Windows 10 v1.0 (MD-100) - Full Access

Question 1 (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.

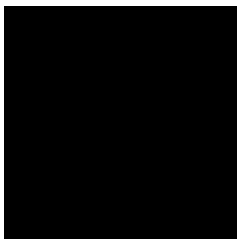
Operational Procedures -
Fabrikam has the following operational procedures:
Updates are deployed by using Windows Update for Business.
When new contractors are hired, administrators must help the contactors configure the following settings on their computer:
- User certificates
- Browser security and 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.

HOTSPOT -
You need to implement a solution to configure the contractors"™ computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Tool to use:
- Microsoft Deployment Toolkit (MDT)
- Windows AutoPilot
- Windows Configuration Designer
- Windows Deployment Services (WDS)

File type to create:
- CAB
- PPKG
- WIM
- XML

Answer :

Answer Area

Tool to use: Windows Configuration Designer

File type to create: PPKG

Explanation:
The requirement states: 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.

contractors can open from a Microsoft SharePoint site to apply the required configurations.
The "~configuration file"™ in this case is known as a "~provisioning package"™.
A provisioning package (.ppkg) is a container for a collection of configuration settings. With Windows 10, you can create provisioning packages that let you quickly and efficiently configure a device without having to install a new image.

The tool for creating provisioning packages is renamed Windows Configuration Designer, replacing the Windows Imaging and Configuration Designer (ICD) tool.
References:
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-install-icd https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

Question 2 (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

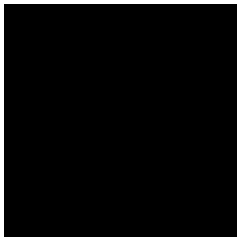
Security policies -
The following security policies are enforced on all the client computers in the domain:
All the computers are encrypted by using BitLocker Drive Encryption (BitLocker). BitLocker recovery information is stored in Active Directory and Azure AD.
The local Administrators group on each 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

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.

You need to ensure that User10 can activate Computer10.
What should you do?

A. Request that a Windows 10 Enterprise license be assigned to User10, and then activate Computer10.
B. From the Microsoft Deployment Toolkit (MDT), add a Volume License Key to a task sequence, and then redeploy Computer10.
C. From System Properties on Computer10, enter a Volume License Key, and then activate Computer10.
D. Request that User10 perform a local AutoPilot Reset on Computer10, and then activate Computer10.

Answer : D

Explanation:
The case study states: User10 reports that Computer10 is not activated.
The solution is to perform a local AutoPilot Reset on the computer. This will restore the computer settings to a fully-configured or known IT-approved state. When
User10 signs in to the computer after the reset, the computer should activate.
You can use Autopilot Reset to remove personal files, apps, and settings from your devices. The devices remain enrolled in Intune and are returned to a fully- configured or known IT-approved state. You can Autopilot Reset a device locally or remotely from the Intune for Education portal.
Incorrect Answers:
A: All users have Microsoft 365 E3 licenses. This license includes Windows 10 Enterprise so we don"™t need to assign a Windows 10 Enterprise license to User10.
B: Volume License Keys aren"™t required.
C: Volume License Keys aren"™t required.
References:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-requirements-licensing
https://docs.microsoft.com/en-us/intune-education/autopilot-reset

Deploy Windows -

Question 3 (Testlet 2)

Case Study -
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case 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 -
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
Contoso has IT, human resources (HR), and finance departments.
Contoso recently opened a new branch office in San Diego. All the users in the San Diego office work from home.

Existing environment -
Contoso uses Microsoft 365.
The on-premises network contains an Active Directory domain named contoso.com. The domain is synced to Microsoft Azure Active Directory (Azure AD).
All computers run Windows 10 Enterprise.
You have four computers named Computer1, Computer2, Computer3, and ComputerA. ComputerA is in a workgroup on an isolated network segment and runs the Long Term Servicing Channel version of Windows 10. ComputerA connects to a manufacturing system and is business critical. All the other computers are joined to the domain and run the Semi-Annual Channel version of Windows 10.
In the domain, you create four groups named Group1, Group2, Group3, and Group4.
Computer2 has the local Group Policy settings shown in the following table.

Policy	Security Setting
Access this computer from the network	Group1
Deny access to this computer from the network	Group2
Allow log on through Remote Desktop Services	Group3
Deny log on through Remote Desktop Services	Group4

The computers are updated by using Windows Update for Business.
The domain has the users shown in the following table.

Name	Member of
User1	Domain Admins, Domain Users
User2	Administrators, Domain Users
User3	Account Operators, Domain Users
User4	Domain Users
User5	Domain Users, Guests
User6	Group2, Group3, Domain Users

Computer1 has the local users shown in the following table.

Name	Member of
User11	Administrators
User12	Users
User13	Guests

Requirements -

Planned Changes -
Contoso plans to purchase computers preinstalled with Windows 10 Pro for all the San Diego office users.

Technical requirements -
Contoso identifies the following technical requirements:
The computers in the San Diego office must be upgraded automatically to Windows 10 Enterprise and must be joined to Azure AD the first time a user starts each new computer. End users must not be required to accept the End User License Agreement (EULA).
Helpdesk users must be able to troubleshoot Group Policy object (GPO) processing on the Windows 10 computers. The helpdesk users must be able to identify which Group Policies are applied to the computers

computers. The helpdesk users must be able to identify which Group Policies are applied to the computers.
Users in the HR department must be able to view the list of files in a folder named D:\Reports on Computer3.
ComputerA must be configured to have an Encrypting File System (EFS) recovery agent.

Quality update installations must be deferred as long as possible on ComputerA.
Users in the IT department must use dynamic lock on their primary device.
User6 must be able to connect to Computer2 by using Remote Desktop.
The principle of least privilege must be used whenever possible.
Administrative effort must be minimized whenever possible.
Kiosk (assigned access) must be configured on Computer1.

You need to meet the technical requirements for the San Diego office computers.
Which Windows 10 deployment method should you use?

A. wipe and load refresh
B. in-place upgrade
C. provisioning packages
D. Windows Autopilot

Answer : D

Explanation:
The requirement states: The computers in the San Diego office must be upgraded automatically to Windows 10 Enterprise and must be joined to Azure AD the first time a user starts each new computer. End users must not be required to accept the End User License Agreement (EULA).
Windows Autopilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. You can also use Windows
Autopilot to reset, repurpose and recover devices.
The OEM Windows 10 installation on the new computers can be transformed into a "business-ready" state, applying settings and policies, installing apps, and even changing the edition of Windows 10 being used (e.g. from Windows 10 Pro to Windows 10 Enterprise) to support advanced features.
The only interaction required from the end user is to connect to a network and to verify their credentials. Everything beyond that is automated.
References:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

---

Question 4 (Testlet 2)

Case Study -
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case 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 -
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
Contoso has IT, human resources (HR), and finance departments.
Contoso recently opened a new branch office in San Diego. All the users in the San Diego office work from home.

Existing environment -
Contoso uses Microsoft 365.
The on-premises network contains an Active Directory domain named contoso.com. The domain is synced to Microsoft Azure Active Directory (Azure AD).
All computers run Windows 10 Enterprise.
You have four computers named Computer1, Computer2, Computer3, and ComputerA. ComputerA is in a workgroup on an isolated network segment and runs the Long Term Servicing Channel version of Windows 10. ComputerA connects to a manufacturing system and is business critical. All the

and runs the Long Term Servicing Channel version of Windows 10. ComputerA connects to a manufacturing system and is business critical. All the other computers are joined to the domain and run the Semi-Annual Channel version of Windows 10.
In the domain, you create four groups named Group1, Group2, Group3, and Group4.
Computer2 has the local Group Policy settings shown in the following table.

Policy	Security Setting
Access this computer from the network	Group1
Deny access to this computer from the network	Group2
Allow log on through Remote Desktop Services	Group3
Deny log on through Remote Desktop Services	Group4

The computers are updated by using Windows Update for Business.
The domain has the users shown in the following table.

Name	Member of
User1	Domain Admins, Domain Users
User2	Administrators, Domain Users
User3	Account Operators, Domain Users
User4	Domain Users
User5	Domain Users, Guests
User6	Group2, Group3, Domain Users

Computer1 has the local users shown in the following table.

Name	Member of
User11	Administrators
User12	Users
User13	Guests

Requirements -

Planned Changes -
Contoso plans to purchase computers preinstalled with Windows 10 Pro for all the San Diego office users.

Technical requirements -
Contoso identifies the following technical requirements:
The computers in the San Diego office must be upgraded automatically to Windows 10 Enterprise and must be joined to Azure AD the first time a user starts each new computer. End users must not be required to accept the End User License Agreement (EULA).
Helpdesk users must be able to troubleshoot Group Policy object (GPO) processing on the Windows 10 computers. The helpdesk users must be able to identify which Group Policies are applied to the computers.
Users in the HR department must be able to view the list of files in a folder named D:\Reports on Computer3.
ComputerA must be configured to have an Encrypting File System (EFS) recovery agent.
Quality update installations must be deferred as long as possible on ComputerA.
Users in the IT department must use dynamic lock on their primary device.
User6 must be able to connect to Computer2 by using Remote Desktop.
The principle of least privilege must be used whenever possible.
Administrative effort must be minimized whenever possible.
Kiosk (assigned access) must be configured on Computer1.

HOTSPOT -
You need to meet the technical requirement for Computer1.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User who should configure Kiosk (assigned access): [▼]
- User1
- User2
- User3
- User11
- User12

Configure Kiosk (assigned access) for: [▼]
- User4
- User5
- User12
- User13

Answer :

Answer Area

User who should configure Kiosk (assigned access): [▼]
- User1
- User2
- User3
- **User11**
- User12

Configure Kiosk (assigned access) for: [▼]
- User4
- User5
- **User12**
- User13

Explanation:
The requirement states: Kiosk (assigned access) must be configured on Computer1.
Kiosk (assigned access) is a feature on Windows 10 that allows you to create a lockdown environment that lets users interact with only one app when they sign into a specified account. With Kiosk (assigned access), users won't be able to get to the desktop, Start menu, or any other app, including the Settings app.

Box 1: User 11 -
Kiosk (assigned access) must be configured by a user who is a member of the Local Administrators group on the Computer.
Box 2: User 12.
Kiosk (assigned access) must be configured for a user account that is a member of the Users group.
References:
https://www.windowscentral.com/how-set-assigned-access-windows-10

Deploy Windows -

Question 5 (Question Set 1)

Your company has an isolated network used for testing. The network contains 20 computers that run Windows 10. The computers are in a workgroup.
During testing, the computers must remain in the workgroup.
You discover that none of the computers are activated.
You need to recommend a solution to activate the computers without connecting the network to the Internet.
What should you include in the recommendation?

A. Volume Activation Management Tool (VAMT)
B. Key Management Service (KMS)
C. Active Directory-based activation
D. the Get-WindowsDeveloperLicense cmdlet

Answer : B

Explanation:
You can configure one of the computers as a Key Management Service (KMS) host and activate the KMS host by phone. The other computers in the isolated network can then activate using the KMS host.
Installing a KMS host key on a computer running Windows 10 allows you to activate other computers running Windows 10 against this KMS host and earlier versions of the client operating system, such as Windows 8.1 or Windows 7. Clients locate the KMS server by using resource records in DNS, so some configuration of DNS may be required. This scenario can be beneficial if your organization uses volume activation for clients and MAK-based activation for a smaller number of servers. To enable KMS functionality, a KMS key is installed on a KMS host; then, the host is activated over the Internet or by phone using
Microsoft"™s activation services.
References:
https://docs.microsoft.com/en-us/windows/deployment/volume-activation/activate-using-key-management-service-vamt

Question 6 (Question Set 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.

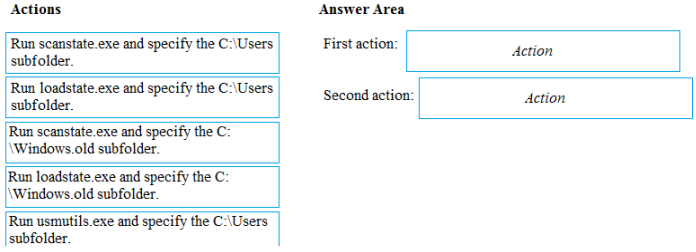
A. Windows 10 Pro in S mode
B. Windows 10 Home in S mode
C. Windows 10 Pro
D. Windows 10 Enterprise

Answer : A

Explanation:
Windows 10 in S mode is a version of Windows 10 that's streamlined for security and performance, while providing a familiar Windows experience. To increase security, it allows only apps from the Microsoft Store, and requires Microsoft Edge for safe browsing.
Azure AD Domain join is available for Windows 10 Pro in S mode and Windows 10 Enterprise in S mode. It's not available in Windows 10 Home in S mode.
References:
https://support.microsoft.com/en-gb/help/4020089/windows-10-in-s-mode-faq

Question 7 (Question Set 1)

DRAG DROP -
You have a computer named Computer1 that runs Windows 8.1. Computer1 has a local user named User1 who has a customized profile.
On Computer1, you perform a clean installation of Windows 10 without formatting the drives.
You need to migrate the settings of User1 from Windows 8.1 to Windows 10.
Which two actions should you perform? To answer, drag the appropriate actions to the correct targets. Each action 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:



Run usmutils.exe and specify the C:\Windows.old subfolder.

Answer :

Actions

- Run scanstate.exe and specify the C:\Users subfolder.
- Run loadstate.exe and specify the C:\Users subfolder.
- Run scanstate.exe and specify the C:\Windows.old subfolder.
- Run loadstate.exe and specify the C:\Windows.old subfolder.
- Run usmutils.exe and specify the C:\Users subfolder.
- Run usmutils.exe and specify the C:\Windows.old subfolder.

Answer Area

First action: Run scanstate.exe and specify the C:\Windows.old subfolder.

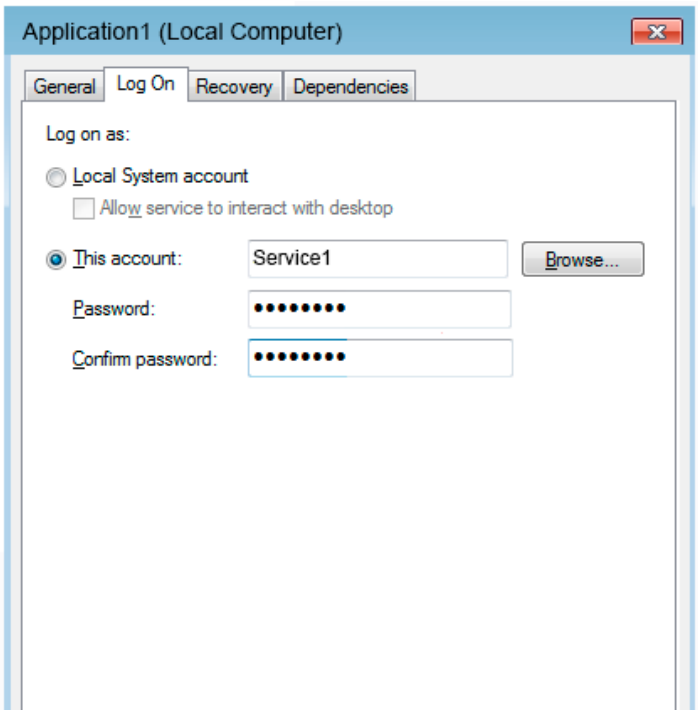
Second action: Run loadstate.exe and specify the C:\Users subfolder.

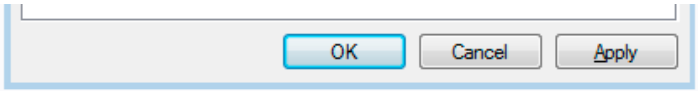
Explanation:
The User State Migration Tool (USMT) includes two tools that migrate settings and data: ScanState and LoadState. ScanState collects information from the source computer, and LoadState applies that information to the destination computer. In this case the source and destination will be the same computer.
As we have performed a clean installation of Windows 10 without formatting the drives, User1"™s customized Windows 8.1 user profile will be located in the
\Windows.old folder. Therefore, we need to run scanstate.exe on the \Windows.old folder.
User1"™s Windows 10 profile will be in the C:\Users folder so we need to run loadstate.exe to apply the changes in the C:\Users folder.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/usmt/offline-migration-reference https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-how-it-works https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-common-migration-scenarios#bkmk-fourpcrefresh

---

Question 8 (Question Set 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 Windows10.
A service named Application1 is configured as shown in the exhibit.





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

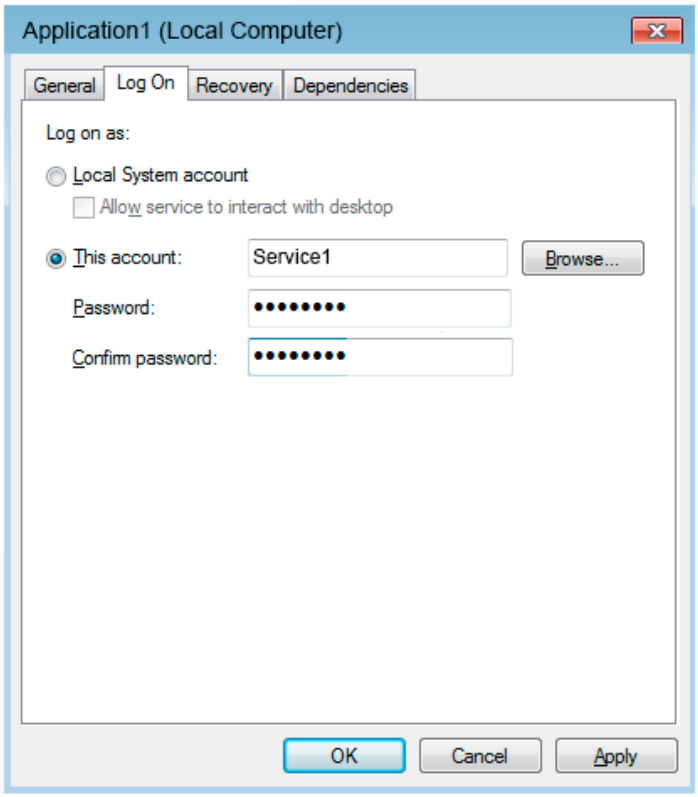
Answer : B

Explanation:
Configuring Application1 to sign in as the LocalSystem account would ensure that the identity used by Application1 cannot be used by a user to sign in to the desktop on Computer1. However, this does not use the principle of least privilege. The LocalSystem account has full access to the system. Therefore, this solution does not meet the goal.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally

---

Question 9 (Question Set 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.
A service named Application1 is configured as shown in the exhibit.



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

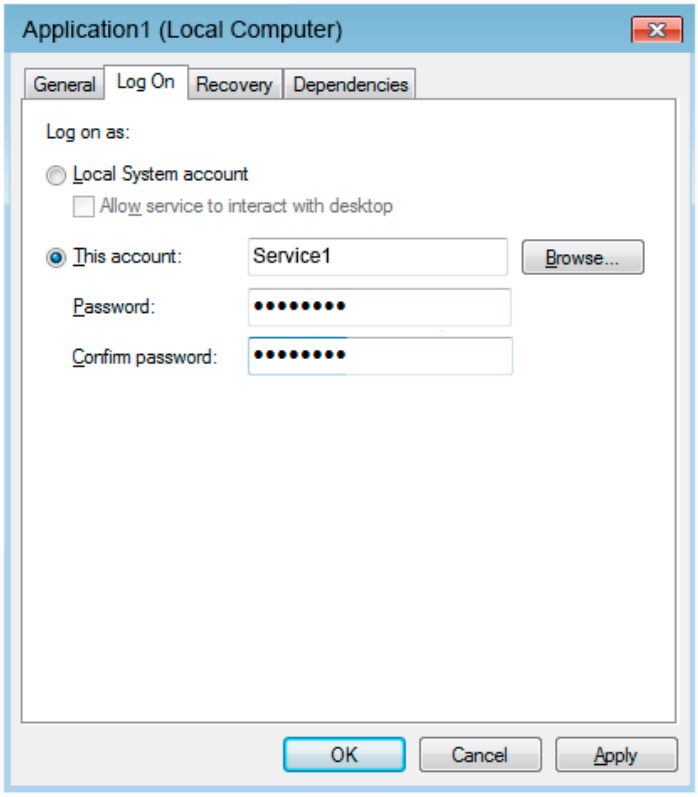
Answer : A

Explanation:
By using the Service1 account as the identity used by Application1, we are applying the principle of least privilege as required in this question.
However, the Service1 account could be used by a user to sign in to the desktop on the computer. To sign in to the desktop on the computer, an account needs the log on locally right which all user accounts have by default. Therefore, we can prevent this by assigning Service1 the deny log on locally user right.
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally

---

Question 10 (Question Set 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.
A service named Application1 is configured as shown in the exhibit.



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

Answer : B

Explanation:
A service account needs the log on as a service user right. When you assign an account to be used by a service, that account is granted the log on as a service user right. Therefore, assigning Service1 the deny log on as a service user right would mean the service would not function.
To sign in to the desktop on the computer, an account needs the log on locally right which all user accounts have by default. To meet the requirements of this question, we need to assign Service1 the deny log on locally user right, not the deny log on as a service user right.
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-as-a-service