QUESTION 281
Your network contains an Active Directory domain. All users have been issued with new computers that run Windows 10 Enterprise. All users have Microsoft 365 E3 licenses.
A user named Mia Hamm has an Active Directory user account named MHamm and a computer named Computer1.
Mia Hamm reports that Computer1 is not activated.
You need to ensure that Mia Hamm can activate Computer1.
What should you do?

A. Assign a Windows 10 Enterprise license to MHamm, and then activate Computer1.
B. From the Microsoft Deployment Toolkit (MDT), redeploy Computer1.
C. From System Properties on Computer1, enter a Volume License Key, and then activate Computer1.
D. Instruct Mia Hamm to perform a local AutoPilot Reset on Computer1, and then activate Computer1.

Answer: D
Explanation:
Mia Hamm reports that Computer1 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 the user signs in to Computer1 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 Mia Hamm.
B: Redeploying Computer1 is not required.
C: A Volume License Key is not required.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-requirements-licensing
https://docs.microsoft.com/en-us/intune-education/autopilot-reset

QUESTION 282
Your network contains an Active Directory domain that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.
The company plans to purchase computers preinstalled with Windows 10 Pro for all users.
The company the following requirements:
- The new computers must be upgraded to Windows 10 Enterprise automatically.

- The new computers must be joined to Azure AD automatically when the user starts the new computers for the first time.
- The users must not be required to accept the End User License Agreement (EULA).

You need to deploy the new computers.
What should you do?

A. Make use of the wipe and load refresh deployment method.
B. Perform in-place upgrade on the new computers.
C. Provide provisioning packages for the new computers.
D. Make use of Windows Autopilot.

Answer: D
Explanation:
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.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

QUESTION 283
Your company is not connected to the internet. The company purchases several new computers with Windows 10 Pro for its users.
None of the new computers are activated.
You need to activate the computers without connecting the network to the Internet.
What should you do?

A. Make use of the Volume Activation Management Tool (VAMT).
B. Make use of the Key Management Service (KMS).
C. Make use of the Windows Process Activation Service.
D. Run the Get-WmiObject -query 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.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/volume-activation/activate-using-key-management-service-vamt

QUESTION 284
Your network contains an Active Directory domain. All users have been issued with computers that run Windows 8.1.
A user named Mia Hamm has a computer named Computer1. You upgrade Computer1 to Windows 10 by performing a clean installation of Windows 10 without formatting the drives.
You need to migrate the settings for Mia Hamm from Windows 8.1 to Windows 10.
Which two actions should you perform?
NOTE: Each correct selection is worth one point.

A. Run scanstate.exe and specify the C:\Users folder

B. Run loadstate.exe and specify the C:\Windows.old folder
C. Run usmultils.exe and specify the C:\Users folder
D. Run scanstate.exe and specify the C:\Windows.old folder
E. Run loadstate.exe and specify the C:\Users folder
F. Run usmultils.exe and specify the C:\Windows.old folder

Answer: DE
Explanation:
D: As we have performed a clean installation of Windows 10 without formatting the drives, User1's 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.
E: 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/usmt-how-it-works
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-common-migration-scenarios#bkmk-fourpcrefresh

QUESTION 285
You have a computer named Computer1 that runs Windows 10.
You deploy an application named Application1 to Computer1.
You need to assign credentials to Application1.
You need to meet the following requirements:
Ensure that the credentials for Application1 cannot be used by any user to log on to Computer1. Ensure that the principle of least privilege is maintained.
What should you do?

A. Configure Application1 to sign in as the Local System account and select the Allow service to interact with desktop check box.
B. Create a user account for Application1 and assign that user account the Deny log on locally user right
C. Create a user account for Application1 and assign that user account the Deny log on as a service user right
D. Configure Application1 to sign in as the Local Service account and select the Allow service to interact with desktop check box.

Answer: B
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.
Incorrect Answers:
A: Configuring Application1 to sign in as the Local System 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 Local System account has full access to the system. Therefore, this solution does not meet the goal.
C: 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.
D: The Local Service Account is a predefined local account used by the service control manager.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally

QUESTION 286
Your network contains an Active Directory domain that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. All users have been issued with laptop computers as well as desktop computers that run Windows 10 Enterprise. All users have Microsoft 365 E3 licenses.
A user named Mia Hamm informs you that she must perform a BitLocker recovery on her laptop but she does not have

her BitLocker recovery key.
You need to ensure that Mia Hamm can perform a BitLocker recovery on her laptop.
What should you do?

A. Instruct Mia Hamm to log on to her desktop computer and run the repair-bde.exe command.
B. Instruct Mia Hamm to use the BitLocker Recovery Password Viewer to view the computer object of the laptop.
C. Instruct Mia Hamm to log on to her desktop computer and go to https://account.activedirectory.windowsazure.com and view the user account profile.
D. Instruct Mia Hamm to run the Enable-BitLocker cmdlet on her laptop.

Answer: C
Explanation:
The BitLocker recovery key is stored in Azure Active Directory.
Reference:
https://celedonpartners.com/blog/storing-recovering-bitlocker-keys-azure-active-directory/

QUESTION 287
Your company has an on-premises network that contains an Active Directory domain. The domain is synced to Microsoft Azure Active Directory (Azure AD). All computers in the domain run Windows 10 Enterprise.
You have a computer named Computer1 that has a folder named Folder1.
You must provide users in group named Group1 with the ability to view the list of files in Folder1. Your solution must ensure that the principle of least privilege is maintained.
What should you do?

A. Assign the Full control permissions for the Folder1 folder to Group1.
B. Assign the Read permissions for the Folder1 folder to Group1.
C. Assign the List folder permissions for the Folder1 folder to Group1.
D. Assign the Take ownership permissions for the Folder1 folder to Group1.

Answer: C
Explanation:
https://www.online-tech-tips.com/computer-tips/set-file-folder-permissions-windows/

QUESTION 288
You have a computer named Computer1 that runs Windows 10.
Computer1 has a folder named C:\Folder1.
You need to meet the following requirements:
- Log users that access C:\Folder1.
- Log users that modify and delete files in C:\Folder1.
Which two actions should you perform?

A. From the properties of C:\Folder1, configure the Auditing settings.
B. From the properties of C:\Folder1, select the Encryption contents to secure data option.
C. From the Audit Policy in the local Group Policy, configure Audit directory service access.
D. From the Audit Policy in the local Group Policy, you configure Audit object access.
E. From the Audit Policy in the local Group Policy, you configure Audit system events.

Answer: AD
Explanation:
Files and folders are objects and are audited through object access.
Reference:
https://www.netwrix.com/how_to_detect_who_changed_file_or_folder_owner.html

QUESTION 289
Your company has a computer named Computer1 that runs Windows 10. Computer1 is used to provide guests with

access to the Internet. Computer1 is a member of a workgroup.
You want to configure Computer1 to use a user account sign in automatically when the the computer is started. The user must not be prompted for a user name and password.
What should you do?

A. Configure Group Policy preferences.
B. Run the BCDBoot command.
C. Edit the Registry.
D. Run the MSConfig command.

Answer: C
Explanation:
In the registry, add a default user name and a default password in the HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon sbukey.
Reference:
https://support.microsoft.com/en-us/help/324737/how-to-turn-on-automatic-logon-in-windows

QUESTION 290
Your network contains an Active Directory domain. The domain contains computers that run Windows 10.
You must ensure that Windows BitLocker Drive Encryption is enabled on all client computers, even though a Trusted Platform Module (TPM) chip is installed in only some of them.
You need to accomplish this goal by using one Group Policy object (GPO).
What should you do?

A. Enable the Allow enhanced PINs for startup policy setting, and select the Allow BitLocker without a compatible TPM check box.
B. Enable the Enable use of BitLocker authentication requiring preboot keyboard input on slates policy setting, and select the Allow BitLocker without a compatible TPM check box.
C. Enable the Require additional authentication at startup policy setting, and select the Allow BitLocker without a compatible TPM check box.
D. Enable the Control use of BitLocker on removable drives policy setting, and select the Allow BitLocker without a compatible TPM check box.

Answer: C
Explanation:
We need to allow Windows BitLocker Drive Encryption on all client computers (including client computers that do not have Trusted Platform Module (TPM) chip).
We can do this by enabling the option to allow BitLocker without a compatible TPM in the group policy. The "Allow BitLocker without a compatible TPM" option is a checkbox in the "Require additional authentication at startup" group policy setting. To access the "Allow BitLocker without a compatible TPM" checkbox, you need to first select Enabled on the "Require additional authentication at startup" policy setting.
Reference:
https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings#bkmk-unlockpol4

QUESTION 291
You have a computer named Computer1. Computer1 runs Windows 10 Pro.
Computer1 is experiencing connectivity issues.
You need to view the IP addresses of any remote computer that Computer1 has an active TCP connection to.
Should you do?

A. In Windows Administrative Tools, open Performance Monitor.
B. In the Control Panel, open Network and Internet. Then select Network and Sharing Center.
C. In Windows Administrative Tools, open Resource Monitor.
D. In the Setting app, open Update and Security. Then open Windows Security and select Firewall and Network protection.

Answer: C

QUESTION 292
You have a computer named Computer1. Computer1 runs Windows 10 Pro.
You attempt to start Computer1 but you receive the following error message:
`Bootmgr is missing.`
You need to be able to start Computer1.
What should you do?

A. Start the computer in recovery mode and run the bootrec /rebuildbcd command.
B. Start the computer in recovery mode and run the diskpart /repair command.
C. Start the computer in recovery mode and run the bcdboot /s command.
D. Start the computer in recovery mode and run the bootcfg /debug command.

Answer: A
Explanation:
https://neosmart.net/wiki/bootmgr-is-missing/

QUESTION 293
Your company has several mobile devices that run Windows 10.
You need configure the mobile devices to meet the following requirements:
Windows updates may only be download when mobile devices are connect to Wi-Fi. Access to email and the Internet must be possible at all times.
What should you do?

A. Open the Setting app and select Update & Security.
Then select and configure Change active hours.
B. Open the Setting app and select Network & Internet.
Then select Change connection properties, and set the Metered connection option for cellular network connections to On.
C. Open the Setting app and select Network & Internet.
Then select Data Usage and set a data limit.
D. Open the Setting app and select Update & Security.
Then select and configure Delivery Optimization.

Answer: B
Explanation:
https://www.makeuseof.com/tag/5-ways-temporarily-turn-off-windows-update-windows-10/

QUESTION 294
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.
Your company has an on-premises network that contains an Active Directory domain. The domain is synced to Microsoft Azure Active Directory (Azure AD). All computers in the domain run Windows 10 Enterprise.
You have a computer named Computer1 that has a folder named C:\Folder1.
You want to use File History to protect C:\Folder1.
Solution: You enable File History on Computer1. You then enable archiving for Folder1.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
File History only backs up copies of files that are in Libraries, and Desktop folders and the OneDrive files available offline on your PC. If you have files or folders elsewhere that you want backed up, you can add them to one of these folders.
Reference:
https://support.microsoft.com/en-us/help/17128/windows-8-file-history