Microsoft

Exam Questions MD-102

Endpoint Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 4)
You have an Azure subscription.
You have an on-premises Windows 11 device named Device 1. You plan to monitor Device1 by using Azure Monitor.
You create a data collection rule (DCR) named DCR1 in the subscription. To what should you associate DCR1 ?

A. Azure Network Watcher
B. Device1
C. a Log Analytics workspace
D. a Monitored Object

Answer: B

Explanation:
To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it. A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1. To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2. You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.
The other options are not correct for this scenario because:

➢ Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources. It is not related to data collection rules or Azure Monitor4.

➢ A Log Analytics workspace is a destination where you can send the data collected by a data collection rule. It is not an entity that you can associate a DCR with5.

➢ A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules. References: Data collection rules in Azure Monitor, Configure data collection for Azure Monitor Agent, U
Azure Policy to install Azure Monitor Agent and associate with a DCR, What is Azure Network
Watcher?, Log Analytics workspaces in Azure Monitor

NEW QUESTION 2
- (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 3
- (Exam Topic 4)
You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to upgrade the computers to Windows 11 Enterprise. What should you configure in Intune?

A. a device compliance policy
B. a device cleanup rule
C. a device enrollment policy
D. a device configuration profile

Answer: D

NEW QUESTION 4
- (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 5
- (Exam Topic 4)
You have 100 Windows 10 devices enrolled in Microsoft Intune.
You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.
Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
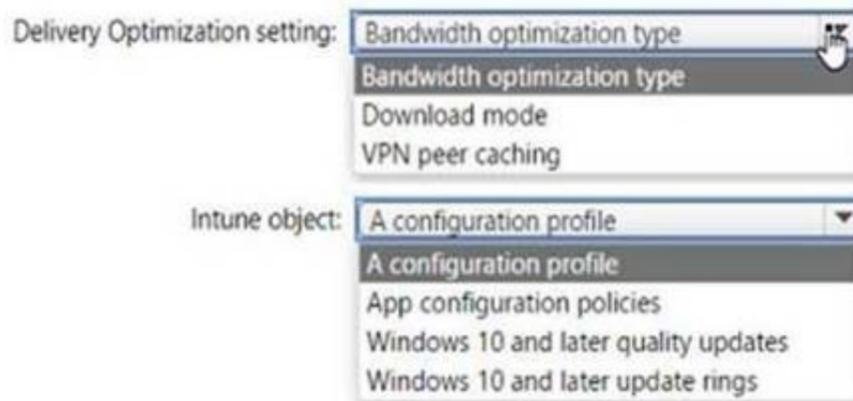
Answer Area

Delivery Optimization setting: Bandwidth optimization type
- Bandwidth optimization type
- Download mode
- VPN peer caching

Intune object: A configuration profile
- A configuration profile
- App configuration policies
- Windows 10 and later quality updates
- Windows 10 and later update rings

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Delivery Optimization setting: B. Download mode Intune object: A configuration profile
To configure the devices to retrieve Windows updates from the internet and from other computers on a local network, you need to configure the Download mode setting in a Delivery Optimization device configuration profile. This setting specifies how the devices use Delivery Optimization to download updates. You can choose from several options, such as HTTP only, LAN only, or Group. For example, you can set the Download mode to Group and specify a group ID for the devices to share updates among themselves and with other devices that have the same group ID. You can also set the Download mode to Internet to allow the devices to download updates from Microsoft or other devices on the internet that use Delivery Optimization. References: https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows

NEW QUESTION 6
- (Exam Topic 4)
You have an on-premises Active Directory domain that syncs to Azure AD tenant.
The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune. The Microsoft Office settings on the computers are configured by using an Group Policy Object (GPO).
You need to migrate the GPO to Intune.
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.

Actions   **Answer Area**

| Assign the policy. |
| Create a compliance policy. |
| Set a scope tag to the policy. |
| Import an ADMX file. |
| Create a configuration profile. |
| Configure the Administrative Templates settings. |
| Assign the profile. |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions   **Answer Area**

| Assign the policy. |
| Create a compliance policy. |
| Set a scope tag to the policy. |
| Import an ADMX file. |
| Create a configuration profile. |
| Configure the Administrative Templates settings. |
| Assign the profile. |

| Create a configuration profile. |
| Configure the Administrative Templates settings. |
| Assign the profile. |

NEW QUESTION 7
- (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   **Answer Area**

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

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 8
- (Exam Topic 4)
You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.
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.

Actions

Obtain the root certificate.
From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.
From the Enterprise CA, configure certificate managers.
From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.
From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

NEW QUESTION 9
- (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 10
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?

A. .intunemac
B. apk
C. jpa
D. .appx

Answer: C

Explanation:
iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

NEW QUESTION 10
- (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.
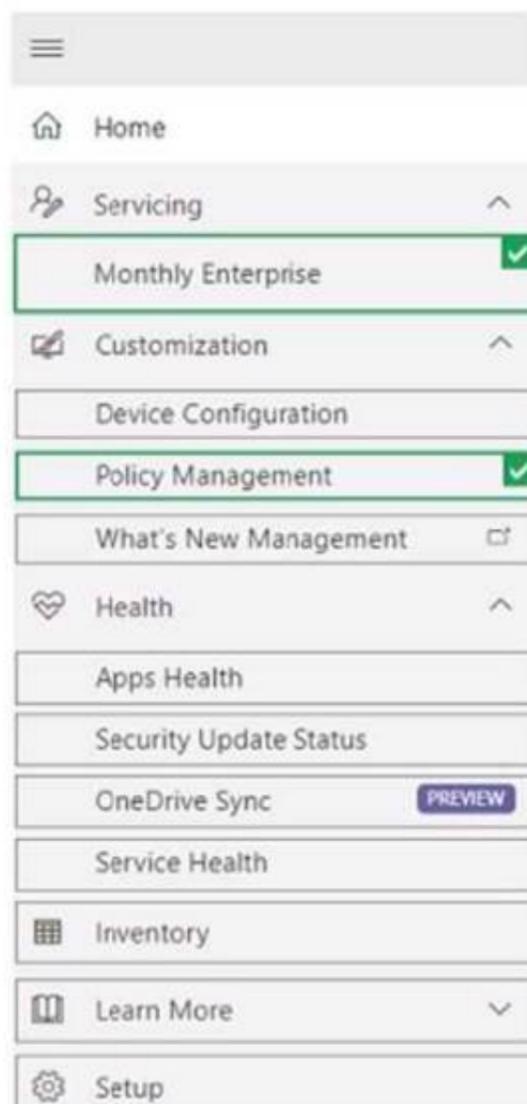
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
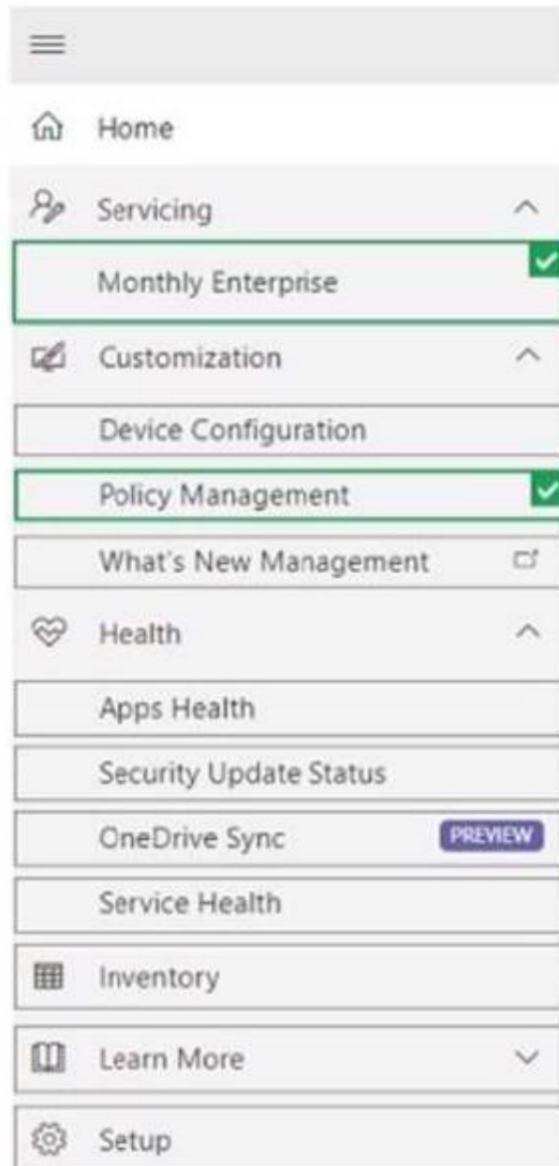
NEW QUESTION 15
- (Exam Topic 4)
You have an Azure AD group named Group1. Group! contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile! to Group1. You need to ensure that Profile! applies to Device1 only. What 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 19
- (Exam Topic 4)
You have a Microsoft 365 subscription. All devices run Windows 10.
You need to prevent users from enrolling the devices in the Windows Insider Program.
What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.
NOTE: Each correct selection is worth one point.

A. a device restrictions device configuration profile
B. an app configuration policy
C. a Windows 10 and later security baseline
D. a custom device configuration profile
E. a Windows 10 and later update ring

Answer: AE

NEW QUESTION 23
- (Exam Topic 4)
You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

A. 30 days
B. 60 days
C. 90 days
D. 365 days

Answer: B

Explanation:
The Device compliance trends report shows the number of devices that are compliant, noncompliant, and not evaluated over time. The report displays trend data for the last 60 days by default, but you can change the time range to view data for the last 7, 14, or 30 days as well. The report does not show data for more than 60
days. References: [Device compliance trends report]

NEW QUESTION 25
- (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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 28
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table. All devices have Microsoft Edge installed.
From the Microsoft Intune admin center, you create a Microsoft You need to apply Edge1 to all the supported devices.
To which devices should you apply Edge1?

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

Answer: E

NEW QUESTION 32
- (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.

Actions		Answer Area
Review the compliance dashboard for results.		1
Create and assign a compliance policy that has System Security settings configured.		2
Review the Conditional Access Insights and Reporting workbook for results.		3
Create a PowerShell discovery script and a JSON file.		4
Upload the PowerShell script to Intune.		
Upload the JSON file to Azure AD.		
Create and assign a custom compliance policy.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Review the compliance dashboard for results.	Create a PowerShell discovery script and a JSON file.
Create and assign a compliance policy that has System Security settings configured.	Upload the PowerShell script to Intune.
Review the Conditional Access Insights and Reporting workbook for results.	Upload the JSON file to Azure AD.
Create a PowerShell discovery script and a JSON file.	Create and assign a custom compliance policy.
Upload the PowerShell script to Intune.	
Upload the JSON file to Azure AD.	
Create and assign a custom compliance policy.	

NEW QUESTION 36
- (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 40
- (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 42
- (Exam Topic 4)
You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:
• MDM user scope: Group1
• MAM user scope: 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.

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	○	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	○
User2 can enroll Device1 in Intune by using automatic enrollment.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	○	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	○
User2 can enroll Device1 in Intune by using automatic enrollment.	○	○

NEW QUESTION 43
- (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 45
- (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 46
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription and 100 computers that run Windows 10.
You need to deploy Microsoft Office Professional Plus 2019 to the computers by using Microsoft Office Deployment Tool (ODT).
What should you use to create a customization file for ODT?

A. the Microsoft 365 admin center
B. the Microsoft Intune admin center
C. the Microsoft Purview compliance portal
D. the Microsoft 365 Apps admin center

Answer: D

NEW QUESTION 51
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.
You have a Microsoft 365 subscription
You plan to use Windows Autopilot to deploy new Windows devices. You plan to create a deployment profile.
You need to ensure that The deployment meets the following requirements:
• Devices must be joined to AD DS regardless of their current working location.
• Users in the marketing department must have a line-of-business (LOB) app installed during the deployment. The solution must minimize administrative effort.
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Devices must be joined to AD DS regardless of their current working location:	Install the Intune connector for Active Directory. ▼
	Deploy Always On VPN.
	Install the Intune connector for Active Directory.
	Modify the Autopilot deployment profile.
	Edit the Co-management settings in Intune.
The marketing department users must have an LOB app installed during the deployment:	Modify the Autopilot deployment profile. ▼
	Modify the Autopilot deployment profile.
	Create a Microsoft Intune app deployment.
	Create a device configuration profile in Intune.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Devices must be joined to AD DS regardless of their current working location:	Install the Intune connector for Active Directory. ▼
	Deploy Always On VPN.
	Install the Intune connector for Active Directory.
	Modify the Autopilot deployment profile.
	Edit the Co-management settings in Intune.
The marketing department users must have an LOB app installed during the deployment:	Modify the Autopilot deployment profile. ▼
	Modify the Autopilot deployment profile.
	Create a Microsoft Intune app deployment.
	Create a device configuration profile in Intune.

NEW QUESTION 54
- (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.

Roles

| Global Administrator |
| Helpdesk Administrator |
| Security Administrator |
| User Administrator |

Answer Area

User1: [Role]

User2: [Role]
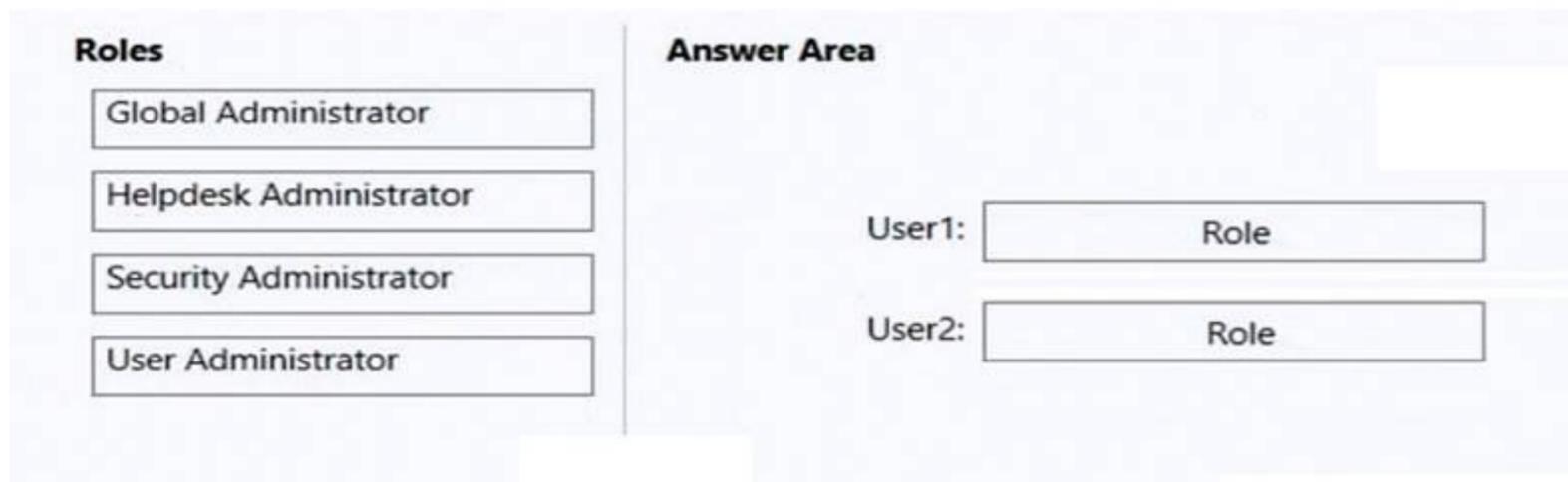
A. Mastered
B. Not Mastered

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 59
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You need to assign roles in Intune to meet the following requirements:
• The members of Group1 must manage Intune roles and assignments.
• The members of Group2 must assign existing apps and policies to users and devices.
The solution must follow the principle of least privilege.
Which role should you assign to each group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Group1: [Intune Service Administrator ▼]
Help Desk Operator
Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

Group2: [Policy and Profile Manager ▼]
Help Desk Operator
Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To assign roles in Intune to meet the requirements, you should assign the following roles to each group: Group1: Intune Role Administrator Group2: Help Desk Operator

➤ The Intune Role Administrator role is the only Intune role that can manage custom Intune roles and add assignments for built-in Intune roles1. This role meets the requirement for Group1 to manage Intune roles and assignments.

➤ The Help Desk Operator role can perform remote tasks on users and devices, and can assign applications or policies to users or devices1. This role meets the requirement for Group2 to assign existing apps and policies to users and devices.

NEW QUESTION 64
- (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 66
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription and 25 Apple iPads.
You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method. What should you do first?

A. Upload a file that has the device identifiers for each iPad.
B. Modify the enrollment restrictions.
C. Configure an Apple MDM push certificate.
D. Add your user account as a device enrollment manager (DEM).

Answer: C

Explanation:
Reference:
https://www.manageengine.com/mobile-device-management/help/enrollment/mdm_creating_apns_certificate.ht Prerequisites for iOS enrollment Before you can enable iOS devices, complete the following steps: Make sure your device is eligible for Apple device enrollment. Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority. Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS and macOS devices.
https://docs.microsoft.com/en-gb/intune/enrollment/apple-mdm-push-certificate-get

NEW QUESTION 71
- (Exam Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	macOS

In Microsoft Intune Endpoint security, you need to configure a disk encryption policy for each device. Which encryption type should you use for each device, and which role-based access control (RBAQ role in
Intune should you use to manage the encryption keys? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Device1:
FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

Device2:
FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

RBAC role:
Help Desk Operator
Application Manager
Intune Role Administrator
Policy and Profile Manager

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 76
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.
You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Enroll the devices in Microsoft Intune by using the Intune Company Portal.
B. Create a compliance policy.
C. Enroll the devices in Microsoft Intune by using Apple Business Manager.

D. Create an iOS app provisioning profile.
E. Create a device configuration profile.

Answer: CE

Explanation:
To deploy a specific iOS update to the unmanaged iPad devices, you need to perform the following actions:

Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to create device groups and assign roles and permissions12.

Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices34.
The other options are not correct for this scenario because:

Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune. However, this method requires user interaction and consent, and does not enroll the devices as supervised devices5.

Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings. However, a compliance policy does not deploy or manage software updates on the devices6.

Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune. However, an iOS app provisioning profile does not affect the software updates on the devices7.
References: What is Apple Business Manager?, Enroll iOS/iPadOS devices in Intune, Manage iOS/iPadOS software update policies in Intune, Software updates planning guide and scenarios for supervised iOS/iPadOS devices in Microsoft Intune, Enroll your personal device in Intune, Device compliance policies in Microsoft Intune, Add an iOS app provisioning profile with Microsoft Intune

NEW QUESTION 81
- (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 84
- (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 89
- (Exam Topic 4)
You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

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

Answer: D

Explanation:
The correct answer is D because app configuration policies can be applied to managed devices and managed apps1. Managed devices are enrolled and managed by Intune, while managed apps are integrated with Intune App SDK or wrapped using the Intune Wrapping Tool1. Device2, Device3, and Device4 are either enrolled in Intune or have managed apps installed, so they can receive app configuration policies2. Device1 is not enrolled in any MDM solution and does not have any managed apps installed, so it cannot receive app configuration policies2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Policy sets - Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets

NEW QUESTION 90
- (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 93
- (Exam Topic 4)
Your company uses Microsoft Intune to manage devices.
You need to ensure that only Android devices that use Android work profiles can enroll in intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer
presents part of the solution.
NOTE Each correct selection is worth one point.

A. From Platform Settings, set Android device administrator Personally Owned to Block.
B. From Platform Settings, set Android Enterprise (work profile) to Allow.
C. From Platform Settings, set Android device administrator Personally Owned to Allow.
D. From Platform Settings, set Android device administrator to Block.

Answer: AB

Explanation:
To ensure that only Android devices that use Android work profiles can enroll in Intune, you need to perform two configurations in the device enrollment restrictions. First, you need to set Android device administrator Personally Owned to Block. This prevents users from enrolling personal Android devices that use device administrator mode. Second, you need to set Android Enterprise (work profile) to Allow. This allows users to enroll corporate-owned or personal Android devices that use work profiles. References: https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

NEW QUESTION 97
- (Exam Topic 4)
You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.
You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard. You need to create a deployment share on Server1.
What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

On Server1:	
Import the Deployment Image Servicing and Management (DISM) PowerShell module.	
Import the WindowsAutopilotIntune Windows PowerShell module.	
Install the Windows Assessment and Deployment Kit (Windows ADK).	
Install the Windows Deployment Services server role.	

Add to the MDT deployment share:	
Windows 10 image and package only	
Windows 10 image and task sequence only	
Windows 10 image only	
Windows 10 image, task sequence, and package	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Install the Windows Deployment Services role. Install and initialize Windows Deployment Services (WDS) On the server:
Open an elevated Windows PowerShell prompt and enter the following command: Install-WindowsFeature -Name WDS -IncludeManagementTools
WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall" WDSUTIL /Set-Server /AnswerClients:All
Box 2: Windows 10 image and task sequence only Create the reference image task sequence
In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-im

NEW QUESTION 100
- (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 102
- (Exam Topic 4)
You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.

MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

You use Distributed File System (DFS) Replication to replicate images in a share named Production. You configure the following settings in the Bootstrap.ini file.

```
[Settings]
Priority=DefaultGateway, Default
[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London
[NewYork]
DeployRoot=\\MDT1\Production$
[London]
DeployRoot=\\MDT2\Production$

KeyboardLocale=en-gb -
[Default]
DeployRoot=\\MDT3\Production$

KeyboardLocale=en-us -
```
You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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
TB1 will download the image from MDT3.	○	○
DT1 will have a KeyboardLocale of en-gb.	○	○
LT1 will download the image from MDT1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
TB1 will download the image from MDT3.	○	⬚◉
DT1 will have a KeyboardLocale of en-gb.	⬚◉	○
LT1 will download the image from MDT1.	⬚◉	○

NEW QUESTION 106
- (Exam Topic 3)
You need to meet the technical requirements for the LEG department computers.
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.

Actions   **Answer Area**

Configure the commercial ID on the LEG
department computers.

Create an Azure Machine Learning service
workspace.

Create an Azure Log Analytics workspace.

Install the Microsoft Monitoring Agent on
the LEG department computers.

Add a solution to a workspace.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a white box Description automatically generated
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-azure-portal

NEW QUESTION 107
- (Exam Topic 3)
You need to prepare for the deployment of the Phoenix office computers. What should you do first?

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

Answer: A

Explanation:
 References:
https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#manage-autopilot-deployment-profiles

NEW QUESTION 110
- (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 111
- (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.
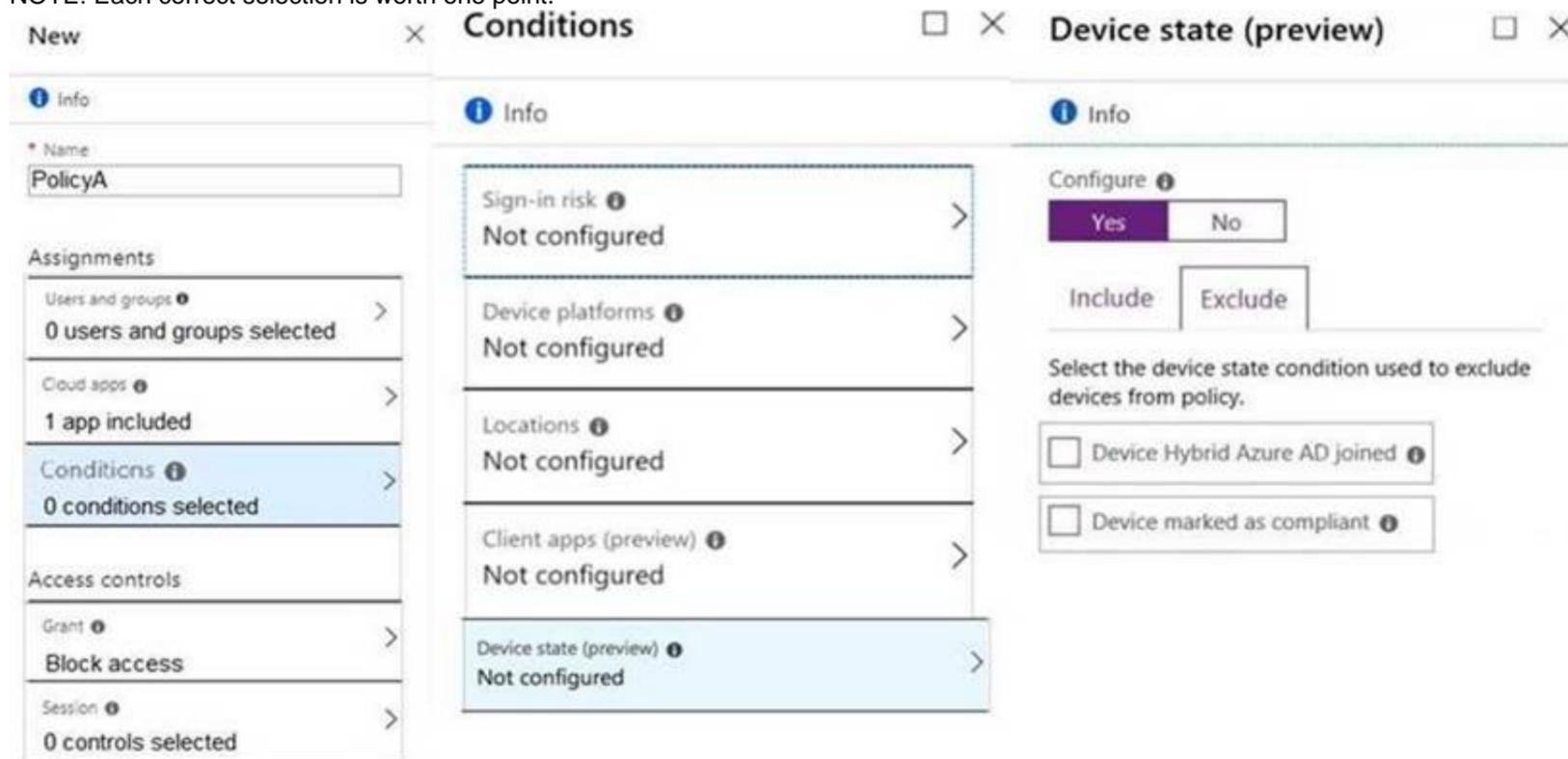
A. Mastered
B. Not Mastered

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 116
- (Exam Topic 3)
To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Policy1:

Device1 only	
Device2 only	
Device3 only	
Device4 only	
Device2 and Device3 only	
Device1 and Device3 only	
Device1, Device2, and Device 3	

Policy2:

Device1 only	
Device2 only	
Device3 only	
Device4 only	
Device2 and Device3 only	
Device1 and Device3 only	
Device1, Device2, and Device 3	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/intune/device-profile-assign

NEW QUESTION 120
- (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.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 125
- (Exam Topic 3)
You need to meet the technical requirements for the IT department. What should you do first?

A. From the Azure Active Directory blade in the Azure portal, enable Seamless single sign-on.
B. From the Configuration Manager console, add an Intune subscription.
C. From the Azure Active Directory blade in the Azure portal, configure the Mobility (MDM and MAM) settings.
D. From the Microsoft Intune blade in the Azure portal, configure the Windows enrollment settings.

Answer: C

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

NEW QUESTION 127
- (Exam Topic 3)
You need to meet the technical requirements for the iOS devices. Which object should you create in Intune?

A. A compliance policy
B. An app protection policy
C. A Deployment profile
D. A device configuration profile

Answer: D

Explanation:
 References:
https://docs.microsoft.com/en-us/intune/device-restrictions-configure https://docs.microsoft.com/en-us/intune/device-restrictions-ios

NEW QUESTION 130
- (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
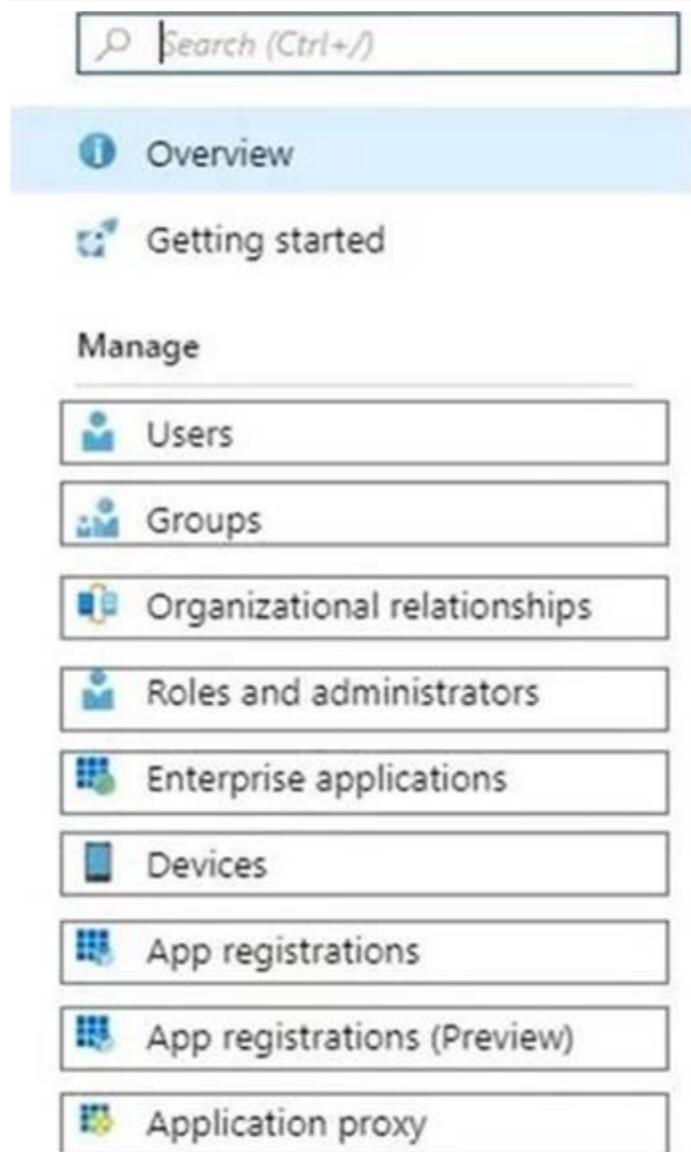

NEW QUESTION 131
- (Exam Topic 2)
You need to meet the technical requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 132
- (Exam Topic 2)
You need to capture the required information for the sales department computers to meet the technical requirements.
Which Windows PowerShell command should you run first?

A. Install-Module WindowsAutoPilotIntune
B. Install-Script Get-WindowsAutoPilotInfo
C. Import-AutoPilotCSV
D. Get-WindowsAutoPilotInfo

Answer: B

Explanation:
 References:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices
"This topic describes how to convert Windows 7 or Windows 8.1 domain-joined computers to Windows 10 devices joined to either Azure Active Directory or Active Directory (Hybrid Azure AD Join) by using Windows Autopilot"

NEW QUESTION 133
- (Exam Topic 2)
What should you use to meet the technical requirements for Azure DevOps?

A. An app protection policy
B. Windows Information Protection (WIP)
C. Conditional access
D. A device configuration profile

Answer: C

Explanation:
 References:
https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access? view=azure-devops

NEW QUESTION 138

- (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 142
- (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 143
- (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 148
- (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 149
- (Exam Topic 1)
You implement the planned changes for Connection1 and Connection2
How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2? To answer select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.
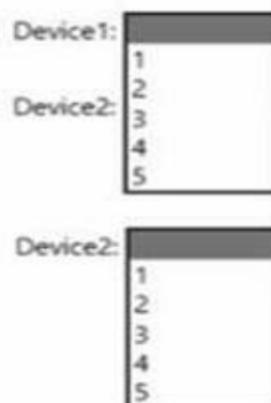
A. Mastered
B. Not Mastered

Answer: A

Explanation:
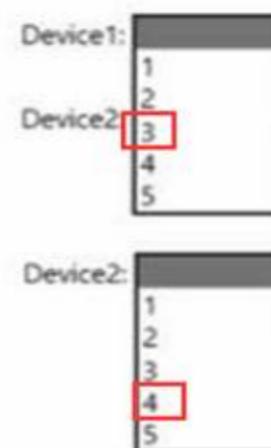
NEW QUESTION 154
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

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 159
- (Exam Topic 1)
You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.
To what should you grant the right to create the computer objects?

A. Server2
B. Server1
C. GroupA
D. DC1

Answer: C

Explanation:
Reference:
https://blog.matrixpost.net/set-up-windows-autopilot-production-environment-part-2/

NEW QUESTION 164
- (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 create and assign a device restrictions profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 165
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1 @contoso.com.
You join a Windows 10 device named Client1 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 accounts | Administrators /add " | AzureAD | \user1@contoso.com" |
| net localgroup | | CONTOSO | |
| net user | | UPN | |

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area
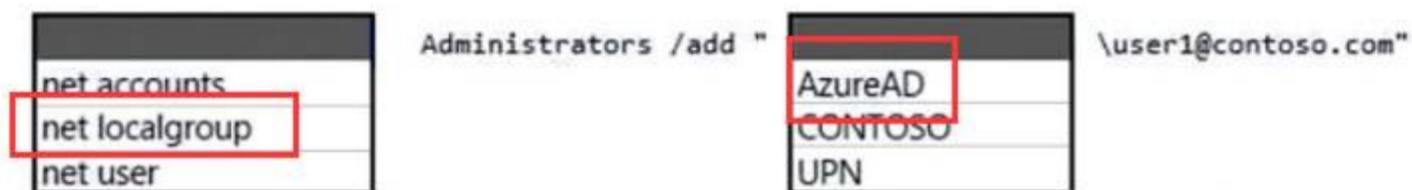
NEW QUESTION 169
- (Exam Topic 4)
You have an Azure AD tenant that contains the devices shown in the following table. You purchase Windows 11 Enterprise E5 licenses.
Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

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

Answer: B

NEW QUESTION 170
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30 days.
You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and
OEM-installed apps must be retained.
What should you use?

A. a Delete action
B. a Retire action
C. a Fresh Start action
D. an Autopilot Reset action

Answer: B

Explanation:
A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are offline for more than 30 days. References:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

---

NEW QUESTION 171
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains a user named User! and a web app named Appl. App1 must only accept modern authentication requests.
You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:
• Assignments
° Users or workload identities: User1
° Cloud apps or actions: App1
• Access controls
° Grant: Block access
You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

A. Filter for devices
B. Device platforms
C. User risk
D. Sign-in risk
E. Client apps

Answer: E

Explanation:
you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13. References: 1: Conditional Access: Block legacy authentication | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy-authentication 2:
What is legacy authentication? | Microsoft Learn
https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/legacy-authentication 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client-apps-condition

NEW QUESTION 172
- (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 175
- (Exam Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown
in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
LON-CL2	✓ Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	✓ Yes
LON-CL4	✓ Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	✓ Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Identified by Intune as a personal device:

| LON-CL2 only |
| LON-CL4 only |
| Both LON-CL2 and LON-CL4 |
| Neither LON-CL2 or LON-CL4 |

Identified by Intune as a corporate device:

| LON-CL2 only |
| LON-CL4 only |
| Both LON-CL2 and LON-CL4 |
| Neither LON-CL2 or LON-CL4 |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register

NEW QUESTION 176
- (Exam Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Intune.
You use the Company Portal app to access and install published apps to enrolled devices. From the Microsoft Intune admin center, you add a Microsoft Store app.
Which two App information types are visible in the Company Portal? NOTE: Each correct selection is worth one point.

A. Privacy URL
B. Information URL
C. Developer
D. Owner

Answer: AC

NEW QUESTION 180
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM). You need to deploy the Microsoft 36S Apps for enterprise suite to all the computers.
What should you do?

A. From the Microsoft Intune admin center, create a Windows 10 device profile.
B. From Azure AD, add an app registration.
C. From Azure A
D. add an enterprise application.
E. From the Microsoft Intune admin center, add an app.

Answer: D

Explanation:
To deploy Microsoft 365 Apps for enterprise to Windows 10 devices that are enrolled in Intune, you need to add an app of type "Windows 10 app (Win32)" in the Microsoft Intune admin center and configure the app settings. You can then assign the app to groups of users or devices. References:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management

NEW QUESTION 184
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	None

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using user1@contoso.com.
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@contoso.com is a member of the local Administrators group on Computer1.	○	○
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	○	○
Admin2@contoso.com can install software on Computer1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	○	○
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	○	○
Admin2@contoso.com can install software on Computer1.	○	○

NEW QUESTION 186
- (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 190
- (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	License
User1	Group1	None
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

Group2 has been assigned in the Enrollment Status Page. You have the devices shown in the following table.

Name	Operating system	Department
Device1	Windows 10 Pro	Marketing
Device2	Windows 11 Home	Research
Device3	Windows 10 Pro	Marketing

You capture and upload the hardware IDs of the devices in the marketing department. You configure Windows Autopilot.
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 complete the Autopilot process on Device1.		
User2 can complete the Autopilot process on Device1.		
User3 can view device setup information during the enrollment phase of Device1.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.		☐
User2 can complete the Autopilot process on Device1.	☐	
User3 can view device setup information during the enrollment phase of Device1.		☐

NEW QUESTION 194
- (Exam Topic 4)
You are replacing 100 company-owned Windows devices.
You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices. The solution must meet the following requirements:
• Back up the user state.
• Minimize administrative effort.
Which task sequence template should you use?

A. Standard Client Task Sequence
B. Standard Client Replace Task Sequence
C. Litetouch OEM Task Sequence
D. Sysprep and Capture

Answer: B

NEW QUESTION 195
- (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 196
- (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 199
- (Exam Topic 4)
You have a Microsoft 365 tenant.
You have devices enrolled in Microsoft Intune.
You assign a conditional access policy named Policy1 to a group named Group1. Policy! restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.
You need to identify which noncompliant devices attempt to access OneDrive for Business. What should you do?

A. From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.
B. From the Microsoft Intune admin center, review Device compliance report.
C. From the Microsoft Intune admin center, review the Noncompliant devices report.
D. From the Microsoft Intune admin center, review the Setting compliance report.

Answer: C

NEW QUESTION 202
- (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 207
- (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 210
- (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 214
- (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 218
- (Exam Topic 4)
In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 and later	Require	Not applicable	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

The Intune compliance policy settings are configured as shown in the following exhibit.

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 / **Not Compliant**

Enhanced jailbreak detection ⓘ — Enabled / **Disabled**

Compliance status validity period (days) ⓘ — 30 ✓

On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	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
On June 4, Device1 is marked as compliant.	○	○
On June 6, Device1 is marked as compliant.	○	○
On June 9, Device2 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO.
Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until june 10th.
Source:
Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.
When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.
This action is supported on all platforms supported by Intune. https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

NEW QUESTION 220
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune. You plan to manage Windows updates by using Intune.
You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.

User experience settings

Automatic update behavior ⓘ	Auto install and restart at maintenance time ⌄
Active hours start * ⓘ	8 AM ⌄
Active hours end * ⓘ	5 PM ⌄
Restart checks ⓘ	**Allow** Skip
Option to pause Windows updates ⓘ	**Enable** Disable
Option to check for Windows updates ⓘ	**Enable** Disable
Change notification update level ⓘ	Use the default Windows Update notifications ⌄
Use deadline settings ⓘ	**Allow** Not configured
Deadline for feature updates ⓘ	5 ✓
Deadline for quality updates ⓘ	2 ✓
Grace period ⓘ	1 ✓
Auto reboot before deadline ⓘ	**Yes** 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

Automatic restarts are blocked [answer choice]. between 8 AM and 5 PM ▼
- before 8 AM
- **between 8 AM and 5 PM**
- after 5 PM

A restart will be forced on a device [answer choice] after the deadline. 5 days ▼
- **1 day**
- 2 days
- 5 days

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Automatic restarts are blocked [answer choice]. between 8 AM and 5 PM ▼
- before 8 AM
- **between 8 AM and 5 PM**
- after 5 PM

A restart will be forced on a device [answer choice] after the deadline. 5 days ▼
- **1 day**
- 2 days
- 5 days

NEW QUESTION 221
- (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
- **net localgroup**
- net user

- AzureAD
- **CONTOSO**
- 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 224
- (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 227
- (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   ④ 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 232
- (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 233
- (Exam Topic 4)
You have an on-premises server named Server! that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

A. Multipath I/O (MPIO)
B. Multipoint Connector
C. Windows Deployment Services (WDS)
D. Windows Server Update Services (WSUS)

Answer: C

NEW QUESTION 237
- (Exam Topic 4)
You have a Microsoft 365 ES subscription that uses Microsoft Intune. You have the apps shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 238
- (Exam Topic 4)

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices. You purchase a Microsoft 365 E5 subscription.
You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.
Which upgrade method should you use?

A. Windows Autopilot
B. a Microsoft Deployment Toolkit (MDT) lite-touch deployment
C. Subscription Activation
D. an in-place upgrade by using Windows installation media

Answer: C

Explanation:
Subscription Activation is a feature that allows you to upgrade from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise without needing a product key or reinstallation. You just need to assign a subscription license (such as Microsoft 365 E5) to the user in Azure AD, and then sign in to the device with that user account. The device will automatically activate Windows Enterprise edition using the firmware-embedded activation key for Windows Pro edition. This method minimizes administrative effort and
simplifies the upgrade process. References: Windows subscription activation, Deploy Windows Enterprise
licenses

NEW QUESTION 241
- (Exam Topic 4)
You use Windows Admin Center to remotely administer computers that run Windows 10.
When connecting to Windows Admin Center, you receive the message shown in the following exhibit.

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

🗀 Go to your Start page

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

Go on to the webpage (Not recommended)

You need to prevent the message from appearing when you connect to Windows Admin Center.
To which certificate store should you import the certificate?

A. Personal
B. Trusted Root Certification Authorities
C. Client Authentication Issuers

Answer: B

NEW QUESTION 244
- (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 245
- (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 249
- (Exam Topic 4)
You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.

Name	Platform	IP address
Device1	Windows	192.168.10.35
Device2	Android	10.10.10.40
Device3	Android	192.168.10.10

The devices are members of a group named Group1.
In Intune, you create a device compliance location that has the following configurations:
• Name: Network1
• IPv4 range: 192.168.0.0/16
In Intune. you create a device compliance policy for the Android platform. The policy has the following configurations:
• Name: Policy1
• Device health: Rooted devices: Block
• Locations: Location: Network1
• Mark device noncompliant: Immediately
• Assigned: Group1
The Intune device compliance policy has the following configurations:
• Mark devices with no compliance policy assigned as: Compliant
• Enhanced jailbreak detection: Enabled
• Compliance status validity period (days): 20
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 compliant. = No

➢ Device1 is marked as noncompliant because it is rooted and the device compliance policy Policy1 blocks rooted devices under the Device health setting1.

➢ Device2 is marked as compliant because it is not rooted and it is within the network location Network1 that is specified in the device compliance policy Policy11.

➢ Device3 is marked as noncompliant because it is outside the network location Network1 that is specified in the device compliance policy Policy11. The device

compliance location setting requires devices to be in a specific network range to be compliant2.

NEW QUESTION 252
- (Exam Topic 4)
You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments. From Deployment Workbench, you modify the WinPE settings and add PowerShell support. You need to generate a new set of WinPE boot image files that contain the updated settings. What should you do?

A. From the Deployment Shares node, update the deployment share.
B. From the Advanced Configuration node, create new media.
C. From the Packages node, import a new operating system package
D. From the Operating Systems node, import a new operating system.

Answer: A

NEW QUESTION 257
- (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 262
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You need to create Endpoint security policies to meet the following requirements:
➢ Hide the Firewall & network protection area in the Windows Security app.
➢ Disable the provisioning of Windows Hello for Business on the devices.
Which two policy types should you use? To answer, select the policies in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated
In the Antivirus policy settings, you can hide the Firewall and network protection area in the Windows Security app.
Windows Hello for Business settings are configured in Identity protection. Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings

NEW QUESTION 264
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain and an Azure AD tenant.
The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

Which device configuration profile type template should you use?

A. Administrative Templates
B. Endpoint protection
C. Device restrictions
D. Custom

Answer: A

Explanation:
To configure the settings shown in the table, you need to use the Administrative Templates device configuration profile type template. This template allows you to configure hundreds of settings that are also available in Group Policy. You can use this template to configure settings such as password policies, account lockout policies, and audit policies. References:
https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows

NEW QUESTION 268
- (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 270
- (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 273
- (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 278
- (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 * ⓘ	Single app, full-screen kiosk ⌄
User logon type * ⓘ	Auto logon (Windows 10, version 1803+) ⌄
Application type * ⓘ	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 * ⓘ	https://contoso.com ✓
Microsoft Edge kiosk mode type ⓘ	Public Browsing (InPrivate) ⌄
Refresh browser after idle time ⓘ	5

Specify Maintenance Window for App Restarts * ⓘ	Require	**Not configured**
Maintenance Window Start Time	MM/DD/YYYY 🗓	h:mm:ss A
Maintenance Window Recurrence ⓘ	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 283
- (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 286
- (Exam Topic 4)
You use Microsoft Endpoint Manager to manage Windows 10 devices.
You are designing a reporting solution that will provide reports on the following:

≫ Compliance policy trends

≫ Trends in device and user enrolment

≫ App and operating system version breakdowns of mobile devices

You need to recommend a data source and a data visualization tool for the design.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Data source:
- Audit logs in Azure Active Directory (Azure AD)
- Audit logs in Microsoft Intune
- Azure Synapse Analytics
- The Microsoft Intune Data Warehouse

Data visualization tool:
- Azure Data Studio
- Microsoft Power BI
- The Azure portal

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/developer/reports-nav-create-intune-reports https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi
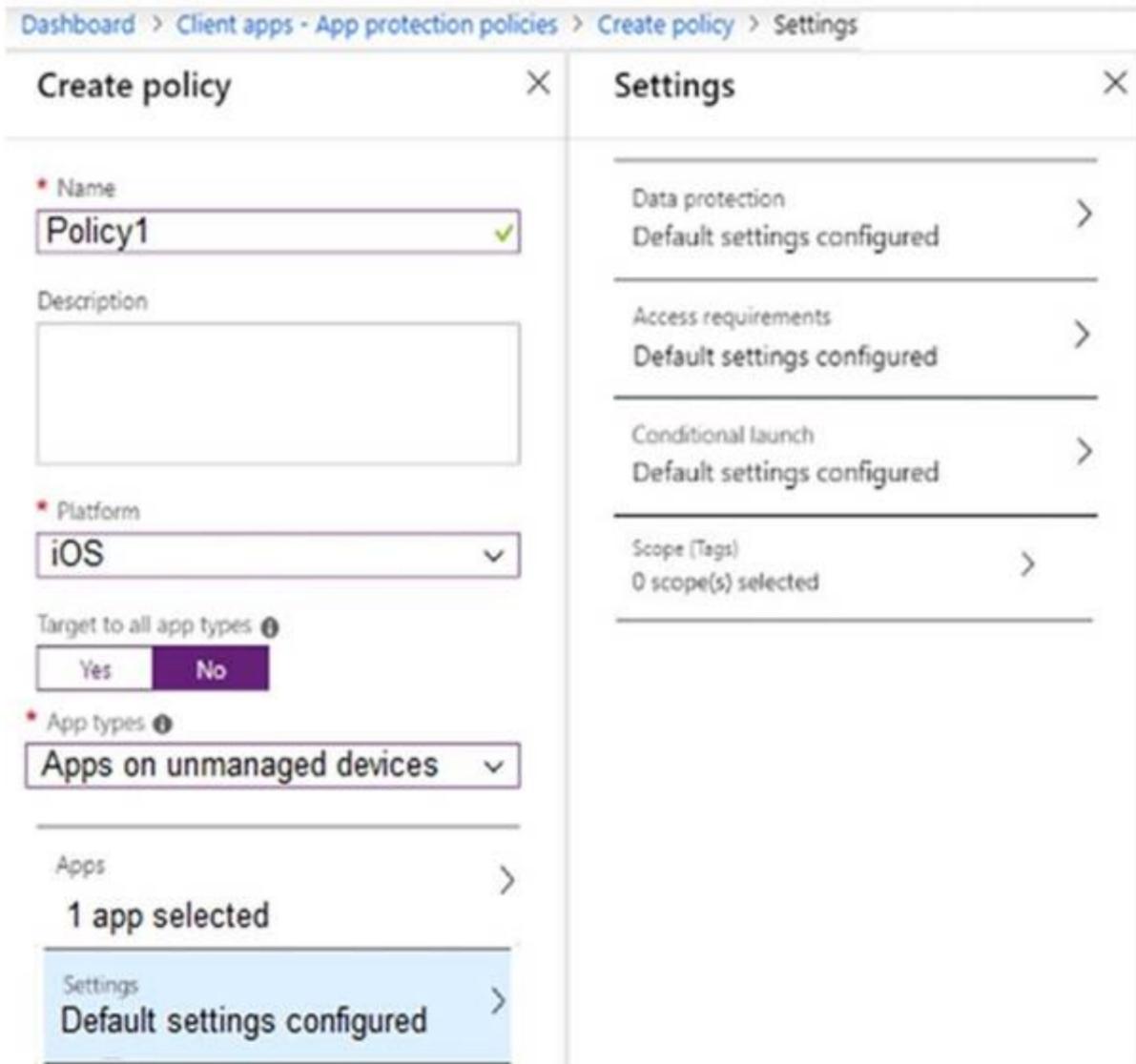
NEW QUESTION 288
- (Exam Topic 4)
You have a Microsoft 365 subscription.
Users have iOS devices that are not enrolled in Microsoft 365 Device Management.
You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)

Dashboard > Client apps - App protection policies > Create policy > Settings

Create policy ✕

* Name
Policy1 ✓

Description

* Platform
iOS ▾

Target to all app types ❶
Yes | No

* App types ❶
Apps on unmanaged devices ▾

Apps ❯
1 app selected

Settings ❯
Default settings configured

Settings ✕

Data protection ❯
Default settings configured

Access requirements ❯
Default settings configured

Conditional launch ❯
Default settings configured

Scope (Tags) ❯
0 scope(s) selected

You need to configure the policy to meet the following requirements:
≫ Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.
≫ Require the users to use an alphanumeric passcode to access the Outlook app.
What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Prevent the users from using Outlook if the operating system version is less than 12.0.0:

▾
Access requirements
Conditional launch
Data protection
Scope

Require the users to use an alphanumeric passcode to access Outlook:

▾
Access requirements
Conditional launch
Data protection
Scope

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios

NEW QUESTION 290
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

A. Import an OS package.
B. Create a selection profile.

C. Add a Gather task to the task sequence.
D. Add a Validate task to the task sequence.

Answer: B

NEW QUESTION 295
- (Exam Topic 4)
You have a hybrid Azure AD tenant.
You configure a Windows Autopilot deployment profile as shown in the following exhibit.
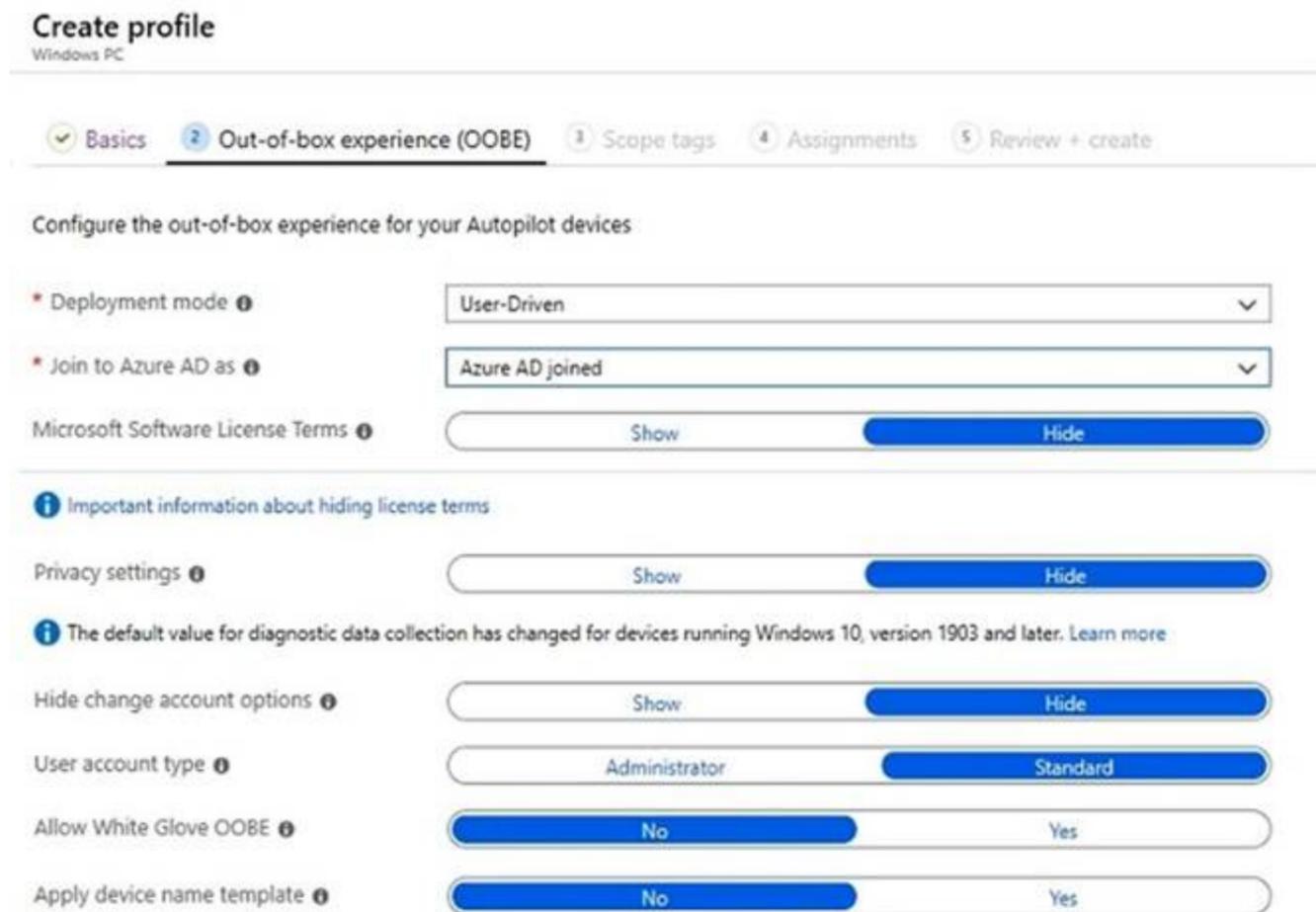
Create profile
Windows PC

✓ Basics | ② Out-of-box experience (OOBE) | ③ Scope tags | ④ Assignments | ⑤ Review + create

Configure the out-of-box experience for your Autopilot devices

* Deployment mode ❶	User-Driven ⌄
* Join to Azure AD as ❶	Azure AD joined ⌄
Microsoft Software License Terms ❶	Show / **Hide**

ℹ Important information about hiding license terms

Privacy settings ❶	Show / **Hide**

ℹ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more

Hide change account options ❶	Show / **Hide**
User account type ❶	Administrator / **Standard**
Allow White Glove OOBE ❶	**No** / Yes
Apply device name template ❶	**No** / Yes

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

To apply the profile to a new computer, you must first | ⌄
- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be | ⌄
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

To apply the profile to a new computer, you must first
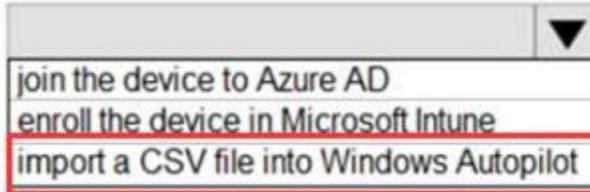
▼
join the device to Azure AD
enroll the device in Microsoft Intune
import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be

▼
joined to Azure AD only
registered in Azure AD only
joined to Active Directory only
joined to Active Directory and registered in Azure AD
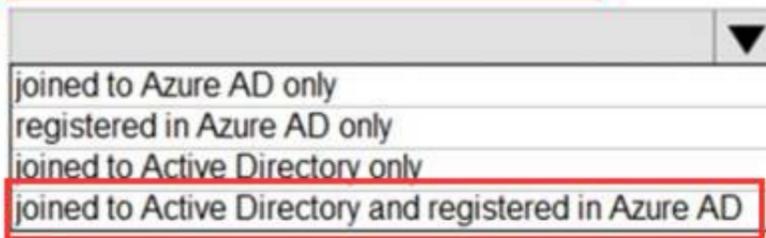
NEW QUESTION 297
- (Exam Topic 4)
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Which groups can you add to Group4?

A. Group2only
B. Group1 and Group2 only
C. Group2 and Group3 only
D. Group1, Group2, and Group3

Answer: C

NEW QUESTION 299
- (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 302
......

Relate Links

100% Pass Your MD-102 Exam with Exambible Prep Materials

https://www.exambible.com/MD-102-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/