**MD-100.51q**

**MD-100**



**Website:** https://vceplus.com
**VCE to PDF Converter:** https://vceplus.com/vce-to-pdf/
**Facebook:** https://www.facebook.com/VCE.For.All.VN/
**Twitter :** https://twitter.com/VCE_Plus

https://vceplus.com/

**Windows 10 (beta)**

**Question Set 1**

**QUESTION 1**

You plan to deploy Windows 10 to 100 secure computers.

You need to select a version of Windows 10 that meets the following requirements:

- Uses Microsoft Edge as the default browser
- Minimizes the attack surface on the computer
- Supports joining Microsoft Azure Active Directory (Azure AD)
- Only allows the installation of applications from the Microsoft Store

What is the best version to achieve the goal? More than one answer choice may achieve the goal. Select the **BEST** answer.

A. Windows 10 Pro in S mode
B. Windows 10 Home in S mode
C. Windows 10 Pro
D. Windows 10 Enterprise

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.microsoft.com/en-za/windows/compare

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

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

You have a computer named Computer1 that runs Windows10.

A service named Application1 is configured as shown in the exhibit.

**Application1 (Local Computer)**

General | Log On | Recovery | Dependencies

Log on as:

○ Local System account
  ☐ Allow service to interact with desktop

● This account:        Service1        [ Browse... ]

  Password:         ••••••••

  Confirm password: ••••••••

[ OK ]  [ Cancel ]  [ Apply ]

You discover that a user used the Service1 account to sign in to Computer1 and deleted some files.

You need to ensure that the identity used by Application1 cannot be used by a user to sign in to sign in to the desktop on Computer1. The solution must use the principle of least privilege.

Solution: On Computer1, you configure Application1 to sign in as the LocalSystem account and select the Allow service to interact with desktop check box. You delete the Service1 account.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
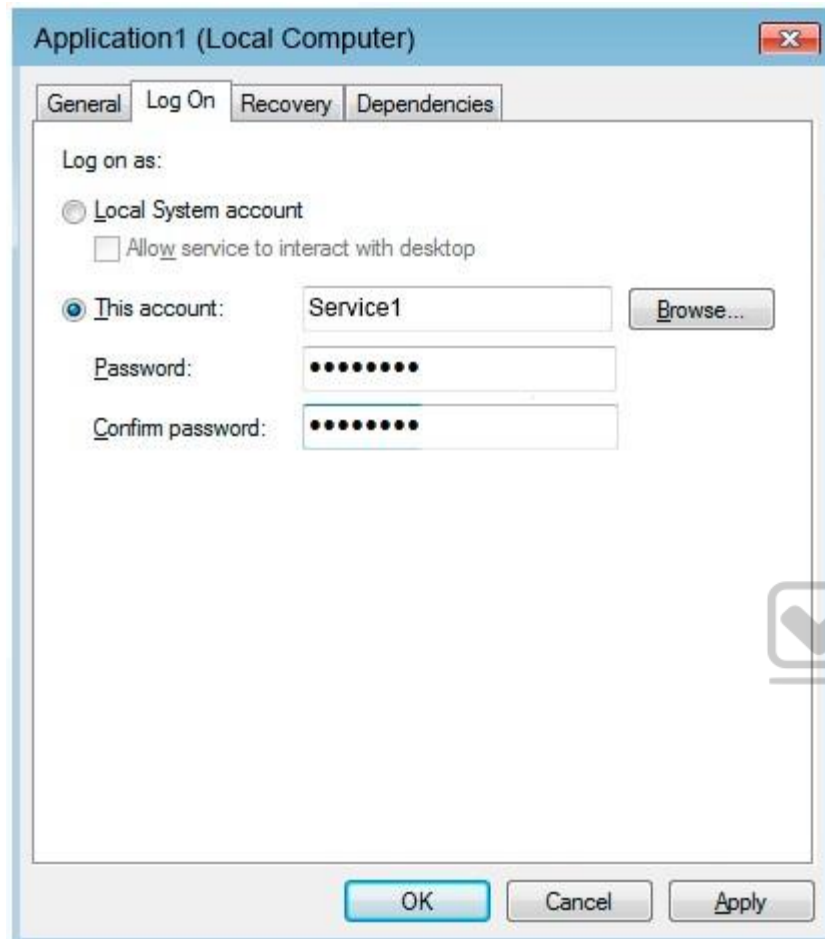**Explanation**

**Explanation/Reference:**

**QUESTION 3**
**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

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

You have a computer named Computer1 that runs Windows 10.

A service named Application1 is configured as shown in the exhibit.

Application1 (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

○ Local System account
  ☐ Allow service to interact with desktop

● This account:    Service1        [ Browse... ]

  Password:        ••••••••

  Confirm password: ••••••••

[ OK ]  [ Cancel ]  [ Apply ]

You discover that a user used the Service1 account to sign in to Computer1 and deleted some files.

You need to ensure that the identity used by Application1 cannot be used by a user to sign in to sign in to the desktop on Computer1. The solution must use the principle of least privilege.

Solution: On Computer1, you assign Service1 the deny log on locally user right.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally
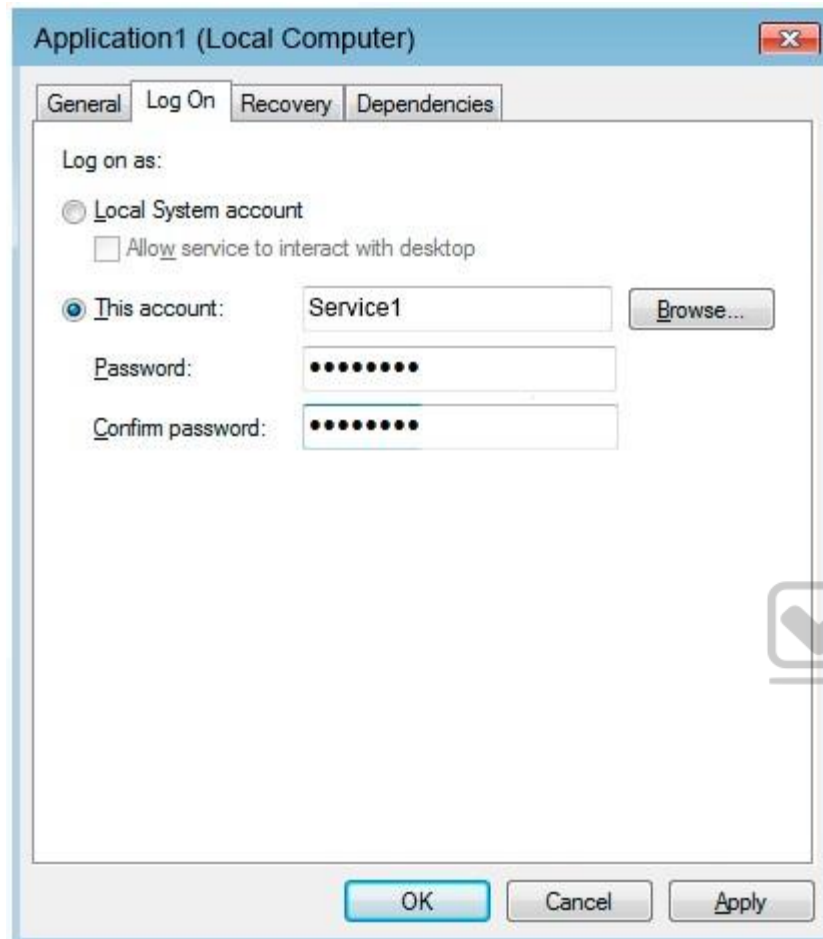
**QUESTION 4**
**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

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

You have a computer named Computer1 that runs Windows 10.

A service named Application1 is configured as shown in the exhibit.

**Application1 (Local Computer)**

General | Log On | Recovery | Dependencies

Log on as:

○ Local System account
  ☐ Allow service to interact with desktop

● This account:    Service1                    Browse...

  Password:        ••••••••

  Confirm password: ••••••••

[ OK ]    [ Cancel ]    [ Apply ]

You discover that a user used the Service1 account to sign in to Computer1 and deleted some files.

You need to ensure that the identity used by Application1 cannot be used by a user to sign in to sign in to the desktop on Computer1. The solution must use the principle of least privilege.

Solution: On Computer1, you assign Service1 the deny log on as a service user right.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-as-a-service

**QUESTION 5**
You have a Microsoft Azure Active Directory (Azure AD) tenant.

Some users sign in to their computer by using Windows Hello for Business.

A user named User1 purchases a new computer and joins the computer to Azure AD.

User1 attempts to configure the sign-in options and receives the error message shown in the exhibit.

**Sign-in options**

*Some settings are hidden or managed by your organization.

**Windows Hello**

Sign in to Windows, apps and services by teaching
Windows to recognize you.

Windows Hello isn't available on this device.

See how it works and find compatible devices.

You open **Device Manager** and confirm that all the hardware works correctly.

You need to ensure that User1 can use Windows Hello for Business facial recognition to sign in to the computer.

What should you do first?

A. Purchase an infrared (IR) camera.
B. Upgrade the computer to Windows 10 Enterprise.
C. Enable UEFI Secure Boot.
D. Install a virtual TPM driver.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-planning-guide

**QUESTION 6**
Your company uses Microsoft Deployment Toolkit (MDT) to deploy Windows 10 to new computers.

The company purchases 1,000 new computers.

You need to ensure that the Hyper-V feature is enabled on the computers during the deployment.

What are two possible ways to achieve the goal? Each correct answer presents part of the solution.

**NOTE:** Each correct selection is worth one point.

A. Add a task sequence step that adds a provisioning package.
B. In a Group Policy object (GPO), from Computer Configuration, configure Application Control Policies.
C. Add a custom command to the Unattend.xml file.
D. Add a configuration setting to Windows Deployment Services (WDS).
E. Add a task sequence step that runs `dism.exe`.

**Correct Answer:** AC
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-image **Testlet 1**

**Case Study**

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

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

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

**To start the case study**
To display the first question in this case study, click the Next **button**. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the **Question** button to return to the question.

**Overview**

**Existing Environment**

Fabrikam, Inc. is a distribution company that has 500 employees and 100 contractors.

**Active Directory**

The network contains an Active Directory forest named fabrikam.com. The forest is synced to Microsoft Azure Active Directory (Azure AD). All the employees are assigned Microsoft 365 E3 licenses.

The domain contains a user account for an employee named User10.

**Client Computers**

All the employees have computers that run Windows 10 Enterprise. All the computers are installed without Volume License Keys. Windows 10 license keys are never issued.

All the employees register their computer to Azure AD when they first receive the computer.

User10 has a computer named Computer10.

All the contractors have their own computer that runs Windows 10. None of the computers are joined to Azure AD.

**Operational Procedures**

Fabrikam has the following operational procedures:

▪ Updates are deployed by using Windows Update for Business.
▪ When new contractors are hired, administrators must help the contactors configure the following settings on their computer:
- User certificates
- Browser security and proxy settings
- Wireless network connection settings

## Security policies

The following security policies are enforced on all the client computers in the domain:

▪ All the computers are encrypted by using BitLocker Drive Encryption (BitLocker). BitLocker recovery information is stored in Active Directory and Azure AD.
▪ The local Administrators group on each computer contains an enabled account named LocalAdmin. ▪
The LocalAdmin account is managed by using Local Administrator Password Solution (LAPS).

## Problem Statements

Fabrikam identifies the following issues:

▪ Employees in the finance department use an application named Application1. Application1 frequently crashes due to a memory error. When Application1 crashes, an event is written to the application log and an administrator runs a script to delete the temporary files and restart the application.
▪ When employees attempt to connect to the network from their home computer, they often cannot establish a VPN connection because of misconfigured VPN settings.
▪ An employee has a computer named Computer11. Computer11 has a hardware failure that prevents the computer from connecting to the network. ▪
User10 reports that Computer10 is not activated.

## Technical requirements

Fabrikam identifies the following technical requirements for managing the client computers:

▪ Provide employees with a configuration file to configure their VPN connection.
▪ Use the minimum amount of administrative effort to implement the technical requirements.
▪ Identify which employees' computers are noncompliant with the Windows Update baseline of the company.
▪ Ensure that the service desk uses Quick Assist to take remote control of an employee's desktop during support calls.
▪ Automate the configuration of the contractors' computers. The solution must provide a configuration file that the contractors can open from a Microsoft SharePoint site to apply the required configurations.

## QUESTION 1
You need to sign in as LocalAdmin on Computer11.

What should you do first?

A. From the LAPS UI tool, view the administrator account password for the computer object of Computer11.
B. From Local Security Policy, edit the policy password settings on Computer11.
C. From the LAPS UI tool, reset the administrator account password for the computer object of Computer11.
D. From Microsoft Intune, edit the policy password settings on Computer11.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://technet.microsoft.com/en-us/mt227395.aspx

**QUESTION 2**
An employee reports that she must perform a BitLocker recovery on her laptop. The employee does not have her BitLocker recovery key but does have a Windows 10 desktop computer.

What should you instruct the employee to do from the desktop computer?

A. Run the `manage-bde.exe –status` command
B. From BitLocker Recovery Password Viewer, view the computer object of the laptop
C. Go to https://account.activedirectory.windowsazure.com and view the user account profile
D. Run the `Enable-BitLockerAutoUnlock` cmdlet

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://celedonpartners.com/blog/storing-recovering-bitlocker-keys-azure-active-directory/

**Question Set 2**

**QUESTION 1**

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

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

You have a computer named Computer1 that runs Windows 10. The computer contains a folder. The folder contains sensitive data.

You need to log which user reads the contents of the folder and modifies and deletes files in the folder.

Solution: From the properties of the folder, you configure the **Auditing** settings and from the Audit Policy in the local Group Policy, you configure Audit directory service access.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://www.netwrix.com/how_to_detect_who_changed_file_or_folder_owner.html

**QUESTION 2**
Your network contains an Active Directory domain. The domain contains 1,000 computers that run Windows 10.

You discover that when users are on their lock screen, they see a different background image every day, along with tips for using different features in Windows 10.

You need to disable the tips and the daily background image for all the Windows 10 computers.

Which Group Policy settings should you modify?

A. Turn off the Windows Welcome Experience
B. Turn off Windows Spotlight on Settings
C. Do not suggest third-party content in Windows spotlight

D. Turn off all Windows spotlight features

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows/configuration/windows-spotlight

**QUESTION 3**
You have a file named Reg1.reg that contains the following content.

```
Windows Registry Editor Version 5.00


[HKEY_CLASSES_ROOT\Directory\Background\shell\Notepad]


[HKEY_CLASSES_ROOT\Directory\Background\shell\Notepad\command]

@="notepad.exe"
```

What is the effect of importing the file?

A. A key named command will be renamed as **notepad.exe**.

B. In a key named Notepad, the command value will be set to **@="notepad.exe"**.

C. In a key named command, the default value will be set to **notepad.exe**.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
You have a computer named Computer1 that runs Windows 10.

On Computer1, you create the local users shown in the following table.

| Name | Member of |
|-------|-----------|
| User1 | Users |
| User2 | Users, Guests |
| User3 | Power Users, Guest |
| User4 | Guests, Users, Administrators |
| User5 | Users, Distributed COM Users |

Which three user profiles will persist after each user signs out? Each correct answer presents part of the solution.

**NOTE:** Each correct selection is worth one point.

A. User1
B. User2
C. User3
D. User4
E. User5

**Correct Answer:** ADE
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
You have 20 computers that run Windows 10. The computers are in a workgroup.

You need to create a local user named Admin1 on all the computers. Admin1 must be a member of the Remote Management Users group.

What should you do?

A. From Windows Configuration Designer, create a provisioning package, and then run the provisioning package on each computer.
B. Create a script that runs the **New-ADUser** cmdlet and the **Set-AdGroup** cmdlet.
C. Create a Group Policy object (GPO) that contains the Local User Group Policy preference.
D. Create a script that runs the **New-MsolUser** cmdlet and the **Add-ADComputerServiceAccount** cmdlet.

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://blogs.technet.microsoft.com/askpfeplat/2017/11/06/use-group-policy-preferences-to-manage-the-local-administrator-group/

**QUESTION 6**
You have several computers that run Windows 10. The computers are in a workgroup and have BitLocker Drive Encryption (BitLocker) enabled.

You join the computers to Microsoft Azure Active Directory (Azure AD).

You need to ensure that you can recover the BitLocker recovery key for the computers from Azure AD.

What should you do first?

A. Disable BitLocker.
B. Add a BitLocker key protector.
C. Suspend BitLocker.
D. Disable the TMP chip.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies#bitlocker-keyprotectors

**QUESTION 7**
HOTSPOT

You have a computer named Computer1 that runs Windows 10 and is joined to an Active Directory domain named adatum.com.

A user named Admin1 signs in to Computer1 and runs the whoami command as shown in the following exhibit.

```
Command Prompt                                          —    □    ×

c:\Users\admin1>whoami /user /groups /priv

USER INFORMATION
----------------

User Name        SID
================ =========================================
adatum\admin1    S-1-5-21-4534338-1127018997-2609994386-4602


GROUP INFORMATION
-----------------

Group Name                                      Type              SI
=============================================== ================= ===
Everyone                                        Well-known group  S-
BUILTIN\Users                                   Alias             S-
BUILTIN\Administrators                          Alias             S-
NT AUTHORITY\INTERACTIVE                        Well-known group  S-
CONSOLE LOGON                                   Well-known group  S-
NT AUTHORITY\Authenticated Users                Well-known group  S-
NT AUTHORITY\This Organization                  Well-known group  S-
LOCAL                                           Well-known group  S-
ADATUM\Domain Admins                            Group             S-
Authentication authority asserted identity      Well-known group  S-
ADATUM\Denied RODC Password Replication Group   Alias             S-
Mandatory Label\Medium Mandatory Level          Label             S-


Privilege Name              Description
=========================== ===============================
SeShutdownPrivilege         Shut down the system
SeChangeNotifyPrivilege     Bypass traverse checking
SeUndockPrivilege           Remove computer from docking statio
SeIncreaseWorkingSetPrivilege  Increase a process working set
SeTimeZonePrivilege         Change the time zone

C:\Users\admin1>
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

https://vceplus.com/

**NOTE:** Each correct selection is worth one point.

**Hot Area:**

Answer Area

On Computer1, if Admin attempts to open Device
Manager, [answer choice].

| ▼ |
|---|
| Admin1 will be prompted for credentials |
| Admin1 will be prompted for consent |
| Admin1 will be denied access |
| Device Manager will open without a prompt |

On Computer1, if Admin attempts to run the command
prompt as an administrator, [answer choice]

| ▼ |
|---|
| Admin1 will be prompted for credentials |
| Admin1 will be prompted for consent |
| Admin1 will be denied access |
| Device Manager will open without a prompt |

**Correct Answer:**

Answer Area

On Computer1, if Admin attempts to open Device
Manager, [answer choice].

| ▼ |
|---|
| Admin1 will be prompted for credentials |
| Admin1 will be prompted for consent |
| Admin1 will be denied access |
| **Device Manager will open without a prompt** |

On Computer1, if Admin attempts to run the command
prompt as an administrator, [answer choice]

| ▼ |
|---|
| Admin1 will be prompted for credentials |
| **Admin1 will be prompted for consent** |
| Admin1 will be denied access |
| Device Manager will open without a prompt |

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
You have a computer named Computer1 that runs Windows 10.

You need to configure User Account Control (UAC) to prompt administrators for their credentials.

Which settings should you modify?

A. Administrators Properties in Local Users and Groups
B. User Account Control Settings in Control Panel
C. Security Options in Local Group Policy Editor
D. User Rights Assignment in Local Group Policy Editor

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-security-policy-settings

**QUESTION 9**
You have several computers that run Windows 10. The computers are in a workgroup.

You need to prevent users from using Microsoft Store apps on their computer.

What are two possible ways to achieve the goal? Each correct answer presents part of the solution.

**NOTE:** Each correct selection is worth one point.

A. From Security Settings in the local Group Policy, configure **Security Options**.
B. From Administrative Templates in the local Group Policy, configure the **Store** settings.
C. From Security Settings in the local Group Policy, configure **Software Restriction Policies**.
D. From Security Settings in the local Group Policy, configure **Application Control Policies**.

**Correct Answer:** BD
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://www.techrepublic.com/article/how-to-manage-your-organizations-microsoft-store-group-policy/

**QUESTION 10**
You have a computer named Computer1 that runs Windows 10.

You need to prevent standard users from changing the wireless network settings on Computer1. The solution must allow administrators to modify the wireless network settings.

What should you use?

A. Windows Configuration Designer
B. MSConfig
C. Local Group Policy Editor
D. an MMC console that has the Group Policy Object Editor snap-in

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Your network contains an Active Directory domain named contoso.com. The domain contains named Computer1 that runs Windows 10.

On Computer1, you create an NTFS folder and assign Full control permissions to Everyone.

You share the folder as Share1 and assign the permissions shown in the following table.

| Name | Permission |
|------|-----------|
| User1 | Full control |
| User2 | Change |

When accessing Share1, which two actions can be performed by User1 but not by User2? Each correct answer presents part of the solution.

**NOTE:** Each correct selection is worth one point.

A. Delete a file created by another user.

B. Set the permissions for a file.
C. Rename a file created by another user.
D. Take ownership of file.
E. Copy a file created by another user to a subfolder.

**Correct Answer:** BD
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.varonis.com/blog/ntfs-permissions-vs-share/

**QUESTION 12**
**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

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

A user named User1 has a computer named Computer1 that runs Windows 10. Computer1 is joined to an Azure Active Directory (Azure AD) tenant named contoso.com. User1 joins Computer1 to contoso.com by using user1@contoso.com.

Computer1 contains a folder named Folder1. Folder1 is in drive C and is shared as Share1. Share1 has the permission shown in the following table.

| Group | Share permission |
|---|---|
| Everyone | Full control |
| AzureAD\user1@contoso.com | Owner |

A user named User2 has a computer named Computer2 that runs Windows 10. User2 joins Computer2 to contoso.com by using user2@contoso.com.

User2 attempts to access Share1 and receives the following error message: "The username or password is incorrect."

You need to ensure that User2 can connect to Share1.

Solution: In Azure AD, you create a group named Group1 that contains User1 and User2. You grant Group1 Change access to Share1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754178(v%3dws.10)

**QUESTION 13**
**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.**

A user named User2 has a computer named Computer2 that runs Windows 10. User2 joins Computer2 to contoso.com by using user2@contoso.com.

Computer1 contains a folder named Folder1. Folder1 is in drive C and is shared as Share1. Share1 has the permission shown in the following table.

| Group | Share permission |
|---|---|
| Everyone | Full control |
| AzureAD\user1@contoso.com | Owner |

A user named User2 has a computer named Computer2 that runs Windows 10. User2 joins Computer2 to contoso.com by using

user2@contoso.com. User2 attempts to access Share1 and receives the following error message: "The username or password is incorrect." You

need to ensure that User2 can connect to Share1.

Solution: You create a local user account on Computer1 and instruct User2 to use the local account to connect to Share1.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**


**QUESTION 14**
**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.**

A user named User1 has a computer named Computer1 that runs Windows 10. Computer1 is joined to an Azure Active Directory (Azure AD) tenant named contoso.com. User1 joins Computer1 to contoso.com by using user1@contoso.com.

Computer1 contains a folder named Folder1. Folder1 is in drive C and is shared as Share1. Share1 has the permission shown in the following table.

| Group | Share permission |
|---|---|
| Everyone | Full control |
| AzureAD\user1@contoso.com | Owner |

A user named User2 has a computer named Computer2 that runs Windows 10. User2 joins Computer2 to contoso.com by using user2@contoso.com.

User2 attempts to access Share1 and receives the following error message: "The username or password is incorrect."

You need to ensure that User2 can connect to Share1.

Solution: In Azure AD, you create a group named Group1 that contains User1 and User2. You grant Group1 Modify access to Folder1.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**

References:

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754178(v%3dws.10)

**QUESTION 15**
You have a computer named Computer1 that runs Windows 10. Computer1 contains a folder named Folder1.

You need to log any users who take ownership of the files in Folder1.

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

**NOTE:** Each correct selection is worth one point.

A. Modify the folder attributes of Folder1.
B. Modify the Advanced Security Settings for Folder1.
C. From a Group Policy object (GPO), configure the Audit Sensitive Privilege Use setting.
D. From a Group Policy object (GPO), configure the Audit File System setting.
E. Install the Remote Server Administration Tools (RSAT).

**Correct Answer:** BD
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://www.netwrix.com/how_to_detect_who_changed_file_or_folder_owner.html

**QUESTION 16**
You are a network administrator at your company.

The company uses an application that checks for network connectivity to a server by sending a ping request to the IPv6 address of the server replies, the application loads.

A user cannot open the application.

You manually send the ping request from the computer of the user and the server does not reply. You send the ping request from your computer and the server replies.

You need to ensure that the ping request works from the user's computer.

Which Windows Defender firewall rule is a possible cause of the issue?

A. File and Printer Sharing (NB-Datagram-In)
B. File and Printer Sharing (Echo request ICMPv6-Out)
C. File and Printer Sharing (NB-Datagram-Out)
D. File and Printer Sharing (Echo Request ICMPv6-In)

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.howtogeek.com/howto/windows-vista/allow-pings-icmp-echo-request-through-your-windows-vista-firewall/

**QUESTION 17**
Your network contains an Active Directory domain. The domain contains computers that run Windows 10.

You need to provide a user with the ability to remotely create and modify shares on the computers. The solution must use the principle of least privilege.

To which group should you add the user?

A. Power Users
B. Remote Management Users
C. Administrators
D. Network Configuration Operators

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**


**QUESTION 18**
You have a computer named Computer1 that runs Windows 10. Computer1 belongs to a workgroup.

You run the following commands on Computer1.

```
New-LocalUser –Name User1 –NoPassword
Add-LocalGroupMember User –Member User1
```
What is the effect of the configurations?

A. User1 is prevented from signing in until the user is assigned additional user rights.
B. User1 appears on the sign-in screen and can sign in without a password.
C. User1 is prevented from signing in until an administrator manually sets a password for the user.
D. User1 appears on the sign-in screen and must set a new password on the first sign-in attempts.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/new-localuser?view=powershell-5.1

**QUESTION 19**
You have a public computer named Computer1 that runs Windows 10/ Computer1 contains a folder named Folder1.

You need to provide a user named User1 with the ability to modify the permissions of Folder1. The solution must use the principle of least privilege.

Which NTFS permission should you assign to User1?

A. Full control
B. Modify
C. Write
D. Read & execute

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754344%28v%3dws.10%29 **Testlet 1**

**Case Study**

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

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

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

**To start the case study**
To display the first question in this case study, click the Next **button**. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the **Question** button to return to the question.

**Overview**

**Existing Environment**

Fabrikam, Inc. is a distribution company that has 500 employees and 100 contractors.

**Active Directory**

The network contains an Active Directory forest named fabrikam.com. The forest is synced to Microsoft Azure Active Directory (Azure AD). All the employees are assigned Microsoft 365 E3 licenses.

The domain contains a user account for an employee named User10.

**Client Computers**

All the employees have computers that run Windows 10 Enterprise. All the computers are installed without Volume License Keys. Windows 10 license keys are never issued.

All the employees register their computer to Azure AD when they first receive the computer.

User10 has a computer named Computer10.

All the contractors have their own computer that runs Windows 10. None of the computers are joined to Azure AD.

**Operational Procedures**

Fabrikam has the following operational procedures:

- Updates are deployed by using Windows Update for Business.
- When new contractors are hired, administrators must help the contactors configure the following settings on their computer:
- User certificates
- Browser security and proxy settings
- Wireless network connection settings

## Security policies

The following security policies are enforced on all the client computers in the domain:

- All the computers are encrypted by using BitLocker Drive Encryption (BitLocker). BitLocker recovery information is stored in Active Directory and Azure AD.
- The local Administrators group on each computer contains an enabled account named LocalAdmin. ▪
The LocalAdmin account is managed by using Local Administrator Password Solution (LAPS).

## Problem Statements

Fabrikam identifies the following issues:

- Employees in the finance department use an application named Application1. Application1 frequently crashes due to a memory error. When Application1 crashes, an event is written to the application log and an administrator runs a script to delete the temporary files and restart the application.
- When employees attempt to connect to the network from their home computer, they often cannot establish a VPN connection because of misconfigured VPN settings.
- An employee has a computer named Computer11. Computer11 has a hardware failure that prevents the computer from connecting to the network. ▪
User10 reports that Computer10 is not activated.

## Technical requirements

Fabrikam identifies the following technical requirements for managing the client computers:

- Provide employees with a configuration file to configure their VPN connection.
- Use the minimum amount of administrative effort to implement the technical requirements.
- Identify which employees' computers are noncompliant with the Windows Update baseline of the company.
- Ensure that the service desk uses Quick Assist to take remote control of an employee's desktop during support calls.
- Automate the configuration of the contractors' computers. The solution must provide a configuration file that the contractors can open from a Microsoft SharePoint site to apply the required configurations.

## QUESTION 1
You need to recommend a solution to configure the employee VPN connections.

What should you include in the recommendation?

A. Remote Access Management Console
B. Group Policy Management Console (GPMC)
C. Connection Manager Administration Kit (CMAK)
D. Microsoft Intune

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/vpn-deploy-client-vpn-connections#bkmk_ProfileXML

**QUESTION 2**
You need to take remote control of an employee's computer to troubleshoot an issue.

What should you send to the employee to initiate a remote session?

A. a numeric security code
B. a connection file
C. an Easy Connect request
D. a password

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://support.microsoft.com/en-us/help/4027243/windows-10-solve-pc-problems-with-quick-assist

**Question Set 2**

**QUESTION 1**
A user named User1 has a computer named Computer1 that runs Windows 10.

User1 connects to a Microsoft Azure virtual machine named VM1 by using Remote Desktop.

User1 creates a VPN connection to a partner organization.

When the VPN connection is established, User1 cannot connect to VM1. When User1 disconnects from the VPN, the user can connect to VM1.

You need to ensure that User1 can connect to VM1 while connected to the VPN.

What should you do?

A. From the proxy settings, add the IP address of VM1 to the bypass list to bypass the proxy.
B. From the properties of VPN1, clear the Use **default gateway on remote network** check box.
C. From the properties of the Remote Desktop connection to VM1, specify a Remote Desktop Gateway (RD Gateway).
D. From the properties of VPN1, configure a static default gateway address.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:** References: https://www.stevejenkins.com/blog/2010/01/using-the-local-default-gateway-with-a-windows-vpn-connection/

**QUESTION 2**
Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.

You enable Windows PowerShell remoting on the computers.

You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.

To which group should you add Admin1?

A. Access Control Assistance Operators
B. Power Users
C. Remote Desktop Users

D. Remote Management Users

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://4sysops.com/wiki/enable-powershell-remoting/

**QUESTION 3**
You have 200 computers that run Windows 10 and are joined to an Active Directory domain.

You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy.

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

**NOTE:** Each correct selection is worth one point.

A. Set the Startup Type of the Windows Remote Management (WS-Management) service to **Automatic**.
B. Enable the Windows Firewall: Allow inbound remote administration exception setting.
C. Enable the Allow remote server management through WinRM setting.
D. Enable the Windows Firewall: Allow inbound Remote Desktop exceptions setting.
E. Enable the Allow Remote Shell access setting.
F. Set the Startup Type of the Remote Registry service to **Automatic**.

**Correct Answer:** ACD
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: http://www.mustbegeek.com/how-to-enable-winrm-via-group-policy/

**QUESTION 4**
A user has a computer that runs Windows 10.

When the user connects the computer to the corporate network, the user cannot access the internal corporate servers. The user can access servers on the Internet.

You run the ipconfig command and receive the following output.

```
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Ethernet 1
Physical Address. . . . . . . . . : 00-50-B6-7B-E4-81
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::5d56:3419:e83b:3c46%17(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.0.121(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Wednesday, October 31, 2018 8:07:14 AM
Lease Expires . . . . . . . . . . : Wednesday, October 31, 2018 8:07:14 PM
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.2
DHCPv6 IAID . . . . . . . . . . . : 536891574
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-22-AC-5F-64-00-50-B6-7B-E4-81
DNS Servers . . . . . . . . . . . : 131.107.10.60
                                     192.168.0.3
NetBIOS over Tcpip. . . . . . . . : Enabled
```

You send a ping request and successfully ping the default gateway, the DNS servers, and the DHCP server.

Which configuration on the computer causes the issue?

A.  the DNS servers
B.  the IPv4 address
C.  the subnet mask
D.  the default gateway address

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
HOTSPOT

You have a computer that runs Windows 10.

From the Settings app, you view the connection properties shown in the following exhibit.

Network profile

⦿ Public

Your PC is hidden from other devices on the network and can't be used for printer and file sharing.

◯ Private

For a network you trust, such as at home or work. Your PC is discoverable and can be used for printer and file sharing if you set it up.

Configure firewall and security settings

Metered connection

If you have a limited data plan and want more control over data usage, make this connection a metered network. Some apps might work differently to reduce data usage when you're connected to this network.

Set as metered connection

⬤ On

Set a data limit to help control data usage on this network

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

**NOTE:** Each correct selection is worth one point.

**Hot Area:**

**Answer Area**

To enable Windows Remote Management
(WinRM), you must first **[answer choice]**.

| ▼ |
| --- |
| set the Network profile to Private |
| run winrm qc at the command prompt |
| turn off Metered connection |

To ensure that Microsoft OneDrive syncs, you
must first **[answer choice]**.

| ▼ |
| --- |
| set the Network profile to Private |
| run winrm qc at the command prompt |
| turn off Metered connection |

**Correct Answer:**

**Answer Area**

To enable Windows Remote Management
(WinRM), you must first **[answer choice]**.

| ▼ |
| --- |
| **set the Network profile to Private** |
| run winrm qc at the command prompt |
| turn off Metered connection |

To ensure that Microsoft OneDrive syncs, you
must first **[answer choice]**.

| ▼ |
| --- |
| set the Network profile to Private |
| run winrm qc at the command prompt |
| **turn off Metered connection** |

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
You have 15 computers that run Windows 10. Each computer has two network interfaces named Interface1 and Interface2.

You need to ensure that network traffic uses Interface1, unless Interface1 is unavailable.

What should you do?

A. Run the **Set-NetIPInterface –InterfaceAlias Interface1 –InterfaceMetric 1** command.
B. Run the **Set-NetAdapterBinding –Name Interface2 –Enabled $true –ComponentID ms_tcpip –ThrottleLimit 0** command.
C. Set a static IP address on Interface 1.
D. From Network Connections in Control Pane, modify the Provider Order.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:

https://tradingtechnologies.atlassian.net/wiki/spaces/KB/pages/27439127/How+to+Change+Network+Adapter+Priorities+in+Windows+10

https://docs.microsoft.com/en-us/powershell/module/nettcpip/set-netipinterface?view=win10-ps

**QUESTION 7**
Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 10. Users in the finance department use the computers.

You have a computer named Computer1 that runs Windows 10.

From Computer1, you plan to run a script that executes Windows PowerShell commands on the finance department computers.

You need to ensure that you can run the PowerShell commands on the finance department from Computer1.

What should you do on the finance department computers?

A. From the local Group Policy, enable the **Allow Remote Shell Access** setting.
B. From the local Group Policy, enable the **Turn on Script Execution** setting.
C. From the Windows PowerShell, run the **Enable-MMAgent** cmdlet.
D. From the Windows PowerShell, run the **Enable-PSRemoting** cmdlet.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-6

**QUESTION 8**
You have an Azure Active Directory (Azure AD) tenant that contains a user named user1@contoso.com.

You have a computer named Computer1 that runs Windows 10.

You join Computer1 to Azure AD. You enable Remote Desktop on Computer1.

User1@contoso.com attempts to connect to Computer1 by using Remote Desktop and receives the following error message: "The logon attempt failed."

You need to ensure that the user can connect to Computer1 by using Remote Desktop.

What should you do first?

A. In Azure AD, assign user1@contoso.com the Cloud device administrator role.
B. From the local Group Policy, modify the Allow log on through Remote Desktop Services user right.
C. In Azure AD, assign user1@contoso.com the Security administrator role.
D. On Computer1, create a local user and add the new user to the Remote Desktop Users group.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-through-remote-desktop-services

**Testlet 1**

**Case Study**

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

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

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

**To start the case study**
To display the first question in this case study, click the Next **button**. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the **Question** button to return to the question.

**Overview**

**Existing Environment**

Fabrikam, Inc. is a distribution company that has 500 employees and 100 contractors.

**Active Directory**

The network contains an Active Directory forest named fabrikam.com. The forest is synced to Microsoft Azure Active Directory (Azure AD). All the employees are assigned Microsoft 365 E3 licenses.

The domain contains a user account for an employee named User10.

**Client Computers**

All the employees have computers that run Windows 10 Enterprise. All the computers are installed without Volume License Keys. Windows 10 license keys are never issued.

All the employees register their computer to Azure AD when they first receive the computer.

User10 has a computer named Computer10.

All the contractors have their own computer that runs Windows 10. None of the computers are joined to Azure AD.

**Operational Procedures**

Fabrikam has the following operational procedures:

▪ Updates are deployed by using Windows Update for Business.

- When new contractors are hired, administrators must help the contactors configure the following settings on their computer:
- User certificates
- Browser security and proxy settings
- Wireless network connection settings

## Security policies

The following security policies are enforced on all the client computers in the domain:

- All the computers are encrypted by using BitLocker Drive Encryption (BitLocker). BitLocker recovery information is stored in Active Directory and Azure AD.
- The local Administrators group on each computer contains an enabled account named LocalAdmin.
The LocalAdmin account is managed by using Local Administrator Password Solution (LAPS).

## Problem Statements

Fabrikam identifies the following issues:

- Employees in the finance department use an application named Application1. Application1 frequently crashes due to a memory error. When Application1 crashes, an event is written to the application log and an administrator runs a script to delete the temporary files and restart the application.
- When employees attempt to connect to the network from their home computer, they often cannot establish a VPN connection because of misconfigured VPN settings.
- An employee has a computer named Computer11. Computer11 has a hardware failure that prevents the computer from connecting to the network.
User10 reports that Computer10 is not activated.

## Technical requirements

Fabrikam identifies the following technical requirements for managing the client computers:

Provide employees with a configuration file to configure their VPN connection.
- Use the minimum amount of administrative effort to implement the technical requirements.
- Identify which employees' computers are noncompliant with the Windows Update baseline of the company.
- Ensure that the service desk uses Quick Assist to take remote control of an employee's desktop during support calls.
- Automate the configuration of the contractors' computers. The solution must provide a configuration file that the contractors can open from a Microsoft SharePoint site to apply the required configurations.

## QUESTION 1
You need to recommend a solution to monitor update deployments.

What should you include in the recommendation?

A. Windows Server Update (WSUS)
B. the Update Management solution in Azure Automation
C. the Update Compliance solution in Azure Log Analytics
D. the Azure Security Center

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-monitor

**Question Set 2**

**QUESTION 1**
You have 20 computers that run Windows 10.

You configure all the computers to forward all the events from all the logs to a computer named Computer1 that runs Windows 10.

When you sign in to Computer1, you cannot see any security events from other computers. You can see all the other forwarded events from the other computers.

You need to ensure that the security events are forwarded to Computer1.

What should you do?

A. On each computer, run **wecutil ac /q**.
B. On each computer, add the NETWORK SERVICE account to the Event Log Readers group.
C. On each computer, run **winrm qc –q**.
D. On Computer1, add the account of Computer1 to the Event Log Readers group.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

**QUESTION 2**
You have a computer that runs Windows 10.

You discover that Windows updates are failing to install on the computer.

You need to generate a log file that contains detailed information about the failures.

Which cmdlet should you run?

A. **Get–LogProperties**
B. **Get–WindowsErrorReporting**
C. **Get–WindowsUpdateLog**

D. **Get–WinEvent**
**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/powershell/module/windowsupdate/get-windowsupdatelog?view=win10-ps

**QUESTION 3**
You have a computer that runs Windows 10.

You can start the computer but cannot sign in.

You need to start the computer into the Windows Recovery Environment (WinRE).

What should you do?

A. Turn off the computer. Turn on the computer, and then press **F8**.
B. Turn off the computer. Turn on the computer, and then press **F10**.
C. From the sign-in screen, hold the Shift key, and then click **Restart**.
D. Hold **Alt**+**Ctrl**+**Delete** for 10 seconds.

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-recovery-environment--windows-re--technical-reference

**QUESTION 4**
HOTSPOT

You are a network administrator at your company.

A user attempts to start a computer and receives the following error message: "Bootmgr is missing."

You need to resolve the issue.

You start the computer in the recovery mode.

Which command should you run next? To answer, select the appropriate options in the answer area.

**NOTE:** Each correct selection is worth one point.

**Hot Area:**

**Answer Area**

| Bootrec | | /FixMbr |
|---|---|---|
| Diskpart | | /RebuildBcd |
| Sfc | | /ScanNow |
| | | /offbootdir |

**Correct Answer:**

**Answer Area**

| **Bootrec** | | /FixMbr |
|---|---|---|
| Diskpart | | **/RebuildBcd** |
| Sfc | | /ScanNow |
| | | /offbootdir |

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://neosmart.net/wiki/bootmgr-is-missing/

**QUESTION 5**
Your company purchases 20 laptops that use a new hardware platform.

In a test environment, you deploy Windows 10 to the new laptops.

Some laptops frequently generate stop errors.

You need to identify the cause of the issue.

What should you use?

A.  Reliability Monitor
B.  Task Manager
C.  System Configuration
D.  Performance Monitor

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://lifehacker.com/how-to-troubleshoot-windows-10-with-reliability-monitor-1745624446
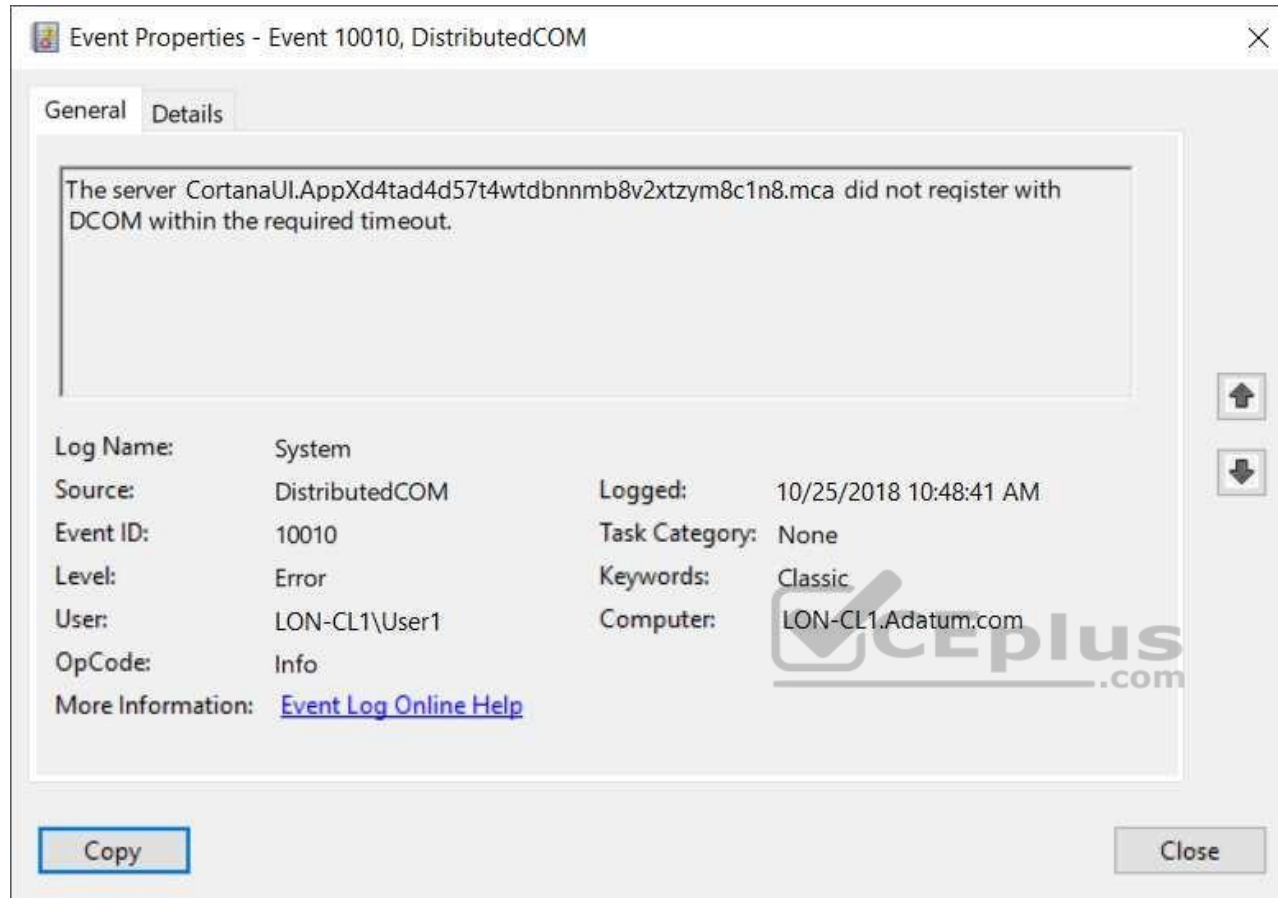
**QUESTION 6**
You have a computer named LON-CL1.Adatum.com that runs Windows 10.

From Event Viewer, you create a custom view named View1 that has the following filter:

▪ User: User1
▪ Logged: Any time
▪ Event logs: System
▪ Computer: LON-CL1
▪ Event IDs: 10000 – 11000
▪ Event level: Error, Verbose

You open **Event Viewer** and discover the event shown in the exhibit. (Click the **Exhibit** tab.)

Event Properties - Event 10010, DistributedCOM                    ✕

General  Details

The server CortanaUI.AppXd4tad4d57t4wtdbnnmb8v2xtzym8c1n8.mca did not register with
DCOM within the required timeout.

⬆

⬇

Log Name:        System
Source:          DistributedCOM        Logged:         10/25/2018 10:48:41 AM
Event ID:        10010                 Task Category:  None
Level:           Error                 Keywords:       Classic
User:            LON-CL1\User1         Computer:       LON-CL1.Adatum.com
OpCode:          Info
More Information:  Event Log Online Help

Copy                                                        Close

The event does not appear in View1.

You need to ensure that the event appears in View1.

What should you do?

A.  Add a Task Category setting to the filter.
B.  Add the computer account to the Event Log Readers group.
C.  Create an event subscription.

D. Modify the Computer setting in the filter.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.techrepublic.com/article/how-to-use-custom-views-in-windows-10s-event-viewer/

**QUESTION 7**
You have a computer named Computer1 that runs Windows 10 and has an application named App1.

You need to use Performance Monitor to collect data about the processor utilization of App1.

Which performance object should you monitor?

A. Process
B. Processor Performance
C. Processor Information
D. Processor

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.cse.wustl.edu/~jain/cse567-06/ftp/os_monitors/index.html

**QUESTION 8**
Your company has a main office and a branch office. The offices connect to each other by using a WAN link. Access to the Internet is provided through the main office.

The branch office contains 25 computers that run Windows 10. The computers contain small hard drives that have very little free disk space.

You need to prevent the computers in the branch office from downloading updates from peers on the network.

What should you do?

A. From the Settings app, modify the Delivery Optimizations settings.

B. Configure the network connections as metered connections.
C. Configure the computers to use BranchCache in hosted cache mode.
D. Configure the updates to use the Semi-Annual Channel (Targeted) channel.

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:** References: https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache

**QUESTION 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 manage devices that run Windows 10.

Ten sales users will travel to a location that has limited bandwidth that is expensive. The sales users will be at the location for three weeks.

You need to prevent all Windows updates from downloading for the duration of the trip. The solution must not prevent access to email and the Internet.

Solution: From Update & Security in the Settings app, you turn on Pause Updates.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.makeuseof.com/tag/5-ways-temporarily-turn-off-windows-update-windows-10/

**QUESTION 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 manage devices that run Windows 10.

Ten sales users will travel to a location that has limited bandwidth that is expensive. The sales users will be at the location for three weeks.

You need to prevent all Windows updates from downloading for the duration of the trip. The solution must not prevent access to email and the Internet.

Solution: From Network & Internet in the Settings app, you set the network connections as metered connections.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.makeuseof.com/tag/5-ways-temporarily-turn-off-windows-update-windows-10/

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

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

You manage devices that run Windows 10.

Ten sales users will travel to a location that has limited bandwidth that is expensive. The sales users will be at the location for three weeks.

You need to prevent all Windows updates from downloading for the duration of the trip. The solution must not prevent access to email and the Internet.

Solution: From Network & Internet in the Settings app, you set a data limit.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

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

You have a computer named Computer1 that runs Windows 10.

You test Windows updates on Computer1 before you make the updates available to other computers.

You install a quality update that conflicts with a customer device driver.

You need to remove the update from Computer1.

Solution: From an elevated command prompt, you run the `vmic qfe delete` command.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
You have a computer that runs Windows 10 and has BitLocker Drive Encryption (BitLocker) enabled on all volumes.

You start the computer from Windows Recovery Environment (WinRE).

You need to read the data on the system drive.

What should you do?

A. Run `cipher.exe` and specify the `/rekey` parameter
B. Run `cipher.exe` and specify the `/adduser` parameter
C. Run `manange-bde.exe` and specify the `-off` parameter
D. Run `manage-bde.exe` and specify the `-unlock` parameter

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References: https://www.repairwin.com/how-to-disable-bitlocker-in-windows-recovery-environment-winre/



https://vceplus.com/