Microsoft

Exam Questions MD-102

Endpoint Administrator

NEW QUESTION 1
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune. You need to review the startup processes and how often each device restarts.
What should you use?

A. Endpoint analytics
B. Intune Data Warehouse
C. Azure Monitor
D. Device Management

Answer: B

NEW QUESTION 2
- (Exam Topic 4)
You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD).
The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements:
≫ The configuration must be managed from a central location.
≫ Internet traffic must be minimized.
≫ Costs must be minimized.
How should you configure Windows Update? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Windows Update technology to use:
- Windows Server Update Services (WSUS)
- Microsoft Endpoint Configuration Manager
- Windows Update for Business

Manage the configuration by using:
- A Group Policy object (GPO)
- Microsoft Endpoint Configuration Manager
- Microsoft Intune

Manage the traffic by using:
- Delivery Optimization
- BranchCache
- Peer cache

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Windows Server Update Services (WSUS)
Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.
Windows Server Update Services is a built-in server role that includes the following enhancements: Can be added and removed by using the Server Manager Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS Etc.
Box 2: A Group Policy object
In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).
Box 3: BranchCache
BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them. BranchCache has two operating modes: Distributed Cache mode and Hosted Cache mode.
Reference: https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-conf

NEW QUESTION 3
- (Exam Topic 4)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Enabled

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

You have a Conditional Access policy named CAPolicy1 that has the following settings:
• Assignments
o Users or workload identities: User 1. User1
o Cloud apps or actions: Office 365 Exchange Online o Conditions: Device platforms: Windows, iOS
• Access controls
o Grant Require multi-factor authentication
You have a Conditional Access policy named CAPolicy2 that has the following settings:
Assignments
o Users or workload identities: Used, User2 o Cloud apps or actions: Office 365 Exch
o Conditions
Device platforms: Android, iOS Filter for devices
Device matching the rule: Exclude filtered devices from policy Rule syntax: device. displayName- contains "1"
Access controls Grant Block access
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	⊙	⊙
If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	⊙	⊙
User2 can access Microsoft Exchange Online from Device2.	⊙	⊙

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screen shot of a computer Description automatically generated with low confidence

NEW QUESTION 4
- (Exam Topic 4)
You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

A. the Azure portal app
B. Endpoint analytics
C. the Company Portal app
D. Microsoft Power BI

Answer: D

Explanation:
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:
Devices Enrollment
App protection policy Compliance policy
Device configuration profiles Software updates
Device inventory logs
Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.

➢ Sign in to the Microsoft Endpoint Manager admin center.

➢ Select Reports > Intune Data warehouse > Data warehouse.

➢ Retrieve the custom feed URL from the reporting blade, for example:

➢ Open Power BI Desktop.

➢ Choose File > Get Data. Select OData feed.

➢ Choose Basic.

➢ Type or paste the OData URL into the URL box.

➢ Select OK.

➢ If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.

➢ Select Organizational account.

≫ Type your username and password.

≫ Select Sign In.

≫ Select Connect.

≫ Select Load.

Reference: https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

NEW QUESTION 5
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune.
You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to meet the following requirements during device provisioning:
• Display the progress of app and profile deployments.
• Join the devices to Azure AD.
What should you configure to meet each requirement? To answer drag the appropriate settings to the correct requirements. Each setting 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.

Settings

| CNAME Validation |
| Co-management Settings |
| Deployment Profiles |
| Enrollment notifications |
| Enrollment Status Page |

Answer Area

Display the progress of app and profile deployments: [   ]

Join the devices to Azure AD: [   ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Settings

| CNAME Validation |
| Co-management Settings |
| Deployment Profiles |
| Enrollment notifications |
| Enrollment Status Page |

Answer Area

Display the progress of app and profile deployments: [Enrollment Status Page]

Join the devices to Azure AD: [Deployment Profiles]

NEW QUESTION 6
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services {AD DS) domain that syncs with an Azure AD tenant by using Azure AD Connect.
You use Microsoft Intune and Configuration Manager to manage devices.
You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:
• Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.
• Devices for The sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to The homes of the sales department users.
• Administrative effort must be minimized.
Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Sales: [Windows Autopilot with automatic registration ▼]
- Configuration Manager
- **Windows Autopilot with automatic registration**
- Windows Autopilot with manual registration
- Windows Autopilot with OEM registration

Marketing: [Configuration Manager ▼]
- **Configuration Manager**
- Windows Autopilot with automatic registration
- Windows Autopilot with manual registration
- Windows Autopilot with OEM registration

A. Mastered

B. Not Mastered

Answer: A

Explanation:
Answer Area

Sales:	Windows Autopilot with automatic registration ⌄
	Configuration Manager
	Windows Autopilot with automatic registration
	Windows Autopilot with manual registration
	Windows Autopilot with OEM registration

Marketing:	Configuration Manager ⌄
	Configuration Manager
	Windows Autopilot with automatic registration
	Windows Autopilot with manual registration
	Windows Autopilot with OEM registration

NEW QUESTION 7
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have the Windows 11 devices shown in the following table.

Name	Member of	BitLocker Drive Encryption (BitLocker)
Device1	Group1	Enabled
Device2	Group1, Group3	Disabled
Device3	Group1, Group2	Enabled

You deploy the device compliance policy shown in the exhibit. (Click the Exhibit tab.)

Basics Edit

Name	Policy1
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings Edit

Device Health

| Require BitLocker | Require |

Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Scope tags Edit

Default

Assignments Edit

Included groups

Group
Group1
Group3

Excluded groups

Group
Group2

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

Answer Area

Statements	Yes	No
Device1 will have Policy1 assigned and will be marked as compliant.	○	○
Device2 will have Policy1 assigned and will be marked as compliant.	○	○
Device3 will have Policy1 assigned and will be marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 will have Policy1 assigned and will be marked as compliant.	⊙	○
Device2 will have Policy1 assigned and will be marked as compliant.	○	⊙
Device3 will have Policy1 assigned and will be marked as compliant.	○	⊙

NEW QUESTION 8
- (Exam Topic 4)
You have a Microsoft 365 subscription.
All users have Microsoft 365 apps deployed.
You need to configure Microsoft 365 apps to meet the following requirements:
• Enable the automatic installation of WebView2 Runtime.
• Prevent users from submitting feedback.
Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

```
☰

⌂  Home

♟  Servicing                        ⌃

   Monthly Enterprise          ✓

🖌  Customization                    ⌃

   Device Configuration

   Policy Management            ✓

   What's New Management        ⌃

💗  Health                           ⌃

   Apps Health

   Security Update Status

   OneDrive Sync        PREVIEW

   Service Health

▦  Inventory

📖  Learn More                       ⌄

⚙  Setup
```
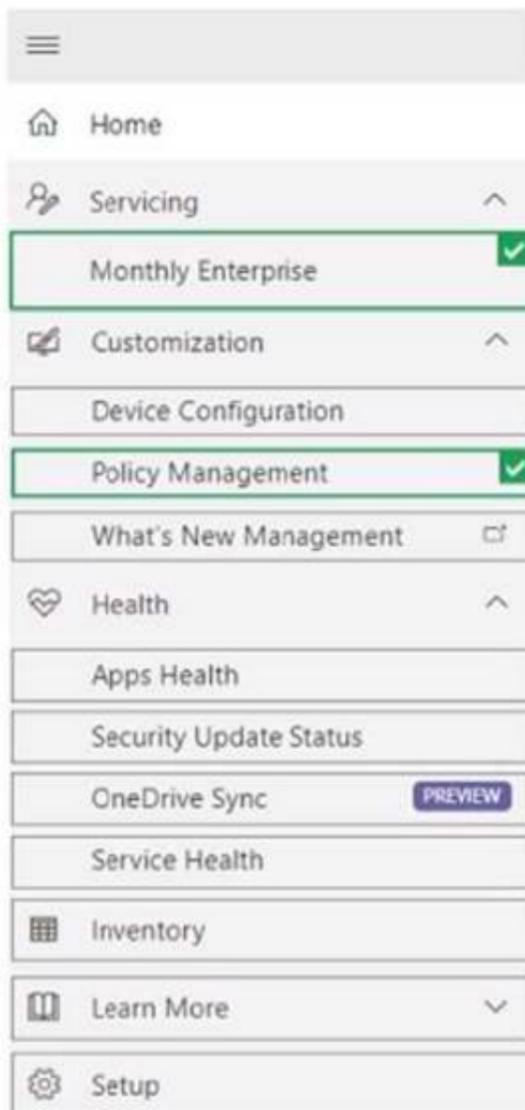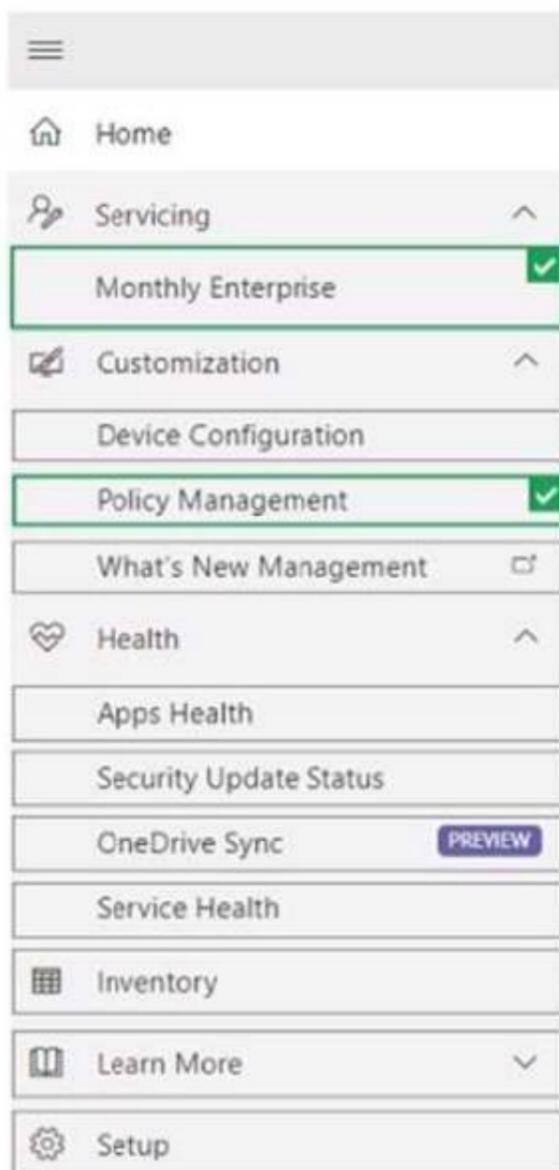
NEW QUESTION 9
- (Exam Topic 4)
You have an Azure AD group named Group1. Group! contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile! to Group1. You need to ensure that Profile! applies to Device1 only. What should you modify in Profile 1?

A. Assignments
B. Settings
C. Scope (Tags)
D. Applicability Rules

Answer: D

Explanation:
To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1. You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability rule that matches Device1's properties and excludes Device2's properties. References:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#applicability-rules

NEW QUESTION 10
- (Exam Topic 4)
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 10
- (Exam Topic 4)
You have a computer that runs Windows 10 and contains two local users named User! and User2. You need to ensure that the users can perform the following anions:
• User 1 must be able to adjust the date and time.
• User2 must be able to clear Windows logs.
The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group 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.

Groups	Answer Area
Administrators	User1:
Event Log Readers	User2:
Performance Log Users	
Power Users	
System Managed Accounts Group	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Groups	Answer Area
Administrators	User1: Administrators
Event Log Readers	User2: Event Log Readers
Performance Log Users	
Power Users	
System Managed Accounts Group	

NEW QUESTION 14
- (Exam Topic 4)
Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Name	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
5	Group5	Name starts with COMP
Last	Ungrouped machines (default)	Not applicable

You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.

computer1

Actions ∨

Domain: adatum.com
OS: Windows10 64-bit (Build 17134)
Machine IP addresses >

What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of:

Group3 only
Group4 only
Grou5 only
Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

Group1 only
Group2 only
Group1 and Group2 only
Group1, Group2, Group3, Group4, and Group5

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1 will be a member of:

▼
Group3 only
Group4 only
Grou5 only
Group3, Group4, and Group5 only

If you add the tag demo to Computer1,
Computer1 will be a member of:

▼
Group1 only
Group2 only
Group1 and Group2 only
Group1, Group2, Group3, Group4, and Group5

NEW QUESTION 17
- (Exam Topic 4)
You have a Microsoft 365 ES subscription that uses Microsoft Intune. Devices are enrolled in Intune as shown in the following table.

Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

The devices are the members of groups as shown in the following table.

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

You create an JOS/iPadOS update profile as shown in the following exhibit.

Create profile

iOS/iPadOS

✅ Basics ✅ Update policy settings ✅ Assignments 🔵 Review + create

Summary

Basics

Name	Profile1
Description	--

Update policy settings

Update to install	Install iOS/iPadOS Latest update
Schedule type	Update outside of scheduled time
Time zone	UTC±00
Time window	

Start day	Start time	End day	End time
Monday	1 AM	Wednesday	1 PM
Friday	1 AM	Saturday	11 PM

Assignments

Included groups

Group	Group Members ⓘ
Group1	3 devices, 0 users

Excluded groups

Group	Group Members ⓘ
Group2	1 devices, 0 users

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

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.		
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.		
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.		☐
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.		☐
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.		☐

NEW QUESTION 20
- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.
When computers start from the LiteTouchPE_x64.Iso image and connect to MDT1. the welcome screen appears as shown In the following exhibit.
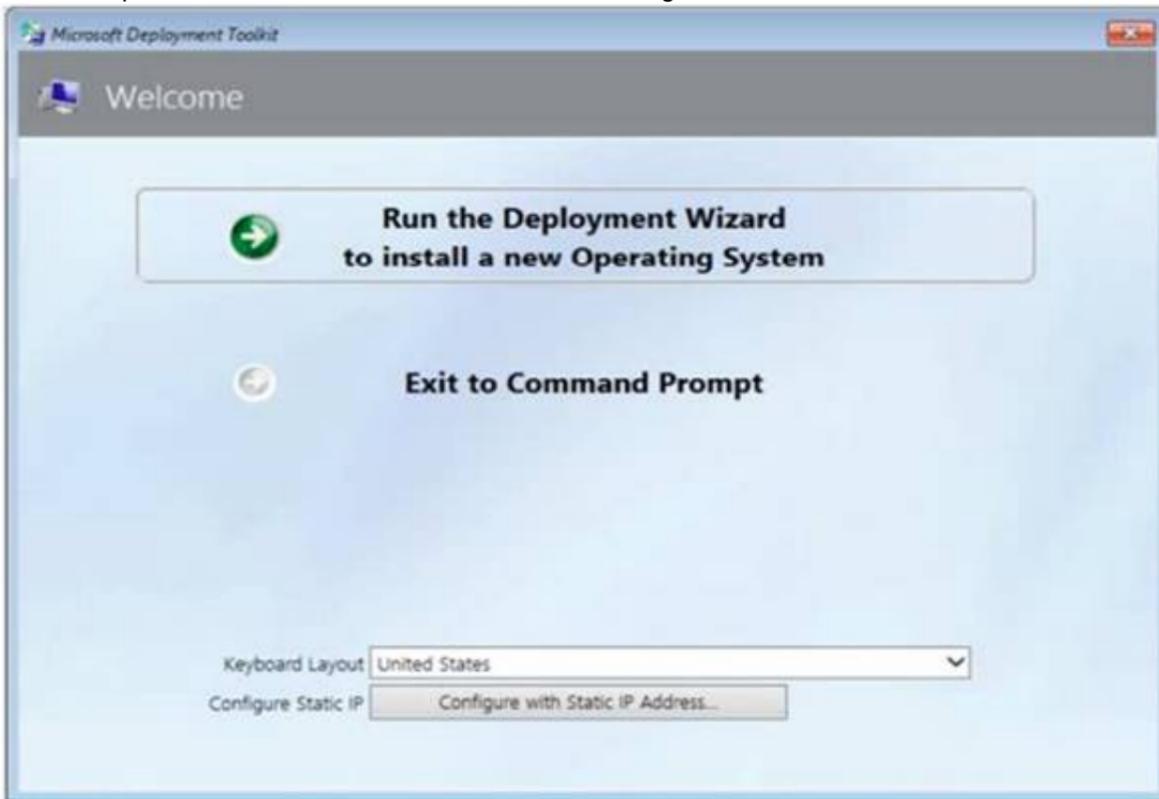
You need to prevent the welcome screen from appearing when the computers connect to MDT1.
Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Modify the Bootstrap.ini file.
Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:
SkipBDDWelcome=YES
Box 2: Modify the CustomSettings.ini file. SkipBDDWelcome
Indicates whether the Welcome to Windows Deployment wizard page is skipped.
For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.
Box 3: Update the deployment share. Reference:
https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages

NEW QUESTION 21
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune. You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the
devices.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.


A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 25
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.
What should you select in the Microsoft Endpoint Manager admin center?

A. App
B. and then App protection policies
C. App
D. and then Monitor
E. Devices, and then Monitor
F. Reports, and the Device compliance

Answer: A

Explanation:
App report: You can search by platform and app, and then this report will provide two different app protection statuses that you can select before generating the report. The statuses can be Protected or Unprotected.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-monitor

NEW QUESTION 26
- (Exam Topic 4)
You have a computer named Computed that has Windows 10 installed. You create a Windows PowerShell script named config.psl.
You need to ensure that config.psl runs after feature updates are installed on Computer5. Which file should you modify on Computer5?

A. LiteTouch.wsf
B. SetupConfig.ini
C. Unattendb*
D. Unattend.xml

Answer: B

Explanation:
SetupConfig.ini is a file that can be used to customize the behavior of Windows Setup during feature updates. You can use this file to specify commands or scripts that run before or after the installation process. To run a PowerShell script after a feature update, you can use the PostOOBE parameter in SetupConfig.ini and specify the path to the script file. References: [SetupConfig.ini reference]

NEW QUESTION 28
- (Exam Topic 4)
You have following types of devices enrolled in Microsoft Intune:
• Windows 10
• Android
• iOS
For which types of devices can you create VPN profiles in Microsoft Intune admin center?

A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and iOS only
D. Android and iOS only
E. Windows 10, Android, and iOS

Answer: E

NEW QUESTION 31
- (Exam Topic 4)
Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune. Currently, Windows updates are downloaded without using Delivery Optimization. You need to configure the computers to use Delivery Optimization. What should you create in Intune?

A. a device compliance policy
B. a Windows 10 update ring

C. a device configuration profile
D. an app protection policy

Answer: C

NEW QUESTION 33
- (Exam Topic 4)
Your company has a Remote Desktop Gateway (RD Gateway).
You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.
You need to configure a Remote Desktop connection to connect through the gateway. Which setting should you configure?

A. Connect from anywhere
B. Server authentication
C. Connection settings
D. Local devices and resources

Answer: A

Explanation:
To connect to a remote server through the RD Gateway, you need to configure the Connect from anywhere setting in the Remote Desktop Connection client. This setting allows you to specify the domain name and port of the RD Gateway server, as well as the authentication method. The other settings are not related to the RD Gateway connection. References: Configure Remote Desktop Connection Settings for Remote Desktop Gateway

NEW QUESTION 38
- (Exam Topic 4)
You are creating a device configuration profile in Microsoft Intu You need to configure specific OMA-URI settings in the profile. Which profile type template should you use?

A. Device restrictions (Windows 10 Team)
B. Identity protection
C. Custom
D. Device restrictions

Answer: C

NEW QUESTION 42
- (Exam Topic 4)
Your company has devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

In Microsoft Endpoint Manager, you define the company's network as a location named Location1. Which devices can use network location-based compliance policies?

A. Device2 and Device3 only
B. Device2 only
C. Device1 and Device2 only
D. Device1 only
E. Device1, Device2, and Device3

Answer: E

Explanation:
Intune supported operating systems
Intune supports devices running the following operating systems (OS): iOS
Android Windows macOS
Note: View the device compliance settings for the different device platforms: Android device administrator
Android Enterprise iOS
macOS
Windows Holographic for Business Windows 8.1 and later
Windows 10/11
Reference: https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 43
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.
You plan to integrate Intune with Microsoft Defender for Endpoint.
You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

A. Connectors and tokens
B. Premium add-ons

C. Microsoft Tunnel Gateway
D. Tenant enrollment

Answer: A

Explanation:
Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure Right Now.
As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.
Reference: https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/

NEW QUESTION 48
- (Exam Topic 4)
You have a Hyper-V host. The host contains virtual machines that run Windows 10 as shown in following table.

Name	Generation	Virtual TPM	Virtual processors	Memory
VM1	1	No	4	16 GB
VM2	2	Yes	2	4 GB
VM3	2	Yes	1	8 GB

Which virtual machines can be upgraded to Windows 11?

A. VM1 only
B. VM2 only
C. VM2 and VM3 only
D. VM1.VM2. andVM3

Answer: C

Explanation:
Windows 11 has certain hardware requirements that must be met in order to upgrade from Windows 10. Some of these requirements are as follows:
➢ A processor with at least 1 GHz
clock speed and2 cores.
➢ A system firmware that supports UEFI
andSecure Boot.
➢ A Trusted Platform Module (TPM)
version2.0
or higher.
➢ At least 4 GB
➢ At least 64 GB
of system memory (RAM). of storage space.
In this scenario, the virtual machines that run Windows 10 have the following specifications:
➢ VM3 is a generation 2 virtual machine with a virtual TPM, 1 virtual processor, and 8 GB of memory.
VM1 cannot be upgraded to Windows 11 because it does not have a virtual TPM and it is not a generation 2 virtual machine. Generation 1 virtual machines do not support UEFI and Secure Boot, which are required for Windows 11. VM2 and VM3 can be upgraded to Windows 11 because they have a virtual TPM and they are generation 2 virtual machines. They also meet the minimum requirements for processor speed, cores, memory, and storage space.

NEW QUESTION 50
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains two users named User1 and User2. You need to ensure that the users can perform the following tasks:
• User1 must be able to create groups and manage users.
• User2 must be able to reset passwords for no administrative users. The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the Microsoft 365 admin center. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers1.
To ensure that User1 can create groups and manage users, you should assign the User Administrator role to User1. This role allows User1 to create and manage all aspects of users and groups, including resetting passwords for non-administrative users1.
To ensure that User2 can reset passwords for non-administrative users, you should assign the Helpdesk Administrator role to User2. This role allows User2 to reset passwords, manage service requests, and monito service health for non-administrative users1.

NEW QUESTION 55
- (Exam Topic 4)
You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.
You need to configure an Intune device configuration profile to meet the following requirements:

⟫ Prevent Microsoft Office applications from launching child processes.

⟫ Block users from transferring files over FTP.
Which two settings should you configure in Endpoint protection? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Create Profile	Endpoint protection
	Windows 10 and later

Create Profile

*Name

MD101 ✓

Description

Enter a description ✓

*Platform

Windows 10 and later ⌄

*Profile type

Endpoint protection ⌄

Settings
Configure ⟩

Scope (Tags)
0 scope(s) selected ⟩

Endpoint protection
Windows 10 and later

Select a category to configure settings

Windows Defender Application Gu...
11 settings available ⟩

Windows Defender Firewall
40 settings available ⟩

Windows Defender SmartScreen
2 settings available ⟩

Windows Encryption
37 settings available ⟩

Windows Defender Exploit Guard
20 settings available ⟩

Windows Defender Application Co...
2 settings available ⟩

Windows Defender Application Gua...
1 setting available ⟩

Windows Defender Security Center
14 settings available ⟩

Local device security options
46 settings available ⟩

Xbox services
5 settings available ⟩

OK

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
References:
https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

NEW QUESTION 59
- (Exam Topic 4)
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 63
- (Exam Topic 4)
You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8, 9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:

⟫ Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.

⟫ Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.
Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

NEW QUESTION 68
- (Exam Topic 4)
You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.) You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR tab.)

Home > Endpoint security > MDM Security Baseline >

Create profile

Block Office applications from injecting code into other processes ⓘ	Disable ∨
Block Office applications from creating executable content ⓘ	Audit mode ∨
Block all Office applications from creating child processes ⓘ	Audit mode ∨
Block Win32 API calls from Office macro ⓘ	Disable ∨
Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ	Disable ∨

Home > Endpoint security > ASR Endpoint security >

Edit profile

∧ Attack Surface Reduction Rules

Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ	Audit mode ⌄
Block Adobe Reader from creating child processes ⓘ	Audit mode ⌄
Block Office applications from injecting code into other processes ⓘ	Audit mode ⌄
Block Office applications from creating executable content ⓘ	Audit mode ⌄
Block all Office applications from creating child processes ⓘ	Audit mode ⌄
Block Win32 API calls from Office macro ⓘ	Audit mode ⌄

You plan to deploy both profiles to devices enrolled in Microsoft Intune. You need to identify how the following settings will be configured on the devices:
• Block Office applications from creating executable content
• Block Win32 API calls from Office macro
Currently, the settings are disabled locally on each device.
What are the effective settings on the devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Block Office applications from creating executable content: ⌄

Audit mode
Block
Disable
Warn

Block Win32 API calls from Office macro: ⌄

Audit mode
Block
Disable
Warn

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Block Office applications from creating executable content: ⌄

Audit mode
Block
Disable
Warn

Block Win32 API calls from Office macro: ⌄

Audit mode
Block
Disable
Warn

NEW QUESTION 71
- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune.
You need to ensure that you can deploy apps to Android Enterprise devices. What should you do first?

A. Create a configuration profile.
B. Add a certificate connector.
C. Configure the Partner device management settings.
D. Link your managed Google Play account to Intune.

Answer: D

NEW QUESTION 73
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.
Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting 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.

Settings

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1: _____ Setting
Device2: _____ Setting
Device3: _____ Setting

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1:
Device Compliance settings for Windows 10/11 in Intune
There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.
Note: Windows Health Attestation Service evaluation rules Require BitLocker:
Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user
data. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.
Not configured (default) - This setting isn't evaluated for compliance or non-compliance.
Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.
Box 2: Prevent jailbroken devices from having corporate access Device Compliance settings for iOS/iPadOS in Intune
There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.
Device Health Jailbroken devices
Supported for iOS 8.0 and later
Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted (jailbroken) devices as not compliant.
Box 3: Prevent rooted devices from having corporate access. Device compliance settings for Android Enterprise in Intune
There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.
Device Health - for Personally-Owned Work Profile Rooted devices
Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted devices as not compliant.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios

NEW QUESTION 75
- (Exam Topic 4)
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. Remote Desktop Users
C. Power Users
D. Remote Management Users

Answer: B

NEW QUESTION 80
- (Exam Topic 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.
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment
share. You create a task sequence, and then you run the MDT deployment wizard on Computer1. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 83
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You plan to enable Microsoft Intune enrollment for the following types of devices:
• Existing Windows 11 devices managed by using Configuration Manager
• Personal iOS devices
The solution must minimize user disruption.
Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Windows 11 devices managed by using Configuration Manager: Windows Autopilot ▼
Co-management
User enrollment
Windows Autopilot

Personal iOS devices: Automated Device Enrollment (ADE) ▼
Apple Configurator
Automated Device Enrollment (ADE)
User enrollment

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Windows 11 devices managed by using Configuration Manager: Windows Autopilot ▼
Co-management
User enrollment
Windows Autopilot

Personal iOS devices: Automated Device Enrollment (ADE) ▼
Apple Configurator
Automated Device Enrollment (ADE)
User enrollment

NEW QUESTION 87
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 11 deployment tasks.
MDT contains the operating system images shown in the following table.

Name	Description
Image1.wim	Custom-built Windows 10 image that has preinstalled custom apps
Image2.wim	Custom-built Windows 10 image without apps
Install.wim	Default Windows 10 image

You need to perform a Windows 11 in-place upgrade on several computers that run Windows 10. From the Deployment Workbench, you open the New Task Sequence Wizard.

You need to identify which task sequence template and which operating system image to use for the task sequence. The solution must minimize administrative effort.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Task sequence template:

Standard Client Task Sequence
Standard Client Replace Task Sequence
Standard Client Upgrade Task Sequence

Operating system image:

Image1.wim
Image2.wim
Install.wim

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Standard Client Upgrade Task Sequence
Use Template: Standard Client Upgrade Task Sequence
In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not plan to significantly change the device's configuration or applications. MDT includes an in-place upgrade task sequence template that makes the process really simple.
Box 2: Install.wim
In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. I
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the

NEW QUESTION 89
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You use Windows Autopilot to deploy Windows 11 to devices.
A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.
You need to ensure that when a deployment fails, the deployment logs can be collected.
What should you configure?

A. the automatic enrollment settings
B. the Windows Autopilot deployment profile
C. the enrollment status page (ESP) profile
D. the device configuration profile

Answer: B

NEW QUESTION 90
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.

Name	Member of
User1	Group1
User2	None
User3	None

You create a policy set named Set1 as shown in the exhibit. (Click the Exhibit tab.)

Device management Edit

Device configuration profiles (1)

Name	Platform	Profile Type
ConfigurationProfile1	Windows 10 and later	Device restrictions

Device compliance policies (1)

Name	Platform	Profile Type
CompliancePolicy1	Windows 10 and later	Windows 10 and later co…

Device enrollment Edit

Windows autopilot deployment profiles

No results

Enrollment status pages

No results.

Assignments Edit

Included groups	All Users
Excluded groups	Group1

You enroll devices in Intune as shown in the following table.

Name	Operating system	User
Device1	Windows 10	User1
Device2	Windows 11	User2
Device3	Android	User3

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

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	⊙
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	⊙
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	⊙

NEW QUESTION 94
- (Exam Topic 4)
You have a Microsoft Intune subscription.
You have devices enrolled in intune as shown in the following table.

Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.
What is the minimum number of app configuration policies required to manage Appl ?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: B

Explanation:
The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn
https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios

NEW QUESTION 98
- (Exam Topic 3)
You need to prepare for the deployment of the Phoenix office computers. What should you do first?

A. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory admin center.
B. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.
C. Extract the hardware ID information of each computer to an XML file and upload the file from the Devices settings in Microsoft Store for Business.
D. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices

NEW QUESTION 103
- (Exam Topic 3)
You need a new conditional access policy that has an assignment for Office 365 Exchange Online. You need to configure the policy to meet the technical requirements for Group4.
Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.
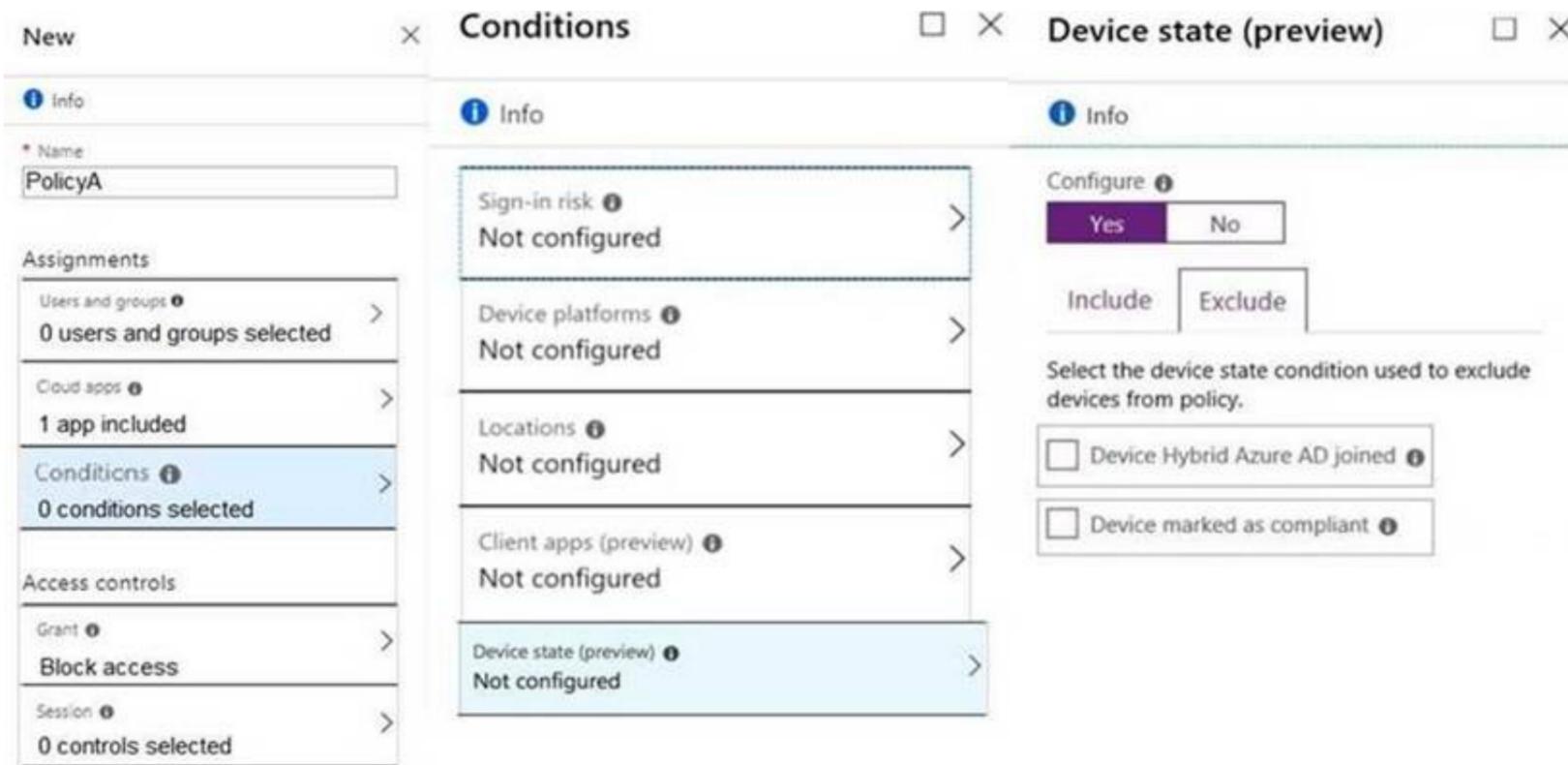
A. Mastered
B. Not Mastered

Answer: A

Explanation:
The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access
A screenshot of a computer Description automatically generated
We therefore need to exclude compliant devices. From the scenario:

> Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions https://docs.microsoft.com/en-us/intune/device-compliance-get-started

NEW QUESTION 108
- (Exam Topic 3)
You are evaluating which devices are compliant.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is compliant	○	○
Device3 is compliant	○	○
Device4 is compliant	○	○

NEW QUESTION 111
- (Exam Topic 2)
What should you configure to meet the technical requirements for the Azure AD-joined computers?

A. Windows Hello for Business from the Microsoft Intune blade in the Azure portal.
B. The Accounts options in an endpoint protection profile.
C. The Password Policy settings in a Group Policy object (GPO).
D. A password policy from the Microsoft Office 365 portal.

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-inorgani

NEW QUESTION 112
- (Exam Topic 2)
What should you upgrade before you can configure the environment to support co-management?

A. the domain functional level
B. Configuration Manager
C. the domain controllers
D. Windows Server Update Services (WSUS)

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

NEW QUESTION 117
- (Exam Topic 2)
You need to resolve the performance issues in the Los Angeles office.
How should you configure the update settings? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area

Change Delivery Optimization download mode to:

Bypass mode
HTTP blended with internet peering
HTTP blended with peering behind same NAT
Simple download mode with no peering

Update Active Hours Start to:

10 AM
11 AM
10 PM
11 PM

Update Active Hours End to:

10 AM
11 AM
10 PM
11 PM

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated with low confidence
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization https://2pintsoftware.com/delivery-optimization-dl-mode/

NEW QUESTION 118
- (Exam Topic 2)
You need to meet the device management requirements for the developers. What should you implement?

A. folder redirection
B. Enterprise State Roaming
C. home folders
D. known folder redirection in Microsoft OneDrive

Answer: B

Explanation:
Litware identifies the following device management requirements:

≫ Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in. Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including
favorites and reading list, across devices.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-refer

NEW QUESTION 123
- (Exam Topic 1)
Which user can enroll Device6 in Intune?

A. User4 and User2 only
B. User4 and User 1 only
C. User1, User2, User3, and User4
D. User4. User Land User2 only

Answer: B

NEW QUESTION 125
- (Exam Topic 1)
User1 and User2 plan to use Sync your settings.
On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

User1:
| No devices |
| Device4 and Device5 only |
| Device1, Device2 and Device3 only |
| Device1, Device2, Device3, Device4, and Device5 |

User2:
| No devices |
| Device4 and Device5 only |
| Device1, Device2 and Device3 only |
| Device1, Device2, Device3, Device4, and Device5 |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/

NEW QUESTION 127
- (Exam Topic 1)
You implement Boundary1 based on the planned changes.
Which devices have a network boundary of 192.168.1.0/24 applied?

A. Device2 only

B. Device3 only
C. Device 1. Device2. and Device5 only
D. Device 1, Device2, Device3, and Device4 only

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows

NEW QUESTION 131
- (Exam Topic 1)
Which devices are registered by using the Windows Autopilot deployment service?

A. Device1 only
B. Device3 only
C. Device1 and Device3 only
D. Device1, Device2, and Device3

Answer: C

Explanation:
Scenario: Windows Autopilot Configuration Assignments
Included groups: Group1
Excluded groups: Group2 Device1 is member of Group1.
Device2 is member of Group1 and member of Group2. Device3 is member of Group1.
Group1 and Group2 have a Membership type of Assigned.
Exclusion takes precedence over inclusion in the following same group type scenarios. Reference: https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

NEW QUESTION 136
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	○	○
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	○	○
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, letter Description automatically generated

NEW QUESTION 141
- (Exam Topic 4)
You have an Azure AD tenant that contains the devices shown in the following table. You purchase Windows 11 Enterprise E5 licenses.
Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

A. Device1 only
B. Device1 and Device2 only
C. Device1 and Device3 only
D. Device1, Device2, Device3, and Device4

Answer: B

NEW QUESTION 146
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

A. an attack surface reduction (ASR) policy
B. a security baseline
C. an endpoint detection and response (EDR) policy
D. an account protection policy

E. an antivirus policy

Answer: C

Explanation:
To onboard the devices to Microsoft Defender for Endpoint, you need to create an endpoint detection and response (EDR) policy in the Microsoft Intune admin center. This policy enables EDR capabilities on devices that are enrolled in Intune and allows you to configure various settings for EDR functionality. You can then assign the policy to groups of users or devices. References:
https://docs.microsoft.com/en-us/mem/intune/protect/edr-windows

NEW QUESTION 147
- (Exam Topic 4)
You have two computers named Computer1 and Computed that run Windows 10. Computed has Remote Desktop enabled.
From Computer1, you connect to Computer2 by using Remote Desktop Connection.
You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.
What should you do?

A. From Computer 2, configure the Remote Desktop settings.
B. From Windows Defender Firewall on Computer 1, allow Remote Desktop.
C. From Windows Defender Firewall on Computer 2, allow File and Printer Sharing.
D. From Computer1, configure the Remote Desktop Connection settings.

Answer: D

NEW QUESTION 152
- (Exam Topic 4)
Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active
Directory (Azure AD).
There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.
You plan to implement Microsoft Defender Exploit Guard.
You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Tool to use to configure the settings:

| Security & Compliance in Microsoft 365 |
| Windows Security app |
| Microsoft Endpoint Manager admin center |

Distribution method:

| An Azure policy |
| An Endpoint Protection configuration profile |
| An Intune device compliance policy |
| A device restrictions configuration profile |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/import-export-expl https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-prot

NEW QUESTION 156
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device1	64-bit version of Windows 10 Pro	Yes	No
Device2	32-bit version of Windows 10 Pro	No	Yes
Device3	64-bit version of Windows 10 Pro	No	Yes

You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11. You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement
Windows 11 Pro on the devices, while retaining all user settings and applications.
Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Windows Autopilot: Device1 and Device3 only
- None of the devices
- Device1 only
- Device1 and Device3 only
- Device1, Device2, and Device3

In-place upgrade: Device1 and Device3 only
- None of the devices
- Device1 only
- Device1 and Device3 only
- Device1, Device2, and Device3

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Windows Autopilot: Device1 and Device3 only
- None of the devices
- Device1 only
- Device1 and Device3 only
- Device1, Device2, and Device3

In-place upgrade: Device1 and Device3 only
- None of the devices
- Device1 only
- Device1 and Device3 only
- Device1, Device2, and Device3

NEW QUESTION 158
- (Exam Topic 4)
Your network contains an Active Directory domain named adatum.com, a workgroup, and computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of	Active Windows Defender Firewall profile
Computer1	Adatum.com	Domain
Computer2	Adatum.com	Domain
Computer3	Workgroup	Public

The local Administrator accounts on Computed, Computed, and Computed have the same user name and password.
On Computed. Windows Defender Firewall is configured as shown in the following exhibit.
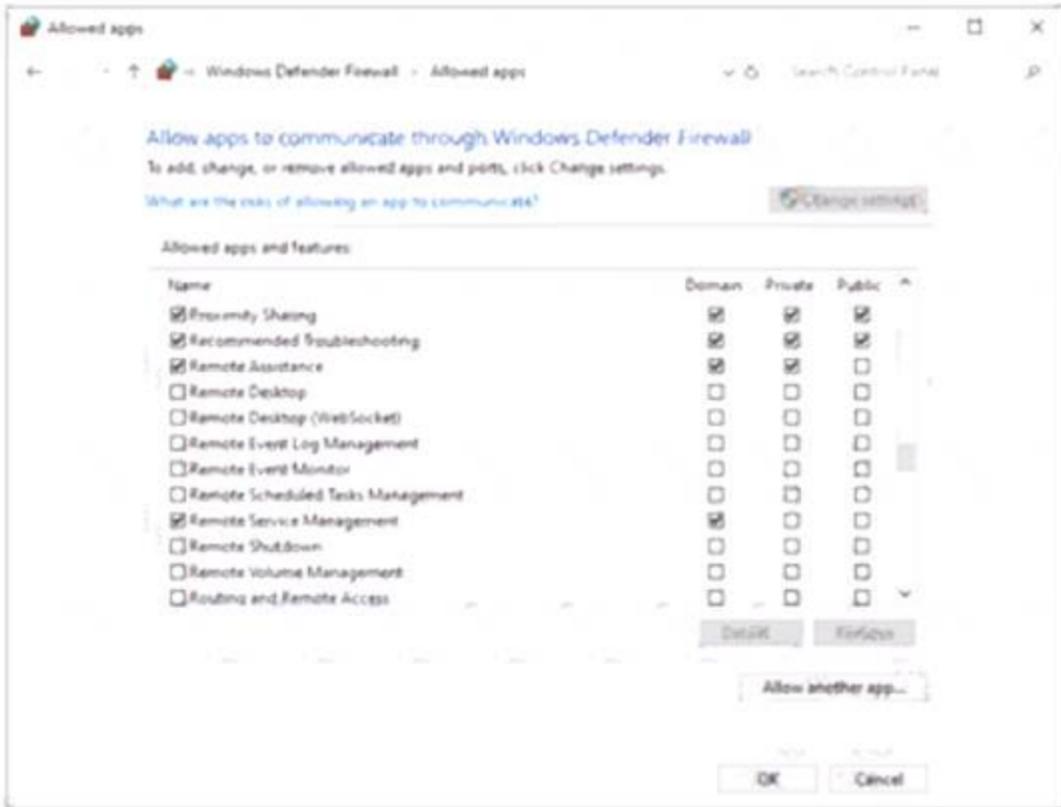
```
Status      Name            DisplayName
------      ----            -----------
Stopped     RasAuto         Remote Access Auto Connection Manager
Running     RasMan          Remote Access Connection Manager
Stopped     RemoteAccess    Routing and Remote Access
Stopped     RemoteRegistry  Remote Registry
Stopped     RetailDemo      Retail Demo Service
Running     RmSvc           Radio Management Service
Running     RpcEptMapper    RPC Endpoint Mapper
Stopped     RpcLocator      Remote Procedure Call (RPC) Locator
Running     RpcSs           Remote Procedure Call (RPC)
```

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.		
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.		
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	☐	
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	☐	
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.		☐

NEW QUESTION 163
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You plan to use Endpoint analytics.
You need to create baseline metrics.
What should you do first?

A. Create an Azure Monitor workbook.
B. Onboard 10 devices to Endpoint analytics.
C. Create a Log Analytics workspace.
D. Modify the Baseline regression threshold.

Answer: C

Explanation:
Onboarding from the Endpoint analytics portal is required for Intune managed devices. Reference: https://docs.microsoft.com/en-us/mem/analytics/enroll-intune

NEW QUESTION 168
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You need to configure an update ring that meets the following requirements:
• Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.
• The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.
• Devices must restart automatically three days after an update is installed.
How should you configure the update ring? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Feature update deferral period (days): | 90 |
3
7
10
14
90

Quality update deferral period (days): | 14 |
3
7
10
14
90

| 7 |
3
7
10
14
90

Grace period: | 3 |
3
7
10
14
90

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Feature update deferral period (days): 90 ▼

| |
| 3 |
| 7 |
| 10 |
| 14 |
| **90** |

Quality update deferral period (days): 14 ▼

| |
| 3 |
| 7 |
| 10 |
| **14** |
| 90 |

7 ▼

| 3 |
| **7** |
| 10 |
| 14 |
| 90 |

Grace period: 3 ▼

| **3** |
| 7 |
| 10 |
| 14 |
| 90 |

NEW QUESTION 169
- (Exam Topic 4)
You have a Microsoft 365 tenant and an internal certification authority (CA).
You need to use Microsoft Intune to deploy the root CA certificate to managed devices.
Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Policy type: ▼

| |
| App configuration policy |
| App protection policy |
| Compliance policy |
| Configuration profile |

Profile: ▼

| |
| Imported public key pair (PKCS) certificate |
| Public key pair (PKCS) certificate |
| Simple Certificate Enrollment Protocol (SCEP) certificate |
| Trusted certificate |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Configuration profile Create a trusted certificate profile. Box 2: Trusted certificate
When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root

NEW QUESTION 173
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft intune as shown in the following table.

Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.
Intune has the device compliance policies shown in the following table.

Name	Platform	Setting	Applied to
Compliance1	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	Group3

The Compliance policy settings are configured as shown in the exhibit. (Click the Exhibit tab.) You create the following Conditional Access policy:

Compliance policies | Compliance policy settings   ...   X

🖫 Save   ✕ Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as   ◉ Compliant

Enhanced jailbreak detection ⓘ   ◉ Disabled

Compliance status validity period (days) ⓘ   [30]

• Name: Policy1
• Assignments
o Users and groups: User1
o Cloud apps or actions: Office 365 SharePoint Online
• Access controls
o Grant Require device to be marked as compliant
• Enable policy: On
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	○	⊡
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	⊡	○
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	○	⊡

NEW QUESTION 176
- (Exam Topic 4)
You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

You are deploying Microsoft 365 apps.
You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Endpoint Manager admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

App Information Edit

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https://products.office.com/en-us/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/en-US/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	...
Logo	Office
	Teams, Word
Architecture	64-bit
Update channel	Current Channel
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License Teams on behalf of users	No
Install background service for Microsoft Search in Bing	No
Apps to be installed as part of the suite	1 language(s) selected

Assignments Edit

Group mode	Group
∨ Required	
⊕ Included	Group1
Available for enrolled devices	

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

Statements	Yes	No
LT1 will have Microsoft Office 365 installed	○	○
LT2 will have Microsoft Office 365 installed	○	○
LT3 will have Microsoft Office 365 installed	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

NEW QUESTION 179
- (Exam Topic 4)
You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	Not applicable	Group3

Intune includes the device compliance policies shown in the following table.

Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	Not applicable

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group1
Policy2	Group1, Group2
Policy3	Group3
Policy4	Group3

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

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Device1 is marked as compliant = No Device2 is marked as compliant = Yes Device3 is marked as comp
= No
➢ Device1 is marked as noncompliant because it does not meet the minimum OS version requirement of Policy1, which is 11.0.0. Device1 has an OS version of 10.0.0, which is lower than the required version1.
➢ Device2 is marked as compliant because it meets all the requirements of Policy2, which are: minimum OS version of 10.0.0, password required, and encryption enabled. Device2 has an OS version of 11.0.0, a password set, and encryption enabled1.
➢ Device3 is marked as noncompliant because it does not meet the encryption requirement of Policy3, which is enabled. Device3 has encryption disabled1.

NEW QUESTION 184
- (Exam Topic 4)
You have the Microsoft Deployment Toolkit (MDT) installed. You install and customize Windows 11 on a reference computer
You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.
Which command should you run before you capture the image?

A. dism
B. wpeinit
C. sysprep
D. bcdedit

Answer: C

Explanation:
To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the sysprep command with the /generalize option. This option removes all unique system information from the Windows installation, such as the computer name, security identifier (SID), and driver cache. The other commands are not used for this purpose. References: Sysprep (Generalize) a Windows installation

NEW QUESTION 186
- (Exam Topic 4)
Your company uses Microsoft Intune.
More than 500 Android and iOS devices are enrolled in the Intune tenant.
You plan to deploy new Intune policies. Different policies will apply depending on the version of Android or iOS installed on the device.
You need to ensure that the policies can target the devices based on their version of Android or iOS. What should you configure first?

A. groups that have dynamic membership rules in Azure AD
B. Device categories in Intune
C. Corporate device identifiers in Intune
D. Device settings in Azure AD

Answer: B

NEW QUESTION 191
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com.
You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

Name	Memory	TPM
Device1	16 GB	None
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

A. Device2 only
B. Device3 only
C. Device2 and Devnce3 only
D. Device 1, Device2, and Device3

Answer: C

Explanation:
Windows Autopilot self-deploying mode requires devices that have a firmware-embedded activation key for Windows 10 Pro or Windows 11 Pro. This feature allows devices to automatically activate Windows Enterprise edition using the subscription license assigned to the user. Device1 does not have a firmware-embedded activation key, so it cannot use self-deploying mode. Device2 and Device3 have firmware-embedded activation keys for Windows 10 Pro, so they can use self-deploying
mode. References: Windows Autopilot self-deploying mode (Public Preview), Deploy Windows Enterpris licenses

NEW QUESTION 194
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to deploy and manage Windows devices.
You have 100 devices from users that left your company.
You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.
What should you do?

A. Deploy a new configuration profile to the devices.
B. Perform a Windows Autopilot reset on the devices.
C. Perform an in-place upgrade on the devices.
D. Perform a clean installation of Windows 11 on the devices.

Answer: B

NEW QUESTION 199
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains a group named Group1.
You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.
You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.
What should you configure?

A. Session access controls
B. an assignment that uses a User risk condition
C. an assignment that uses a Sign-in risk condition
D. Grant access controls

Answer: A

Explanation:
User sign-in frequency
Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.
The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.
Sign-in frequency control

≫ Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.

≫ Browse to Azure Active Directory > Security > Conditional Access.

≫ Select New policy.

≫ Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

≫ Choose all required conditions for customer's environment, including the target cloud apps.

≫ Under Access controls > Session.
Select Sign-in frequency.
Choose Periodic reauthentication and enter a value of hours or days or select Every time.

≫ Save your policy. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life

NEW QUESTION 201
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.
What should you configure?

A. the Azure Monitor agent
B. a device compliance policy
C. a Conditional Access policy
D. an Intune data collection policy

Answer: D

NEW QUESTION 206
- (Exam Topic 4)
You use a Microsoft Intune subscription to manage iOS devices.
You configure a device compliance policy that blocks jailbroken iOS devices. You need to enable Enhanced jailbreak detection.
What should you configure?

A. the Compliance policy settings
B. the device compliance policy
C. a network location
D. a configuration profile

Answer: D

NEW QUESTION 211
- (Exam Topic 4)
You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.
You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

Answer: CE

Explanation:
To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices. References:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

NEW QUESTION 216
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You need to review the startup times and restart frequencies of the devices. What should you use?

A. Azure Monitor
B. intune Data Warehouse
C. Microsoft Defender for Endpoint
D. Endpoint analytics

Answer: D

Explanation:
Endpoint analytics is a feature of Microsoft Intune that provides insights into the performance and health of devices. You can use endpoint analytics to review the startup times and restart frequencies of the devices, as well as other metrics such as sign-in times, battery life, app reliability, and software inventory. References: https://docs.microsoft.com/en-us/mem/analytics/overview

NEW QUESTION 221
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Application admin
Admin2	Cloud application admin
Admin3	Office apps admin
Admin4	Security admin

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization. Which users can download the Office customization file from the admin center?

A. Admin1, Admin2, Admin3. and Admin4
B. Admin1, Admin2, and Admin3 only
C. Admin3 only
D. Admin3 and Admin4 only
E. Admin1 and Admin3 only

Answer: B

Explanation:
* Admin1
An application admin has full access to enterprise applications, applications registrations, and application proxy settings.
* Admin2
Mark your app as publisher verified.
In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.
* Admin3
Office Apps admin - Assign the Office Apps admin role to users who need to do the following:
- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health Reference:
Office Apps admin - Assign the Office Apps admin role to users who need to do the following https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified

NEW QUESTION 225
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com that contains a user named Used. User! has a user principal name (UPN) of user1@contoso.com.
You join a Windows 11 device named Client 1 to contoso.com. You need to add User1 to the local Administrators group of Client1.
How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

net localgroup ▼   Administrators /add "   CONTOSO ▼   \user1@contoso.com"
net accounts   AzureAD
net localgroup   CONTOSO
net user   UPN
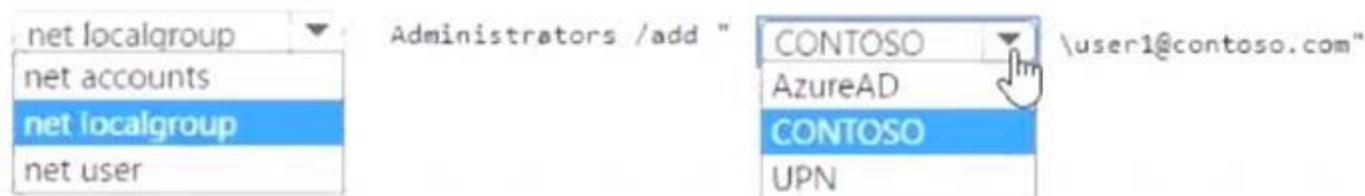
A. Mastered
B. Not Mastered

Answer: A

Explanation:
net localgroup Administrators /add "AzureAD\user1@contoso.com"
This command will add the Azure AD user with the UPN of user1@contoso.com to the local Administrators group of the device1. You need to use the AzureAD prefix and double backslashes to specify the user's domain2. You also need to enclose the user's name in quotation marks if it contains special characters like @1.
You can run this command from an elevated command prompt on Client1, or remotely by using PowerShell or other tools1. You can also use the Intune Role Administrator role or the Additional local administrators on all Azure AD joined devices setting to manage the local administrators group on Azure AD joined devices34.

NEW QUESTION 229
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com.
You have a workgroup computer named Computer! that runs Windows 11. You need to add Computer1 to contoso.com.
What should you use?

A. dsreecmd.exe
B. Computer Management
C. netdom.exe
D. the Settings app

Answer: A

NEW QUESTION 232
- (Exam Topic 4)
You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.
You discover that Group Policy settings override the settings configured in Microsoft Intune policies. You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings. What should you do?

A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
B. From the Microsoft Intune admin center, create a custom device profile.
C. From the Microsoft Intune admin center, create an Administrative Templates device profile.
D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

Answer: C

NEW QUESTION 234
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
Auto-enrollment in Intune is configured.
You have 100 Windows 11 devices in a workgroup.
You need to connect the devices to the corporate wireless network and enroll 100 new Windows devices in Intune.
What should you use?

A. a provisioning package
B. a Group Policy Object (GPO)
C. mobile device management (MDM) automatic enrollment
D. a device configuration policy

Answer: C

NEW QUESTION 235
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS
devices. The solution must minimize administrative effort.
What should you do?

A. Onboard the macOS devices to the Microsoft Purview compliance portal.
B. From the Microsoft Intune admin center, create a security baseline.
C. Install Defender for Endpoint on the macOS devices.
D. From the Microsoft Intune admin center, create a configuration profile.

Answer: C

Explanation:
To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices.
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-install-with-int

NEW QUESTION 240
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	None
Device2	Windows 10	Joined	None
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured as shown in the following exhibit.

Create profile   ...
Windows PC

✅ Basics   ✅ Out-of-box experience (OOBE)   ✅ Assignments   4️⃣ Review + create

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	--

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

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: No
Device1 has no Mobile device Management (MDM) configured.
Note: Device1 is running Windows 8.1, and is registered, but not joined. Device1 is in Group1.
Profile1 is assigned to Group1. Box 2: No
Device2 has no Mobile device Management (MDM) configured. Note: Device2 is running Windows 10, and is joined.
Device2 is in Group2. Group2 is in Group1.
Profile1 is assigned to Group1. Box 3: Yes
Device3 has Mobile device Management (MDM) configured. Device3 is running Windows 10, and is joined
Device1 is in Group1.
Profile1 is assigned to Group1.
Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD, Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations, policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.
Reference: https://xo.xello.com.au/blog/windows-autopilot

NEW QUESTION 242
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings Edit

Update settings

Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel

User experience settings

Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

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,

Answer Area

Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**.

- can be deferred for 30 days
- can be deferred indefinitely
- can be deferred for 30 days
- will be installed immediately

Updates that contain new Windows functionality will be installed within **[answer choice]** of release.

- 1 day
- 1 day
- 30 days
- 60 days

A. Mastered
B. Not Mastered

Answer: A

Explanation:
*Updates that contain fixes and improvements to existing Windows functionality can be deferred for 30 days. This is because the update rings policy named Policy1 has the "Quality updates deferral period (days)" setting set to 30. This means that quality updates, which include fixes and improvements to existing Windows functionality, can be deferred for up to 30 days from the date they are released by Microsoft. After 30 days, the devices will automatically install the quality updates. References:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure
*Updates that contain new Windows functionality will be installed within 60 days of release.
This is because the update rings policy named Policy1 has the "Feature updates deferral period (days)" setting set to 60. This means that feature updates, which include new Windows functionality, can be deferred for up to 60 days from the date they are released by Microsoft. After 60 days, the devices will automatically install the feature updates. References:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure

NEW QUESTION 243
- (Exam Topic 4)
You have computers that run Windows 10 and are configured by using Windows AutoPilot. A user performs the following tasks on a computer named Computer1:

≫ Creates a VPN connection to the corporate network

⟩ Installs a Microsoft Store app named App1

⟩ Connects to a Wi-Fi network

You perform a Windows AutoPilot Reset on Computer1.

What will be the state of the computer when the user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The Wi-Fi connection will be:

Removed
Retained and the passphrase will be retained
Retained but the passphrase will be reset

App1 will be:

Reinstalled at sign-in
Removed
Retained

The VPN connection will be:

Removed
Retained and the credentials will be cached
Retained but the credentials will be reset

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 244
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune. You create an app configuration policy that contains the following settings:
• Device enrollment type: Managed devices
• Profile Type: All Profile Types
• Platform: Android Enterprise
Which two types of apps can be associated with the policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Built-in Android app
B. Managed Google Play store app
C. Web link
D. Android Enterprise system app
E. Android store app

Answer: BD

NEW QUESTION 245
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the objects shown in the following table. You are creating a compliance policy named Compliance1.
Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

A. Group3 and Group4 only
B. Group3, Group4, and Admin1 only
C. Group1, Group2, and Group3 only
D. Group1, Group2, Group3, and Group4 only
E. Group1, Group2, Group3, Group4, and Admin1

Answer: C

Explanation:
Reference:
https://www.ravenswoodtechnology.com/microsoft-intune-compliance-notifications/ https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

NEW QUESTION 247
- (Exam Topic 4)
You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 11.
You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 11 Enterprise to new computers. The computers have a single hard disk.

You need to modify the task sequence to create a system volume and a data volume.
Which phase should you modify in the task sequence?

A. Initialization
B. State Restore
C. Preinstall
D. Postinstall

Answer: C

NEW QUESTION 252
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

In the Microsoft Intune admin center, you are creating a Microsoft 365 Apps app named App1. To which objects can you assign App1?

A. Group3 and Group4 only
B. Admin1, Group3, and Group4 only
C. Group1, Group3, and Group4 only
D. Group1, Group2, Group3, and Group4 only
E. Admin1, Group1. Group2, Group3, andGroup4

Answer: C

Explanation:
In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using device groups. In this scenario, the objects shown in the table are as follows:

➤ Admin1 is an individual user account that belongs to the Global administrators

➤ Group1 is a user group that contains 100 users.

➤ Group2 is a device group that contains 50 devices.

➤ Group3 is a user group that contains 200 users.

➤ Group4 is a device group that contains 150 devices.
role group.
Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment. Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

NEW QUESTION 255
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10. You implement hybrid Azure AD and Microsoft Intune.
You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort.
What should you use?

A. an Autodiscover address record
B. a Group Policy object (GPO)
C. an Autodiscover service connection point (SCP)
D. a Windows Autopilot deployment profile

Answer: D

NEW QUESTION 260
- (Exam Topic 4)
You have a Hyper-V host that contains the virtual machines shown in the following table.

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

A. VM1 only
B. VM3only
C. VM1 and VM2 only

D. VM2 and VM3 only
E. VM1, VM2, and VM3

Answer: E

NEW QUESTION 261
- (Exam Topic 4)
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. Enable the Allow Remote Shell access setting.
B. Enable the Allow remote server management through WinRM setting.
C. Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.
D. Enable the Windows Defender Firewall: Allow inbound Remote Desktop exceptions setting.
E. Set the Startup Type of the Remote Registry service to Automatic
F. Enable the Windows Defender Firewall: Allow inbound remote administration exception setting.

Answer: BCF

Explanation:
To enable WinRM on domain computers using Group Policy, you need to perform the following actions:

Enable the Allow remote server management through WinRM setting under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service. This setting allows you to specify the IP address ranges that can connect to the WinRM service.

Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic under Computer Configuration > Preferences > Control Panel Settings > Services. This setting ensures that the WinRM service starts automatically on the computers.

Enable the Windows Defender Firewall: Allow inbound remote administration exception setting under Computer Configuration > Policies > Security Settings > Windows Firewall and Advanced Security > Windows Firewall and Advanced Security > Inbound Rules. This setting creates a firewall rule that allows incoming TCP connections on port 5985 for WinRM. References: How to Enable WinRM via Group Policy, Installation and configuration for Windows Remote Management

NEW QUESTION 266
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User! uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1. You need to identify what will occur when User1 next signs in to the devices.
What should you identify for each device? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Device1: Will activate as Windows 11 Enterprise
- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Device2: Will not upgrade to Windows 11 Enterprise
- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Device 1:

Will activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windo 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 1 has Windows 11 Pro, so it meets the requirement. When User1 signs in to Device 1 with their Azure AD account, the device will automatically activate as Windows 11 Enterprise without changing the edition.

Will not activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 2 has Windows 10 Home, so it does not meet the requirement. When User1 signs in to Device 2 with their Azure AD account, the device will not activate as Windows 11 Enterprise by subscription.

NEW QUESTION 269
- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to perform the following tasks for User1:

⟫ Set the Usage location to Canada.

⟫ Configure the Phone and Email authentication contact info for self-service password reset (SSPR). Which two settings should you configure in the Azure Active Directory admin center? To answer, select the
appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Manage

- 👤 Profile
- 🟦 Custom security attributes (Preview)
- 👤 Assigned roles
- 📇 Administrative units
- 👥 Groups
- ⊞ Applications
- 👤 Licenses
- 🖥 Devices
- 🔑 Azure role assignments
- 🛡 Authentication methods

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 273
- (Exam Topic 4)
You have a Microsoft 365 subscription that includes Microsoft Intune.
You have an update ring named UpdateRingl that contains the following settings:
• Automatic update behavior: Auto install and restart at a scheduled time
• Automatic behavior frequency: First week of the month
• Scheduled install day: Tuesday
• Scheduled install time: 3 AM
From the Microsoft Intone admin center, you select Uninstall for the feature updates of UpdateRing1. When will devices start to remove the feature updates?

A. when a user approves the uninstall
B. as soon as the policy is received
C. next Tuesday
D. the first Tuesday of the next month

Answer: C

NEW QUESTION 274
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 500 Android Enterprise devices. All the devices are enrolled in Microsoft Intune.
You need to deliver bookmarks to the Chrome browser on the devices What should you create?

A. a compliance policy
B. a configuration profile
C. an app protection policy
D. an app configuration policy

Answer: D

NEW QUESTION 278
- (Exam Topic 4)
You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to set a custom image as the wallpaper and sign-in screen.
Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Device restrictions
Windows 10 and later

| ✓ Basics | ② Configuration settings | 3 Assignments | 4 Applicability Rules | 5 Review + create |

- ∨ App Store
- ∨ Cellular and connectivity
- ∨ Cloud and Storage
- ∨ Cloud Printer
- ∨ Control Panel and Settings
- ∨ Display
- ∨ General
- ∨ Locked Screen Experience ✅
- ∨ Messaging
- ∨ Microsoft Edge Browser
- ∨ Network proxy
- ∨ Password
- ∨ Per-app privacy exceptions
- ∨ Personalization ✅
- ∨ Printer
- ∨ Privacy
- ∨ Projection

Previous | **Next**

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Device restrictions
Windows 10 and later

✓ Basics   ② Configuration settings   ③ Assignments   ④ Applicability Rules   ⑤ Review + create

∨ App Store	
∨ Cellular and connectivity	
∨ Cloud and Storage	
∨ Cloud Printer	
∨ Control Panel and Settings	
∨ Display	
∨ General	
∨ Locked Screen Experience	✓
∨ Messaging	
∨ Microsoft Edge Browser	
∨ Network proxy	
∨ Password	
∨ Per-app privacy exceptions	
∨ Personalization	✓
∨ Printer	
∨ Privacy	
∨ Projection	

[Previous]   [**Next**]

NEW QUESTION 280
- (Exam Topic 4)
You have a Microsoft Intune subscription that has the following device compliance policy settings: Mark devices with no compliance policy assigned as: Compliant
Compliance status validity period (days): 14
On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:
- Name: Policy1
- Platform: Windows 10 and later
- Require BitLocker: Require
- Mark device noncompliant: 5 days after noncompliance
- Scope (Tags): Tag1
- Name: Policy2
- Platform: Windows 10 and later
- Firewall: Require
- Mark device noncompliant: Immediately
- Scope (Tags): Tag2
On January 5, you assign Policy1 and Policy2 to Group1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
On January 7, Device1 is marked as compliant.	○	○
On January 8, Device1 is marked as compliant.	○	○
On January 8, Device2 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No.
Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.
Box 2: No
For the same reason as Box1. Box 3: Yes
Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.
The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

NEW QUESTION 281
- (Exam Topic 4)
You have 100 computers that run Windows 10.
You plan to deploy Windows 11 to the computers by performing a wipe and load installation. You need to recommend a method to retain the user settings and the user data.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions		Answer Area
Configure known folder redirection in Microsoft OneDrive.		
Run scanstate.exe.		
Run loadstate.exe.		
Enable Enterprise State Roaming.	⟩ ⟨	⋀ ⋁
Create a system image backup.		
Deploy Windows 11.		
Restore a system image backup.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions		Answer Area
Configure known folder redirection in Microsoft OneDrive.		Create a system image backup.
Run scanstate.exe.		
Run loadstate.exe.		Deploy Windows 11.
Enable Enterprise State Roaming.	⟩ ⟨	
Create a system image backup.		Restore a system image backup.
Deploy Windows 11.		⋀ ⋁
Restore a system image backup.		

NEW QUESTION 285
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains a computer named Computer! that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:
• For the WinRM service, set Startup type to Automatic.
• Create a listener that accepts requests from any IP address.
• Enable a firewall exception for WS-Management communications. Which PowerShell cmdlet should you use?

A. Connect-WSMan
B. Enable-PSRemoting

C. Invoke-WSManAction
D. Enable-PSSessionConfiguration

Answer: B

NEW QUESTION 287
- (Exam Topic 4)
You have the device configuration profile shown in the following exhibit.

Kiosk ···   ✕
Windows 10 and later

✓ Basics   ② **Configuration settings**   ③ Assignments   ···

Configure your devices to run in kiosk mode. Before you select a kiosk mode, review your
app assignments in the Mobile Apps blade. Apps that you want to run in kiosk mode
should be assigned to a Windows device. Learn more about Windows kiosk mode.

Select a kiosk mode * ① | Single app, full-screen kiosk   ⌄ |

User logon type * ① | Auto logon (Windows 10, version 1803+) ⌄ |

Application type * ① | Add Microsoft Edge browser   ⌄ |

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version
1909 and later. Learn more about Microsoft Edge kiosk mode.

Edge Kiosk URL * ① | https://contoso.com   ✓ |

Microsoft Edge kiosk mode type ① | Public Browsing (InPrivate)   ⌄ |

Refresh browser after idle time ① | 5 |

Specify Maintenance Window for App   (Require   **Not configured**)
Restarts * ①

Maintenance Window Start Time | MM/DD/YYYY   🗓 | h:mm:ss A |

Maintenance Window Recurrence ① | Daily (recommended)   ⌄ |

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.

Answer Area

Users	
can access any URL.
cannot view the address bar in Microsoft Edge.
can only access URLs that include contoso.com.
can only access URLs that start with https://contoso.com/ .

Windows 10 devices can have	
a single Microsoft Edge instance that has a single tab.
a single Microsoft Edge instance that has multiple tabs.
multiple Microsoft Edge instances that have multiple tabs.
multiple Microsoft Edge instances that each has a single tab.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Users can only access URLs that start with https://contoso.com/ Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab

he device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:

- Kiosk mode: Enabled
- Kiosk type: Multi-app
- Allowed URLs: https://contoso.com/*
- Address bar: Disabled

These settings mean that users can only access URLs that start with https://contoso.com/ and cannot view the address bar in Microsoft Edge. The kiosk type of Multi-app allows users to open multiple instances of Microsoft Edge, but each instance can only have a single tab. Therefore, users cannot access any URL, cannot view the address bar in Microsoft Edge, and can have multiple Microsoft Edge instances that each has a single tab. References: https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings#kiosk-browser-settings

NEW QUESTION 291
- (Exam Topic 4)
You have computers that run Windows 10 and are managed by using Microsoft Intune. Users store their files in a folder named D:\Folder1.
You need to ensure that only a trusted list of applications is granted write access to D:\Folder1. What should you configure in the device configuration profile?

A. Microsoft Defender Exploit Guard
B. Microsoft Defender Application Guard
C. Microsoft Defender SmartScreen
D. Microsoft Defender Application Control

Answer: A

NEW QUESTION 292
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You have the devices shown in the following table.

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

A. Device3 only
B. Device2 and Device3 only
C. Device 1 and Device2 only
D. Device1, Device2, and Device3

Answer: A

NEW QUESTION 296
- (Exam Topic 4)
You have 25 computers that run Windows 10 Pro.
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.
What should you use?

A. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise
B. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise
C. Windows Autopilot
D. Subscription Activation

Answer: C

NEW QUESTION 300
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

You assign Windows 10/11 Enterprise E5 licenses to Gtoup1 and Uset2. You deploy the devices shown in the following table.

Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device3	Windows 10 Pro	Azure AD

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

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.		
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.		
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.		☐
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	☐	
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.		☐

NEW QUESTION 303
- (Exam Topic 4)
Your company standardizes on Windows 10 Enterprise for all users.
Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.
You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps. The solution must meet the following
requirements:
• Ensure that any applications installed by the users are retained.
• Minimize user intervention.
What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. Windows Autopilot
B. Microsoft Deployment Toolkit (MDT)
C. a Windows Configuration Designer provisioning package
D. Windows Deployment Services (WDS)

Answer: A

NEW QUESTION 307
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You need provide a user the ability to disable Security defaults and principle of least privilege. Which role should you assign to the user?

A. Global Administrator
B. Conditional Access Administrator
C. Security Administrator
D. Intune Administrator

Answer: B

Explanation:
To enable or disable security defaults in your directory, sign in to theAzure portalas a security administrator, Conditional Access administrator, or global administrator.
Note: Conditional Access Administrator
Users with this role have the ability to manage Azure Active Directory Conditional Access settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

NEW QUESTION 311
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You plan to create Windows 11 device builds for the marketing and research departments The solution must meet the following requirements:
• Marketing department devices must support Windows Update for Business.
• Research department devices must have support for feature update versions for up to 36 months from release. What is the minimum Windows 11 edition required for each department? To answer, select the appropriate
options in the answer area.
NOTE: Each correct selection is worth one point

Answer Area

Marketing: Windows 11 Pro ▼
- Windows 11 Enterprise
- **Windows 11 Pro**
- Windows 11 Pro for Workstations

Research: Windows 11 Enterprise ▼
- **Windows 11 Enterprise**
- Windows 11 Pro
- Windows 11 Pro for Workstations

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Marketing: Windows 11 Pro ▼
- Windows 11 Enterprise
- **Windows 11 Pro**
- Windows 11 Pro for Workstations

Research: Windows 11 Enterprise ▼
- **Windows 11 Enterprise**
- Windows 11 Pro
- Windows 11 Pro for Workstations

NEW QUESTION 316
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

MD-102 Practice Exam Features:

* MD-102 Questions and Answers Updated Frequently

* MD-102 Practice Questions Verified by Expert Senior Certified Staff

* MD-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MD-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The MD-102 Practice Test Here