

# Configuring Windows Server Hybrid Advanced Services

## 1. DRAG DROP (Drag and Drop is not supported)

You are planning the implementation of Cluster2 to support the on-premises migration plan. You need to ensure that the disks on Cluster2 meet the security requirements.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

### Actions

- Add a disk resource to the cluster.
- Enable BitLocker on the volume.
- Update the BitLockerProtectorInfo property of the volume.
- Create a Cluster Shared Volume (CSV).
- Put the disk in maintenance mode.

### Answer Area

A. See Explanation section for answer.

Answer(s): A

## 2. HOTSPOT (Drag and Drop is not supported)

You need to implement a security policy solution to authorize the applications. The solution must meet the security requirements.

Which service should you use to enforce the security policy, and what should you use to manage the policy settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Enforce the security policy:

- Microsoft Defender Application Control
- Microsoft Defender Application Guard
- Microsoft Defender Credential Guard
- Microsoft Defender for Endpoint

Manage the policy settings:

- Configuration profiles in Microsoft Intune
- Compliance policies in Microsoft Intune
- Group Policy Objects (GPOs)

A. See Explanation section for answer.

Answer(s): A

3. You are remediating the firewall security risks to meet the security requirements. What should you configure to reduce the risks?

A. a Group Policy Object (GPO)

B. adaptive network hardening in Microsoft Defender for Cloud

C. a network security group (NSG) in Sub1

D. an Azure Firewall policy

**Answer(s): A**

---

4. You are planning the deployment of Microsoft Sentinel.

Which type of Microsoft Sentinel data connector should you use to meet the security requirements?

A. Threat Intelligence - TAXII

B. Azure Active Directory

C. Microsoft Defender for Cloud

D. Microsoft Defender for Identity

**Answer(s): D**

---

5. HOTSPOT (Drag and Drop is not supported)

You need to configure BitLocker on Server4.

On which volumes can you turn on BitLocker, and on which volumes can you turn on auto-unlock? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

BitLocker:

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

Auto-unlock:

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

A. See Explanation section for answer.

**Answer(s): A**

---

6. HOTSPOT (Drag and Drop is not supported)

What is the effective minimum password length for User1 and Admin1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

User1: 

	▼
8	
9	
10	
11	
12	

Admin1: 

	▼
8	
9	
10	
11	
12	

A. See Explanation section for answer.

Answer(s): A

---

#### 7. HOTSPOT (Drag and Drop is not supported)

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
User1 can sign in to Server4 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to Server4 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to Server4 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>

A. See Explanation section for answer.

Answer(s): A

---

#### 8. HOTSPOT (Drag and Drop is not supported)

With which servers can Server1 and Server3 communicate? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Server1 can communicate with:

	▼
Server2 only	
Server3 only	
Server2 and Server3 only	
Server2, Server3, and Server4	
None of the servers	

Server3 can communicate with:

	▼
Server2 only	
Server1 and Server2 only	
Server1 and Server4 only	
Server1, Server2, and Server4	
None of the servers	

A. See Explanation section for answer.

**Answer(s): A**

---

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a server named Server1 that runs Windows Server.

You need to ensure that only specific applications can modify the data in protected folders on Server1.

Solution: From Virus & threat protection, you configure Controlled folder access.

Does this meet the goal?

A. Yes

B. No

**Answer(s): A**

---

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a server named Server1 that runs Windows Server.

You need to ensure that only specific applications can modify the data in protected folders on Server1.

Solution: From Virus & threat protection, you configure Tamper Protection Does this meet the goal?

A. Yes

B. No

**Answer(s): B**

---

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a server named Server1 that runs Windows Server.

You need to ensure that only specific applications can modify the data in protected folders on Server1.

Solution: From App & browser control, you configure the Exploit protection settings.  
Does this meet the goal?

A. Yes

B. No

**Answer(s): B**

---

**12. DRAG DROP** (Drag and Drop is not supported)

You have an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant. The AD DS domain contains a domain controller named DC1. DC1 does NOT have internet access.

You need to configure password security for on-premises users. The solution must meet the following requirements:

- Prevent the users from using known weak passwords.
- Prevent the users from using the company name in passwords.

What should you do? To answer, drag the appropriate configurations to the correct targets. Each configuration may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**Configurations**

- Configure Azure AD Identity Protection.
- Configure Azure AD Password Protection.
- Install the Azure AD Pass-through Authentication Agent.
- Install the Azure AD Password Protection DC agent.
- Install the Azure AD Password Protection proxy service.

**Answer Area**

- On DC1:
- On a member server:
- In Azure:

A. See Explanation section for answer.

**Answer(s): A**

---

**13. HOTSPOT** (Drag and Drop is not supported)

The Default Domain Policy Group Policy Object (GPO) is shown in the GPO exhibit. (Click the GPO tab.)

Group Policy Management

File Action View Window Help

Group Policy Management

- Forest: Fabrikam.com
  - Domains
    - Fabrikam.com
      - Default Domain Policy
      - Domain Controllers
      - ServiceAccounts
      - Group Policy Objects
      - WMI Filters
      - Starter GPOs
    - Sites
      - Group Policy Modeling
      - Group Policy Results

### Default Domain Policy

Scope Details Settings Delegation

**Default Domain Policy**  
Data collected on: 10/18/2021 9:06:02 PM

**General**

- Details
- Links
- Security Filtering
- Delegation

**Computer Configuration (Enabled)**

**Policies**

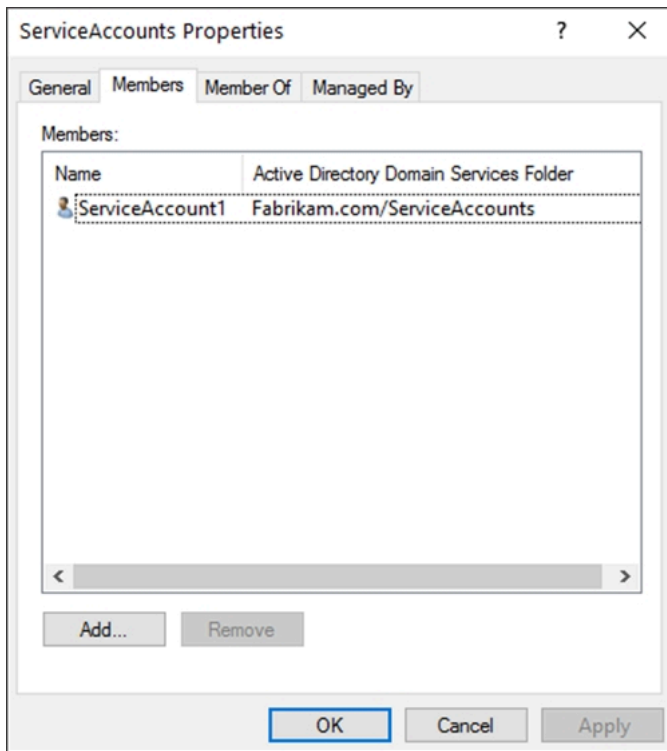
- Windows Settings
- Security Settings
  - Account Policies/Password Policy
 

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
  - Account Policies/Account Lockout Policy
  - Account Policies/Kerberos Policy
  - Local Policies/Security Options
  - Public Key Policies/Encrypting File System

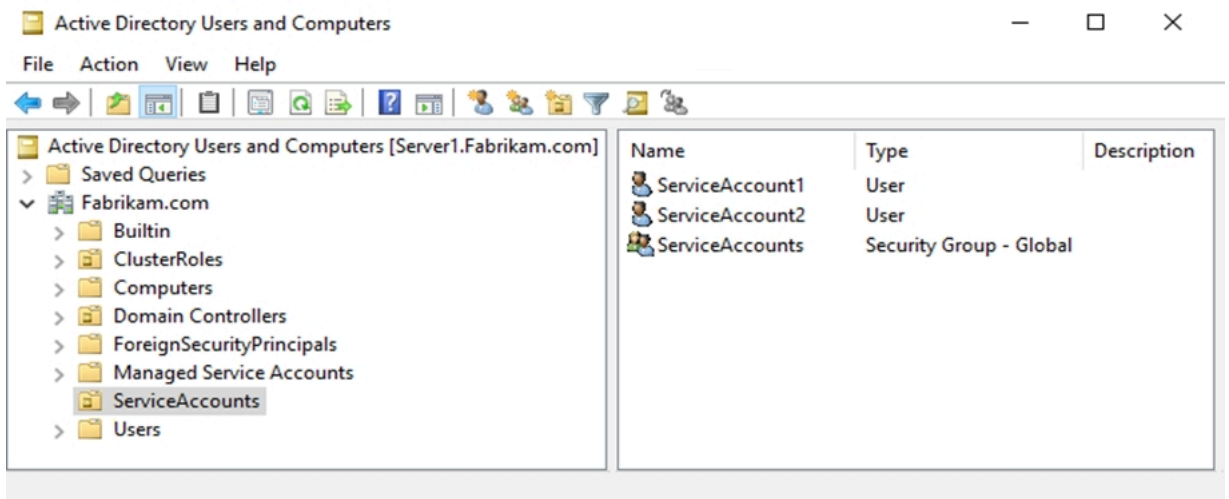
**User Configuration (Enabled)**

No settings defined.

The members of a group named Service Accounts are shown in the Group exhibit. (Click the Group tab.)



An organizational unit (OU) named ServiceAccounts is shown in the OU exhibit. (Click the OU tab.)



You create a Password Settings Object (PSO) as shown in the PSO exhibit. (Click the PSO tab.)



# Service Accounts Policy

**Password Settings**

Directly Applies To

Extensions

**Password Settings**

Name: \* Service Accounts Policy

Precedence: \* 10

Enforce minimum password length  
Minimum password length (character... \* 16

Enforce password history  
Number of passwords remembered: \* 12

Password must meet complexity requirements

Store password using reversible encryption

Protect from accidental deletion

Description:

Password age options:

Enforce minimum password age  
User cannot change the password

Enforce maximum password age  
User must change the password

Enforce account lockout  
Number of failed logon attempts: 3  
Reset failed logon attempt after: 30 minutes  
Account will be locked out for:  
 For a duration of (r) 30 minutes  
 Until an administrator resets the account

**Directly Applies To**

Name	Mail
ServiceAccounts	

**Extensions**

[More Information](#)

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
The password of ServiceAccount1 must be at least 16 characters long.	<input type="radio"/>	<input type="radio"/>
The password of ServiceAccount2 must be at least 16 characters long.	<input type="radio"/>	<input type="radio"/>
Accounts that have the Service Accounts Policy applied can change their password to P@\$\$w0rd1.	<input type="radio"/>	<input type="radio"/>

A. See Explanation section for answer.

**Answer(s):** A

## 14. DRAG DROP (Drag and Drop is not supported)

Your network contains an Active Directory Domain Services (AD DS) domain. You need to implement a solution that meets the following requirements:

- Ensures that the members of the Domain Admins group are allowed to sign in only to domain controllers
- Ensures that the lifetime of Kerberos Ticket Granting Ticket (TGT) for the members of the Domain Admins group is limited to one hour

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list



of actions to the answer area and arrange them in the correct order.

Select and Place:

**Actions**

- Create a Dynamic Access Control central access policy.
- Configure the Kerberos Policy settings for the Default Domain Policy Group Policy Object (GPO).
- Create a Dynamic Access Control claim type.
- Create an authentication policy.
- Assign the authentication policy silo to user and computer accounts.
- Create an authentication policy silo.

**Answer Area**

A. See Explanation section for answer.

**Answer(s):** A

15. You have an Azure virtual machine named VM1 that runs Windows Server. You plan to deploy a new line-of-business (LOB) application to VM1.

You need to ensure that the application can create child processes.

What should you configure on VM1?

A. Microsoft Defender Credential Guard

B. Microsoft Defender Application Control

C. Microsoft Defender SmartScreen

D. Exploit protection

**Answer(s):** D

16. HOTSPOT (Drag and Drop is not supported)

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains the organizational units (OUs) shown in the following table.

Name	Contents
Domain Controllers	All the domain controllers in the domain
Domain Servers	All the servers that run Windows Server in the domain
Domain Client Computers	All the client computers that run Windows 10 in the domain
Domain Users	All the users in the domain

In the domain, you create the Group Policy Objects (GPOs) shown in the following table.

Name	IPsec setting
GPO1	Require authentication by using Kerberos V5 for inbound connections
GPO2	Request authentication by using Kerberos V5 for inbound connections
GPO3	Require authentication by using X.509 certificates for inbound connections
GPO4	Request authentication by using X.509 certificates for inbound connections

You need to implement IPsec authentication to ensure that only authenticated computer accounts can connect to the members in the domain. The solution must minimize administrative effort.

Which GPOs should you apply to the Domain Controllers OU and the Domain Servers OU? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Domain Controllers:

	▼
GPO1	
GPO2	
GPO3	
GPO4	

Domain Servers:

	▼
GPO1	
GPO2	
GPO3	
GPO4	

A. See Explanation section for answer.

**Answer(s):** A

---

**17.** You have 100 Azure virtual machines that run Windows Server. The virtual machines are onboarded to Microsoft Defender for Cloud.

You need to shut down a virtual machine automatically if Microsoft Defender for Cloud generates the "Antimalware disabled in the virtual machine" alert for the virtual machine.

What should you use in Microsoft Defender for Cloud?

A. a logic app

B. a workbook

C. a security policy

D. adaptive network hardening

**Answer(s):** A

---

**18.** You have a Microsoft Sentinel deployment and 100 Azure Arc-enabled on-premises servers. All the Azure Arc-enabled resources are in the same resource group.

You need to onboard the servers to Microsoft Sentinel. The solution must minimize administrative effort.

What should you use to onboard the servers to Microsoft Sentinel?

A. Azure Automation

B. Azure Policy

C. Azure virtual machine extensions

D. Microsoft Defender for Cloud

**Answer(s):** B

---

**19.** You have an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant by using password hash synchronization.

You have a Microsoft 365 subscription. All devices are hybrid Azure AD-joined.

Users report that they must enter their password manually when accessing Microsoft 365 applications.

You need to reduce the number of times the users are prompted for their password when they access Microsoft 365 and Azure services. What should you do?

A. In Azure AD, configure a Conditional Access policy for the Microsoft Office 365 applications.

B. In the DNS zone of the AD DS domain, create an autodiscover record.

C. From Azure AD Connect, enable single sign-on (SSO).

D. From Azure AD Connect, configure pass-through authentication.

**Answer(s): C**

---

**20.** You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have 50 Azure virtual machines that run Windows Server. You need to ensure that any security exploits detected on the virtual machines are forwarded to Defender for Cloud. Which extension should you enable on the virtual machines?

A. Vulnerability assessment for machines

B. Microsoft Dependency agent

C. Log Analytics agent for Azure VMs

D. Guest Configuration agent

**Answer(s): A**

---