? 答えを得るには、適切なコマンドレットを正しいクラスターにドラッグします。

各コマンドレットは、1回、複数回、またはまったく使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:



In a disaggregated deployment (separate Hyper-V compute cluster and Scale-Out File Server storage cluster), Storage Quality of Service (Storage QoS) is implemented with centralized policies that are defined on the SOFS and applied to VM virtual disks from the Hyper-V side. The Administering Windows Server Hybrid Core Infrastructure materials describe centralized Storage QoS as follows: "In a SOFS-based deployment, you create Storage QoS policies on the Scale-Out File Server. Policies define minimum and maximum IOPS

/throughput and are stored on the cluster so they can be referenced by any VM using CSV shares exposed by the SOFS." The guide further states: "To apply a Storage QoS policy to a virtual hard disk, use the Hyper-V cmdlet to set the VHD attachment and reference the policy by name or ID. The policy then governs I/O for that disk regardless of which Hyper-V host the VM runs on." Accordingly, on the SOFS cluster, you run New-StorageQosPolicy to create the centralized policy (for example, with MinimumIops, MaximumIops, or bandwidth constraints). On the Hyper-V cluster, you attach or update the VM disk to consume that policy using Set-VMHardDiskDrive (for example, -QoSPolicyID or -QoSPolicyName). The Set-VMStorage cmdlet pertains to Hyper-V Virtual SAN configuration and is not used for Storage QoS. This pattern ensures you can control and cap bandwidth usage between the SOFS storage and the Hyper-V compute clusters while maintaining consistent, cluster-wide enforcement.

質問: 99

Windows Server を実行する VM1 という Azure 仮想マシンがあります。VM1 で以下の操作を実行します。

- * ボリュームCにFolder1という名前のフォルダを作成します
- * ボリューム D に Folder2 という名前のフォルダーを作成します。
- * VM1 に新しいデータ ディスクを追加し、ドライブ文字 E が割り当てられた新しいボリュームを作成します。
- * ボリューム E に App1 という名前のアプリをインストールします。

VM1 のサイズを変更する予定です。

VM1 のサイズを変更すると、どのオブジェクトが表示されますか？

- A. Folder1 と Folder2 のみ
- B. フォルダ1、ボリュームE、およびApp1のみ
- C. フォルダ1のみ
- D. 折りたたまれました。フォルダ2、アプリ1、ボリュームE

正解: ([正解を表示します](#))

In the Windows Server hybrid IaaS guidance for AZ-800 (Administering Windows Server Hybrid Core Infrastructure), resizing an Azure VM changes compute characteristics only (vCPU/memory/size family). The learning path on managing Windows Server IaaS VMs states that the VM's OS and any attached data disks persist across stop/deallocate and resize operations, and that drive letters and file data remain intact once the VM starts again.

Applications installed on those persistent disks continue to function because the underlying VHDs are unchanged. The only disk that may be transient is the temporary (ephemeral) OS cache or D: temporary disk provided by some sizes; however, managed OS disk (C:) and any managed data disks (such as D: and the newly added E:) retain their contents. Consequently, the folders created on C: and D: remain, the additional data disk that was initialized as volume E remains attached with the same drive letter, and App1 installed on E: is still present after the resize. Therefore, after resizing VM1 you will still have Folder1, Folder2, volume E, and App1, making option D correct.

質問: 100

Windows Server を実行する Server1 というサーバーがあります。Server1 には、次の表に示す記憶域プールがあります。

Name	Number of 7,200-RPM HDDs	Number of 10,000-RPM HDDs	Number of SSDs
Pool1	4	4	None
Pool2	None	2	2
Pool3	8	None	4

ストレージ階層を使用する VDisk1 という仮想ディスクを作成する予定です。VDisk1 の作成に使用できるプールはどれですか？

- A. プール2とプール3のみ
- B. プール2のみ
- C. プールのみ
- D. プール、プール2、プール3
- E. プール1とプール2のみ
- F. プール1とプール3のみ
- G. プール3のみ

正解: A ([コメントを發表する](#))

In the Administering Windows Server Hybrid Core Infrastructure (AZ-800) study domain for Storage Spaces, Microsoft specifies that storage tiers are created within a single storage pool that contains two classes of media: a fast tier (typically SSD) and a standard/capacity tier (HDD). The guide states that storage tiers "use SSDs for frequently accessed ('hot') data and HDDs for less frequently accessed ('cold') data within the same storage pool," and that tiering is available only when the pool includes both SSD and HDD devices. It further clarifies that different HDD spindle speeds (e.g., 7,200 vs 10,000 RPM) do not constitute different media types for tiering—they are all HDDs.

Applying these rules to the table:

- * Pool1 contains only HDDs (7,200-RPM and 10,000-RPM) and no SSDs, so it cannot host a tiered virtual disk.
- * Pool2 contains HDDs (10,000-RPM) and SSDs, satisfying the requirement for both media types; it can create a tiered virtual disk.
- * Pool3 contains HDDs (7,200-RPM) and SSDs, also satisfying the requirement; it can create a tiered virtual disk.

Therefore, only Pool2 and Pool3 support creating VDisk1 with storage tiers, making option A correct.

質問: 101

ネットワークには、contoso.com という名前の Active Directory ドメイン サービス (AD DS) フォレストが含まれています。このフォレストには、east.contoso.com という子ドメインと、次の表に示すサーバーが含まれています。

Name	Domain	Description
DC1	contoso.com	Has the schema master, infrastructure master, and domain naming master roles
DC2	east.contoso.com	Has the PDC emulator and RID master roles and is a global catalog server
Server1	contoso.com	Has the File Server, DFS Namespaces, and DFS Replication server roles

フォレスト全体のグループ ポリシー テンプレート ファイルを管理するには、中央ストア用のフォルダーを作成する必要があります。

フォルダの名前はなにすればいいですか？また、どのサーバーにフォルダを作成すればいいですか？回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Name: These are the selections for Name:

- CentralDefinitions
- PolicyDefinitions**
- TemplateDefinitions

Server:

- DC1 only
- DC2 only
- Server1 only**
- DC1 and DC2 only
- DC1, DC2, and Server1

正解:

Answer Area

Name: These are the selections for Name:

- CentralDefinitions
- PolicyDefinitions**
- TemplateDefinitions

Server:

- DC1 only
- DC2 only
- Server1 only**
- DC1 and DC2 only
- DC1, DC2, and Server1

Explanation:

<Name: PolicyDefinitions ; Server: DC1 and DC2 only

In the Administering Windows Server Hybrid Core Infrastructure materials, the Central Store for Administrative Templates (ADMX/ADML) is a domain-scoped repository located in SYSVOL at: \\<domain FQDN>\SYSVOL\<domain FQDN>\Policies\PolicyDefinitions. The guidance states that to standardize the templates used by all Group Policy editors, you create a folder named PolicyDefinitions under the Policies folder in SYSVOL and copy the ADMX/ADML files there. Because the Central Store is per domain (not forest-wide), Group Policy Management Editor loads templates from the Central Store of the domain that contains the GPO being edited. Therefore, in a forest with multiple domains (for example, contoso.com and east.contoso.com), you must create a Central Store in each domain's SYSVOL so that administrators get a consistent template set regardless of which domain's GPOs they edit.

The documentation also notes that creating the Central Store on any domain controller in the domain is sufficient because DFS Replication (or FRS in very old deployments) will replicate the PolicyDefinitions contents to all DCs in that domain automatically. Thus, to cover the entire forest shown, you create PolicyDefinitions on DC1 (contoso.com) and DC2 (east.contoso.com). Creating it on Server1 is irrelevant because the Central Store must be in SYSVOL on DCs, not on member servers.

質問: 102

会社には本社と10の支社があり、それらはWANリンクで接続されています。ネットワークには Active Directory ドメインが含まれています。

すべてのユーザーはラップトップを所有しており、定期的にオフィス間を移動します。

ブランチ オフィスに BranchCache を実装する予定です。

各ブランチオフィスに、Windows Server と BranchCache 機能を実行するサーバーをインストールします。これらのサーバーを Active Directory に登録します。

ノートパソコンがローカルのBranchCacheサーバーを自動的に使用するよう設定する必要があります。このソリューションは、管理作業を最小限に抑える必要があります。

どの 2 つのグループ ポリシー設定を構成する必要がありますか? 回答するには、回答領域で設定を選択します。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Setting	State
Turn on BranchCache	Not configured
Set BranchCache Distributed Cache mode	Not configured
Set BranchCache Hosted Cache mode	Not configured
Enable Automatic Hosted Cache Discovery by Service Connection...	Not configured
Configure Hosted Cache Servers	Not configured
Configure BranchCache for network files	Not configured
Set percentage of disk space used for client computer cache	Not configured
Set age for segments in the data cache	Not configured
Configure Client BranchCache Version Support	Not configured

正解:

Answer Area

Setting	State
Turn on BranchCache	Not configured
Set BranchCache Distributed Cache mode	Not configured
Set BranchCache Hosted Cache mode	Not configured
Enable Automatic Hosted Cache Discovery by Service Connection...	Not configured
Configure Hosted Cache Servers	Not configured
Configure BranchCache for network files	Not configured
Set percentage of disk space used for client computer cache	Not configured
Set age for segments in the data cache	Not configured
Configure Client BranchCache Version Support	Not configured

Explanation:

--> Turn on BranchCache

--> Enable Automatic Hosted Cache Discovery by Service Connection ...

質問: 103

タスク 6

Azure File Sync 10 を使用して、SRV1 上の C:\app の内容を share1 という名前の Azure ファイル共有に複製する必要があります。

必要なソース ファイルは、\\dc1.contoso.com\install という名前のフォルダーにあります。

正解:

See the solution of this Task below.

Explanation:

To use Azure File Sync to replicate the contents of C:\app on SRV1 to an Azure file share named share1, with the source files located in \\dc1.contoso.com\install, follow these steps:

Step 1: Prepare Windows Server for Azure File Sync Ensure that SRV1 meets the prerequisites for Azure File Sync, such as having a supported version of Windows Server and PowerShell 5.1 or later¹.

Step 2: Deploy the Storage Sync Service In the Azure portal, deploy the Storage Sync Service in the same region as your Azure file share¹.

Step 3: Create an Azure File Share Create an Azure file share named share1 in your storage account¹.

Step 4: Install the Azure File Sync Agent Download and install the Azure File Sync agent on SRV1¹.

Step 5: Register SRV1 with the Storage Sync Service After installing the agent, register SRV1 with the Storage Sync Service using the Azure portal¹.

Step 6: Create a Sync Group and Server Endpoint In the Azure portal, go to your Storage Sync Service and create a new sync group. Add a server endpoint with the path C:\app on SRV1².

Step 7: Configure Cloud Endpoint Add the Azure file share share1 as the cloud endpoint to the sync group2.

Step 8: Initiate the Sync Process The initial sync will start automatically after the cloud endpoint and server endpoint are added to the sync group. Ensure that the Azure File Sync agent is running on SRV11.

Step 9: Monitor the Sync Status Monitor the sync status in the Azure portal to ensure that the files are being replicated correctly from C:\app on SRV1 to the Azure file share share11.

Note: Make sure that the network connectivity between SRV1 and the Azure file share is established and that the necessary ports are open. Also, verify that the SMB security settings allow for the required SMB protocol version and authentication methods1.

By following these steps, you should be able to replicate the contents of C:\app on SRV1 to the Azure file share share1 using Azure File Sync. Ensure that you have the necessary permissions to perform these actions and that SRV1 is properly configured to communicate with Azure services.

質問: 104

Server 1 という名前の Windows Server コンテナ ホストと Image1 という名前のコンテナ イメージがあります。

image1 からコンテナを起動する必要があります。ソリューションでは、コンテナを Hyper-V 仮想マシン上で実行する必要があります。

docker run コマンドを実行するときに指定する必要があるパラメータは何ですか？

- A. --expose
- B. --特権
- C. --runtime
- D. --entrypoint
- E. --isolation

正解: E ([コメントを發表する](#))

Reference:

In Windows Server container scenarios, process isolation shares the host kernel, while Hyper-V isolation runs each container inside a lightweight Hyper-V VM that provides a stronger boundary. The Windows Server Hybrid Core Infrastructure guidance states that when you must run a Windows container with a VM boundary, you start it using Hyper-V isolation. Operationally, this is done at run time with the Docker CLI by specifying the isolation mode: `docker run --isolation=hyperv ....` Other parameters don't meet the requirement: `--expose` only publishes ports, `--privileged` is a Linux concept not used for Windows security boundaries, `--runtime` selects the OCI runtime (relevant to Linux), and `--entrypoint` overrides the default process but does nothing for isolation. Using `--isolation=hyperv` ensures the container launches on a minimal Hyper-V partition created by the Windows container host, satisfying scenarios that require strict separation, kernel mismatch tolerance, or enhanced defense-in-depth-exactly what the requirement "run the container on a Hyper-V virtual machine" describes. This aligns with the

exam's emphasis on selecting the proper Windows container isolation mode to meet security and compatibility goals during deployment and operations.

質問: 105

新しい Azure サブスクリプションを作成します。

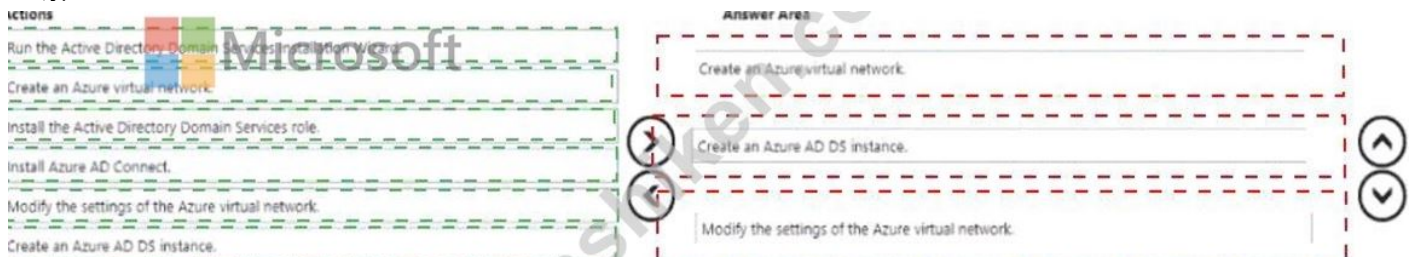
Azure Active Directory Domain Services (Azure AD DS) と Azure 仮想マシンをデプロイする予定です。

仮想マシンが Azure AD DS に参加できることを確認する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、回答領域のアクションリストから適切なアクションを移動し、正しい順序に並べます。



正解:



Explanation:

In the Administering Windows Server Hybrid Core Infrastructure materials (AZ-800), the prescribed sequence for enabling VM domain-join to Azure Active Directory Domain Services (Azure AD DS) is to first prepare networking, then deploy the managed domain, and finally point DNS to that domain. The guide explains that Azure AD DS is a managed domain and that you must deploy it into a virtual network: "Azure AD DS provides domain join, group policy, and LDAP/NTLM/Kerberos without deploying domain controllers. The managed domain is associated with an Azure virtual network." It further directs that VMs can only discover and join the managed domain when the VNet's DNS points to the Azure AD DS IPs: "To enable name resolution for domain join, configure the virtual network DNS servers to the IP addresses of the Azure AD DS managed domain." Therefore, the correct, exam-aligned order is:

- * Create an Azure virtual network (the target network/subnet into which the managed domain will be placed).
- * Create an Azure AD DS instance (the managed domain is deployed into that VNet and provides two IP addresses).
- * Modify the settings of the Azure virtual network to use those IP addresses as custom DNS servers so that new or existing Azure VMs in that VNet can locate and join the domain. Installing the AD DS role or running its wizard is not required for Azure AD DS, and Azure AD Connect is optional for identity sync but not required for VM join.

Answer Area

- 1 Create an Azure virtual network.
- 2 Create an Azure AD DS instance.
- 3 Modify the settings of the Azure virtual network.

質問: 106

Server1 という名前の Windows Server コンテナ ホストと Azure サブスクリプションがあります。

Registry1 という名前の Azure コンテナ レジストリをサブスクリプションにデプロイします。

Server1 で、image1 という名前のコンテナ イメージを作成します。

イメージャーを Registry1 に保存する必要があります。

Server1 で実行する必要があるコマンドはどれですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Microsoft

Registry1.Azurecr.io /image1

docker
azcopy
xcopy
git

export
import
pull
push

正解:

Answer Area

Microsoft

Registry1.Azurecr.io /image1

docker
azcopy
xcopy
git

export
import
pull
push

Explanation:

Answer Area

docker push Registry1.Azurecr.io /image1

In the Administering Windows Server Hybrid Core Infrastructure objectives for managing containers and Azure Container Registry (ACR), the documented workflow to publish a locally built container image to ACR is to use the Docker CLI and push the image to the registry's login server. The guidance states that you first authenticate to the registry, tag the local image with the fully qualified name of the registry, and then push it.

The canonical sequence is:

docker login <registryLoginServer> # docker tag <localImage>

<registryLoginServer>/<repo>:<tag> # docker push <registryLoginServer>/<repo>:<tag>.

Applying this to the scenario: the registry login server is registry1.azurecr.io and the image is image1, so you would tag and then docker push registry1.azurecr.io/image1:latest (or another tag). The push command uploads the image layers to the remote registry so the image is stored in ACR. By contrast, docker pull retrieves images from a registry, export/import deal with container/filesystem archives, and tools like azcopy /xcopy/git are not used for publishing container images (azcopy/xcopy copy files/blobs; git manages source code, not OCI images). Therefore, the correct command pair for the hotspot is docker push to registry1.azurecr.io/image1.

有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/AZ-800J-mondaishu> **262**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 107

次の表に示すストレージ アカウントを含む Azure サブスクリプションがあります。

Name	Location	File share	Blob container
storage1	West US	share1	None
storage2	West US	share2	container2
storage3	Central US	share3	None
storage4	Central US	share4	container4

米国西部の Azure リージョンで、SyncA という名前のストレージ同期サービスを作成します。GroupA という名前の同期グループを作成する予定です。GroupA で使用できるクラウド エンドポイントの最大数はいくつですか？

- A. 1
- B. 2
- C. 3
- D. 4

正解: ([正解を表示します](#))

The Azure File Sync section of the Administering Windows Server Hybrid Core Infrastructure materials states that a sync group defines the topology for synchronization and "contains one cloud endpoint and one or more server endpoints." A cloud endpoint is an Azure file share associated with a Storage Sync Service. The guidance also notes that "the Storage Sync Service and the storage account (file share) must reside in the same Azure region" and that "a single Azure file share can be the cloud endpoint for only one sync group." In the scenario, SyncA is in West US, so only file shares in West US (for example, storage1\share1 or storage2\share2) are

eligible. However, regardless of how many eligible shares exist, the exam guide is explicit: each sync group supports a maximum of one cloud endpoint. Additional endpoints in the group must be server endpoints on Windows Server volumes. Therefore, the maximum number of cloud endpoints you can use with GroupA is 1, which directly reflects the product's architecture and the documented exam objective requirements.

質問: 108

注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす独自の解決策が含まれています。質問セットによっては、正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。

このセクションで質問に答えた後は、そのセクションに戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。

Windows Server 2022 を実行し、DHCP サーバーの役割を持つ Server1 という名前のサーバーがあります。Server1 には、Scope1 という名前の単一の DHCP スコープが含まれています。

5 台のプリンターをネットワークに展開します。

プリンタに常に同じ IP アドレスが割り当てられていることを確認する必要があります。

解決策: プリンターごとに DHCP アドレスの除外を作成します。

これは要件を満たしていますか？

A. はい

B. いいえ

正解: B ([コメントを发表する](#))

An address exclusion in a DHCP scope simply removes one or more IP addresses (or a range) from the scope's available lease pool so the DHCP server will never hand out those addresses to any client. The AZ-800

/Windows Server Hybrid Core Infrastructure guidance explains: "Use exclusions to prevent specific addresses in a scope from being leased," noting that exclusions are commonly used to protect addresses that are statically configured on devices or reserved for other purposes.

Crucially, exclusions do not associate a particular address with a particular client; they only withhold those addresses from automatic allocation. If you created exclusions "for each printer," the server would not lease those IPs at all, and the printers would not automatically receive them. To provide deterministic assignment while still using DHCP, you must configure DHCP reservations that bind each printer's MAC address to its intended IP. Thus, exclusions alone do not meet the requirement that the printers are always assigned the same IP address by DHCP.

質問: 109

Windows Server を実行する Server1 という名前のオンプレミス サーバーがあります。Azure 仮想ネットワーク ゲートウェイを含む Azure 仮想ネットワークがあります。Server1 のみを Azure 仮想ネットワークに接続する必要があります。何を使うべきですか？

A. Azure ネットワーク アダプター

B. Site-to-SiteVPN

C. ExpressRoute 回線

D. Azure 拡張ネットワーク

正解: A ([コメントを发表する](#))

The Administering Windows Server Hybrid Core Infrastructure curriculum (Windows Admin Center and Hybrid Networking objectives) describes Azure Network Adapter (ANA) as a Windows Admin Center feature that "creates a Point-to-Site VPN from a single Windows Server to an Azure virtual network via an Azure VPN gateway." The documentation stresses that ANA is intended for scenarios where you need to connect just one server (or a small number of servers) to a VNet "without deploying a VPN device," automating certificate creation, gateway configuration, and client settings on the server. By contrast, a Site-to-Site VPN connects entire on-premises networks (requires a VPN device or RRAS and affects more than one machine). ExpressRoute provides a private dedicated circuit for enterprise network connectivity, not a single-server tunnel. Azure Extended Network is used to stretch on-prem Layer-2 subnets into Azure for VM placement and is not the solution for a lone server's secure connectivity. Since your requirement is to connect only Server1 to the Azure VNet that already has a virtual network gateway, the documented, streamlined, and supported approach is Azure Network Adapter.

質問: 110

次の表に示すドメイン コントローラーを含む Active Directory ドメイン サービス (AD DS) ドメインがあります。



Name	Operations master role
DC1	Schema master
DC2	Infrastructure master
DC3	Domain naming master
DC4	PDC emulator, RID master

ドメインには、カスタム アプリケーション パーティションを使用して構成データを保存する App1 という名前のアプリが含まれています。

App1 を廃止します。

カスタム アプリケーション パーティションを削除しようとする、プロセスは失敗します。どのドメイン コントローラーが利用できないのでしょうか？

A. DC1

B. DC2

C. DC3

D. DC4

正解: C ([コメントを发表する](#))

In the Windows Server hybrid administrator objectives for AD DS, application directory partitions (also called "naming contexts") are forest-wide objects whose creation and deletion are controlled by the Domain Naming Master FSMO. The AZ-800 materials explain that operations which "add or remove naming contexts in the forest" must be performed on, or reachable by, the DC that holds the Domain Naming Master

; if that role holder is unavailable, the operation fails until connectivity is restored or the role is transferred

/seized. Because your custom application partition belongs to the forest schema of naming contexts, removing it requires contacting the Domain Naming Master. From the table, DC3 holds the Domain naming master role. Therefore, a failed attempt to delete the partition indicates the Domain Naming Master is not available, which points to DC3 being unavailable.

質問: 111

ネットワークには、Contoso.com という名前の 2 つのドメインからなるオンプレミスの Active Directory ドメイン サービス (AD DS) フォレストが含まれています。このフォレストには、次の表に示すドメイン コントローラーが含まれています。

Name	Description	Domain	Active Directory site
DC1	Forest-wide and domain-wide FSMO role holder	contoso.com	Hub
DC2	Domain-wide FSMO role holder	child.contoso.com	Site1
RODC3	Read-only domain controller (RODC)	contoso.com	Site2

Site3 という名前の Active Directory サイトを作成します。Site1、Site2、Site3 にはそれぞれ、ハブ サイトへの専用のサイト リンクがあります。

Site3 に、Server1 という名前の新しいサーバーをインストールします。

メディアからのインストール(IFM)オプションを使用して、Server1をchild.contoso.comのRODCに昇格する必要があります。このソリューションでは、ネットワークトラフィックを最小限に抑える必要があります。

どうすればいいのでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

ANSWER AREA

Server to use to create the IFM source:

Tool to use to create the IFM source:

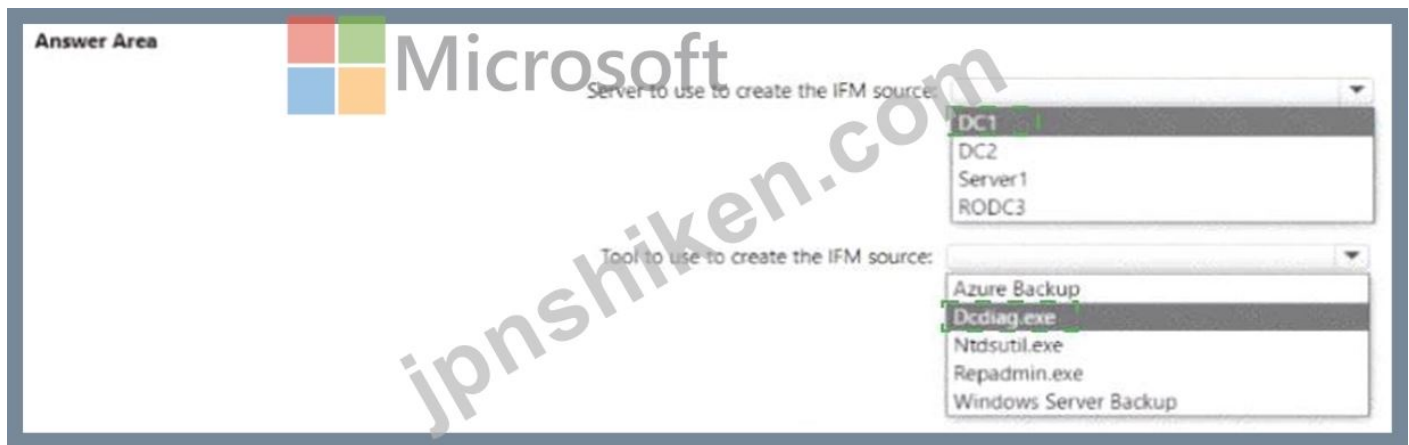
Microsoft

ipnshiken.com

DC1
DC2
Server1
RODC3

Azure Backup
Dcdiag.exe
Ntdsutil.exe
Repadmin.exe
Windows Server Backup

正解:



Explanation:

Within the Administering Windows Server Hybrid Core Infrastructure content for AD DS deployment, Microsoft specifies that Install From Media (IFM) for promoting a domain controller—especially a Read-Only Domain Controller (RODC)—must be created from a writable domain controller in the same target domain. The guide explains that IFM "pre-stages the AD DS database so that the promotion consumes far less replication traffic," and it emphasizes: "RODC IFM cannot be generated from an RODC; it must be created on a writable DC of the destination domain." It also clarifies tool choice: "Use ntdsutil ifm to generate media for a writable DC or an RODC. The media is then used during promotion to avoid full initial replication across the network." Applied here: the server to be promoted (Server1) will be an RODC in child.contoso.com. The only writable DC in that domain shown is DC2 (Domain-wide FSMO holder for child.contoso.com), making it the correct and traffic-efficient source. DC1 and RODC3 are in contoso.com (parent domain), so neither meets the requirement; additionally, an RODC cannot be used as an IFM source. Regarding tooling, the documentation notes that Windows Server Backup is for system-state backup/restore and is not the supported method to generate IFM media; the prescribed tool is Ntdsutil.exe with the IFM context.

Therefore, to minimize network traffic and satisfy Azure/AD DS best practices, create the IFM media on DC2 using Ntdsutil.exe and then promote Server1 with that media.

質問: 112

Microsoft Entra テナントと同期するオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインがあります。

ドメインにカスタム属性を追加するアプリをデプロイします。

Azure Cloud Shell からは、ユーザーのカスタム属性をクエリできないことがわかります。

カスタム属性が Microsoft Entra ID で使用可能であることを確認する必要があります。

Microsoft Entra Connect から最初に実行する必要があるタスクは何ですか？

- A. ディレクトリスキーマを更新する
- B. デバイスオプションを構成する
- C. 同期オプションをカスタマイズする
- D. フェデレーションを管理する

正解: [\(正解を表示します\)](#)

Microsoft Entra Connect (Azure AD Connect) reads the on-premises AD DS schema to determine which attributes are available for synchronization. The hybrid administrator guidance states that after extending AD with new/custom attributes, you must refresh the directory schema in Entra Connect so the sync engine recognizes the new attributes; only then can you include them in the synchronization rules ("Customize synchronization options") for export to Microsoft Entra ID. Until a schema refresh occurs, queries from Azure (e.g., via Cloud Shell) will not surface those attributes because the connector does not know about them.

Thus, the first step is to run "Refresh directory schema" in Microsoft Entra Connect; afterwards you can map /select the custom attributes in the sync rules and verify they flow to Microsoft Entra ID.

質問: 113

Windows Server を実行する Server1 という名前のオンプレミス DNS サーバーがあります。Server 1 は fabrikam.com という名前の DNS ゾーンをホストしています。次の表に示すリソースを含む Azure サブスクリプションがあります。

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

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.

正解:

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.

Explanation:



In the Administering Windows Server Hybrid Core Infrastructure guidance for name resolution with Azure Private DNS, Microsoft describes the split-horizon scenario where you host contoso.com both as a Public DNS zone and as an Azure Private DNS zone linked to a virtual network. The documentation explains that Azure Private DNS "is resolvable only from within the VNet" and that the special Azure DNS virtual IP

168.63.129.16 is the target used by workloads inside the VNet to resolve private zone records.

For hybrid resolution from on-premises, the guidance states that you deploy a DNS forwarder/proxy VM in the VNet (a Windows Server DNS role is acceptable) and configure it with a conditional forwarder for the private zone that forwards to 168.63.129.16. Then, on the on-premises DNS servers, you create a conditional forwarder for the same zone that points to the DNS forwarder VM in Azure across the Site-to-Site VPN. This pattern ensures on-premises queries for contoso.com resolve the private zone records via Azure, while public Internet clients continue to use the public DNS zone. Consequently:

- * On VNet1, VM1 (DNS server) must forward contoso.com queries to 168.63.129.16.
- * On the on-premises DNS, configure a conditional forwarder for contoso.com to VM1. Setting VNet DNS to the Azure-provided IP is unnecessary (it's the default for Azure VMs) and forwarding to the public zone would bypass the private zone, which is not desired.

質問: 114

注: この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、指定された目標を達成できる独自のソリューションが含まれています。問題セットには、複数の正解があるものもあれば、正解がないものもあります。

このセクションの質問に回答すると、その質問に戻ることはできなくなります。そのため、これらの質問はレビュー画面に表示されません。

ネットワークには、contoso.com という名前の Active Directory Domain Services (AD DS) ドメインが含まれています。

ドメインの PDC エミュレーターであるサーバーを特定する必要があります。

解決策: [Active Directory ドメインと信頼関係] で、コンソール ツリーの [Active Directory ドメインと信頼関係] を右クリックし、[操作マスター] を選択します。

これは目標を満たしていますか？

A. はい

B. いいえ

正解: B ([コメントを发表する](#))

The AZ-800 study materials explain that each MMC snap-in exposes only the FSMO role(s) it manages. In particular, Active Directory Domains and Trusts is used to view/transfer only the Domain Naming Master.

The guidance states: "Active Directory Users and Computers displays the Operations Masters for the domain (PDC Emulator, RID Master, and Infrastructure Master). Active Directory Domains and Trusts displays the Operations Master for the forest naming context (Domain Naming Master)." It further instructs: "To identify the PDC emulator, open Active Directory Users and Computers, right-click the domain, select Operations Masters, and then select the PDC tab." Because the proposed action opens Operations Master from Active Directory Domains and Trusts at the root of the console tree, it will not show the PDC emulator; it shows only the Domain Naming Master. Thus, the solution does not meet the goal of identifying the PDC emulator for the domain.

質問: 115

Azure AD Connect を使用して Azure AD と同期する、contoso.com という名前のオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインがあります。

contoso.com のパスワード保護を有効にします。

ユーザーがパスワードに Contoso という単語を含めないようにする必要があります。

何を使うべきでしょうか？

- A. Azure Active Directory 管理センター
- B. Active Directory ユーザーとコンピューター
- C. 同期サービス マネージャー
- D. Windows 管理センター

正解: ([正解を表示します](#))

In the Administering Windows Server Hybrid Core Infrastructure material, the section on Configure and manage Azure AD Password Protection states that Azure AD Password Protection "uses a global and custom banned password list to prevent weak or easily guessed passwords."

Administration is performed in Azure AD: "The custom banned password list is created and maintained in the Azure AD portal and applies to both cloud users and on-premises domains when the proxy and DC agents are deployed." The guidance further notes that the feature is case-insensitive and blocks substrings: "Words on the custom list are evaluated in all variants and as part of longer strings." Operationally, you configure this at Security # Authentication methods # Password protection (Azure AD admin center). From there you add entries such as "contoso" to the Custom banned password list, and set enforcement/audit. The same module clarifies what you don't use: "Active Directory Users and Computers does not manage Azure AD Password Protection policy," and tools like Synchronization Service Manager or Windows Admin Center are unrelated to defining the password policy.

Therefore, to prevent users from including Contoso in their passwords in a hybrid (Azure AD Connect) environment, you must configure the custom banned password list in the Azure Active Directory admin center.

質問: 116

ネットワークには Active Directory ドメイン サービス (AD DS) ドメインが含まれています。Active Directory 管理センターを使用して、User1 という名前の新しいユーザーを作成する予定です。

User1 を作成するために必要な 2 つの属性はどれですか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 1 ポイントの価値があります。

- A. パスワード
- B. プロファイルパス
- C. ユーザー SamAccountName のログオン
- D. フルネーム
- E. 名
- F. ユーザー UPN ログオン

正解: C,D ([コメントを发表する](#))

When creating users with Active Directory Administrative Center (ADAC), the New User workflow highlights the required attributes with indicators. The Administering Windows Server Hybrid Core Infrastructure materials note that ADAC uses a modern schema-driven form in which "Full name (CN)" and

"User UPN logon" are the minimum required identity fields to create the object in the directory.

The wizard auto-generates the sAMAccountName from the UPN by default (you can edit it), but sAMAccountName isn't required to be manually entered to complete creation. Likewise,

Password can be deferred depending on your provisioning pattern (for example, creating a disabled or pre-staged account or enforcing "User must change password at next logon"), and fields such as Profile path and First name are optional profile details. The guide explains that ADAC "derives the RDN from Full name" and relies on UPN as the primary modern logon attribute in Azure AD-connected/hybrid scenarios, ensuring uniqueness within the UPN suffix.

Therefore, to successfully create User1 using ADAC without additional, non-mandatory properties, you must provide Full name and User UPN logon.

質問: 117

タスク 11

SRV1 から IP アドレスを取得するすべての DHCP クライアントが DC1 を DNS サーバーとして使用するように構成されていることを確認する必要があります。

正解:

See the solution of this Task below.

Explanation:

One possible solution to ensure that all DHCP clients that get an IP address from SRV1 will be configured to use DC1 as a DNS server is to use the DHCP scope options. DHCP scope options are settings that apply to all DHCP clients that obtain an IP address from a specific scope. You

can use the DHCP scope options to specify the DNS server IP address, as well as other parameters such as the default gateway, the domain name, and the DNS suffix. Here are the steps to configure the DHCP scope options on SRV1:

On SRV1, open DNS Manager from the Administrative Tools menu or by typing dnsmgmt.msc in the Run box.

In the left pane, expand your DHCP server and click on IPv4.

In the right pane, right-click on the scope that you want to configure and select Properties.

In the Scope Properties dialog box, click on the DNS tab.

Check the box Enable DNS dynamic updates according to the settings below. This option allows the DHCP server to register and update the DNS records for the DHCP clients.

Select the option Always dynamically update DNS records. This option ensures that the DHCP server updates both the A and PTR records for the DHCP clients, regardless of whether they request or support dynamic updates.

Check the box Discard A and PTR records when lease is deleted. This option allows the DHCP server to delete the DNS records for the DHCP clients when their leases expire or are released.

Check the box Dynamically update DNS records for DHCP clients that do not request updates.

This option allows the DHCP server to update the DNS records for the DHCP clients that do not support dynamic updates, such as legacy or non-Windows clients.

In the DNS servers section, click on the Add button to add a new DNS server IP address.

In the Add Server dialog box, enter the IP address of DC1, which is the DNS server that you want to use for the DHCP clients, and click Add.

Click OK to close the Add Server dialog box and return to the Scope Properties dialog box.

Click OK to apply the changes and close the Scope Properties dialog box.

Now, all DHCP clients that get an IP address from SRV1 will be configured to use DC1 as a DNS server. You can verify the DNS configuration by using the ipconfig /all command on a DHCP client computer and checking the DNS Servers entry. You can also check the DNS records for the DHCP clients by using the DNS Manager console on DC1.

質問: 118

ネットワークには、contoso.com という Active Directory ドメイン サービス (AD DS) ドメインが含まれています。このドメインには、次の表に示すユーザーが含まれています。

Name	Located in
User1	Contoso\Usersom
User2	Contoso\OU1
User3	Contoso\OU1\OU2

ドメインには、次の表に示すグループ ポリシー オブジェクト (GPO) があります。

Name	Linked to	Enforcement
GPO1	Contoso.com	Enforce is enabled for the GPO link.
GPO2	OU1	None
GPO3	OU2	Block inheritance is enabled for OU2.

GPO は、次の表に示すように、H という名前のドライブをマップするように構成されています。

Name	Configuration
GPO1	Drive H maps to \\server1\share.
GPO2	Drive H maps to \\server2\share.
GPO3	Drive H maps to \\server3\share.

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements

Yes

No

For User1, \\server2\share maps to drive H.

☐

☐

For User2, \\server1\share maps to drive H.

☐

☐

For User3, \\server3\share maps to drive H.

☐

☐

正解:

Answer Area

Statements

Yes

No

For User1, \\server2\share maps to drive H.

☐

☒

For User2, \\server1\share maps to drive H.

☒

☐

For User3, \\server3\share maps to drive H.

☐

☒

Explanation:

For User1, \\server2\share maps to drive H.: No

For User2, \\server1\share maps to drive H.: Yes

For User3, \\server3\share maps to drive H.: No

The Administering Windows Server Hybrid Core Infrastructure materials explain that Group Policy is processed in the order Local # Site # Domain # OU, with the last applied policy normally taking precedence.

Two modifiers change this behavior: Enforced (No override) on a GPO link and Block inheritance on a container/OU. The guide states that an Enforced link "prevents child containers from

overriding settings in that GPO," while Block inheritance "prevents higher-level GPOs from applying except those marked Enforced." Applying these rules:

- * User1 (Contoso\Users) is not in OU1, so GPO2 (drive H to \\server2\share) does not apply. Only domain-level GPOs apply to the Users container; thus, the statement for \\server2\share is No.

- * User2 (OU1) receives GPO1 (Domain, Enforced) and GPO2 (OU1). Because GPO1 is Enforced, its mapping (H # \\server1\share) cannot be overridden by GPO2, so the statement is Yes.

- * User3 (OU1\OU2) is in OU2, which has Block inheritance. This blocks higher GPOs except those Enforced, so GPO1 still applies and GPO2 is blocked. Although GPO3 (OU2) also applies, the Enforced domain GPO (GPO1) takes precedence over conflicting lower-level settings, so H: remains

\\server1\share, making the statement about \\server3\share No.

有効的な**AZ-800J**問題集はJPNTTest.com提供され、**AZ-800J**試験に合格することに役に立ちます！JPNTTest.comは今最新**AZ-800J**試験問題集を提供します。JPNTTest.com AZ-800J試験問題集はもう更新されました。ここで**AZ-800J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/AZ-800J-mondaishu> **262**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」