

MD-102 Dumps

Endpoint Administrator

<https://www.certleader.com/MD-102-dumps.html>



NEW QUESTION 1

- (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.

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

NEW QUESTION 2

- (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>

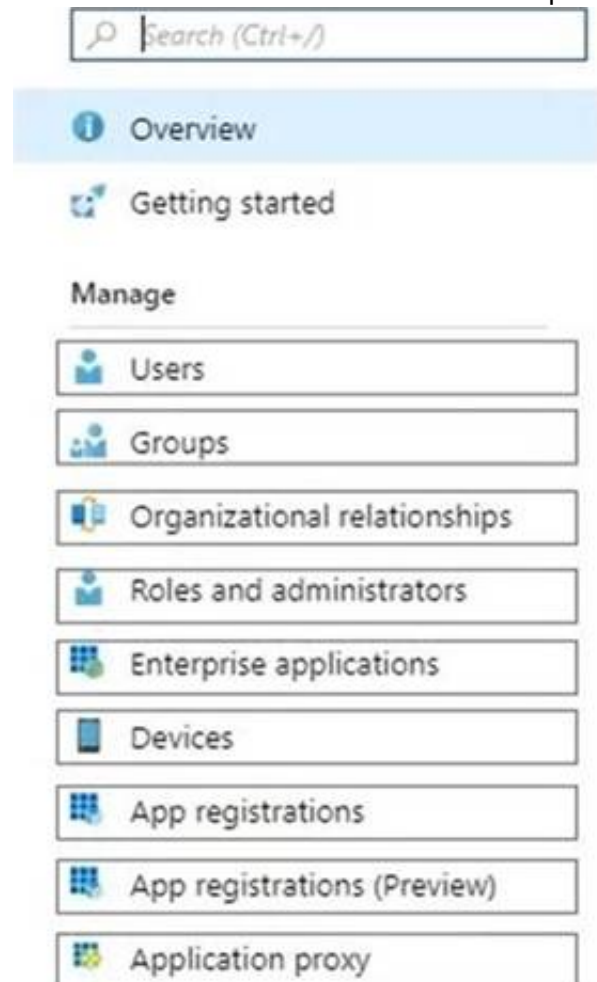
NEW QUESTION 3

- (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 4**

- (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 5

- (Exam Topic 3)

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 6**

- (Exam Topic 3)

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 7**

- (Exam Topic 3)

You have the on-premises servers shown in the following table.

Name	Description
DC1	Domain controller that runs Windows Server 2022
Server1	Standalone server that runs Windows Server 2022
Server2	Member server that runs Windows Server 2022 and has the Remote Access role installed
Server3	Member server that runs Windows Server 2019
Server4	Red Hat Enterprise Linux (RHEL) 8.4 server

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.

You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.

To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Server:

Ports:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Server4

Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.

Box 2: TCP 443 and UDP 443 only

Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.

By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Saerver Configuration – Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.

Incorrect:

TCP 1723 is not used.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-overview>

NEW QUESTION 8

- (Exam Topic 3)

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

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.	<input type="radio"/>	<input type="radio"/>
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>

- 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 9
- (Exam Topic 3)
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 10

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

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

You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11. You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications.

Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 10

- (Exam Topic 3)

You have 100 computers that run Windows 10.

You plan to deploy Windows 11 to the computers by performing a wipe and load installation. You need to recommend a method to retain the user settings and the user data.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Configure known folder redirection in Microsoft OneDrive.
- Run scanstate.exe.
- Run loadstate.exe.
- Enable Enterprise State Roaming.
- Create a system image backup.
- Deploy Windows 11.
- Restore a system image backup.

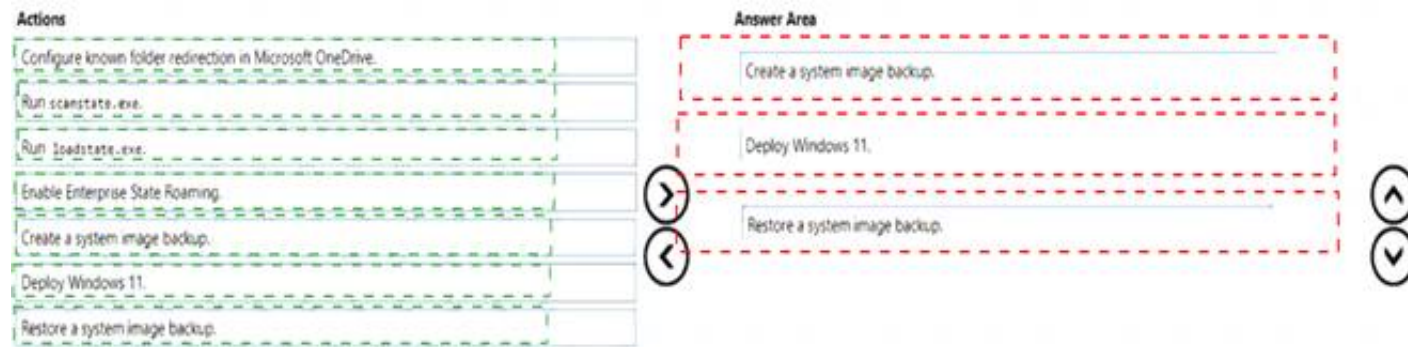
Answer Area



- A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 15

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains a user named User1 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 17

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS devices. You assign CAPolicy1 to Group1. You discover that User1 can still connect to Exchange Online from an iOS device. You need to ensure that CAPolicy1 is enforced. What should you do?

- A. Configure a new terms of use (TOU).
B. Assign CAPolicy1 to Group2.
C. Enable CAPolicy1
D. Add a condition in CAPolicy1 to filter for devices.

Answer: B

Explanation:

Common signals that Conditional Access can take in to account when making a policy decision include the following signals:

* User or group membership

Policies can be targeted to specific users and groups giving administrators fine-grained control over access.

* Device

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Use filters for devices to target policies to specific devices like privileged access workstations.

* Etc.

Reference: <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

NEW QUESTION 19

- (Exam Topic 3)

You have an on-premises server named Server1 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 24

- (Exam Topic 3)

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

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

Answer: B

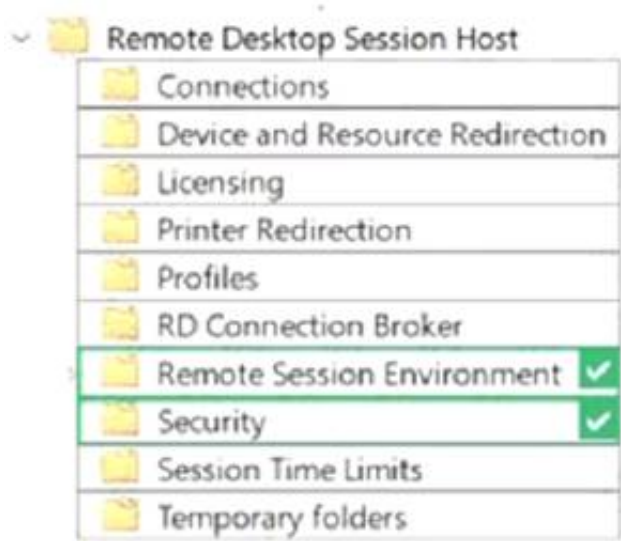
NEW QUESTION 27

- (Exam Topic 3)

Your network contains an Active Directory domain. The domain contains 1.000 computers that run Windows 11. You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:

- Prevent the sharing of clipboard contents.
- Ensure that users authenticate by using Network Level Authentication (NLA).

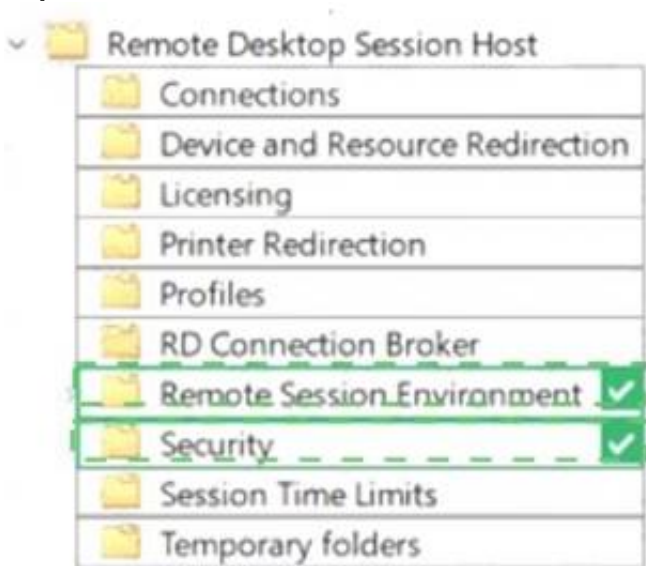
Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 31

- (Exam Topic 3)

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.	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference: <https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll> <https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/>

NEW QUESTION 33

- (Exam Topic 3)

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 37

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

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

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

Answer: B

Explanation:

* Admin1

An application admin has full access to enterprise applications, applications registrations, and application proxy settings.

* Admin2

Mark your app as publisher verified.

In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.

* Admin3

Office Apps admin - Assign the Office Apps admin role to users who need to do the following:

- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health

Reference:

Office Apps admin - Assign the Office Apps admin role to users who need to do the following <https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified>

NEW QUESTION 40

- (Exam Topic 3)

You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs.

The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

- A. 1 only
- B. 2 and 3 only
- C. 1 and 3 only
- D. 1, 2, and 4 on
- E. 1, 2, 3, and 4

Answer: E

Explanation:

All events from Windows event logs are collected in the Log Analytics workspace, regardless of the event level or source. Therefore, events 1, 2, 3, and 4 are all collected in the workspace. References: <https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events>

NEW QUESTION 45

- (Exam Topic 3)

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

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

Answer: C

Explanation:

To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to

deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices.
References:

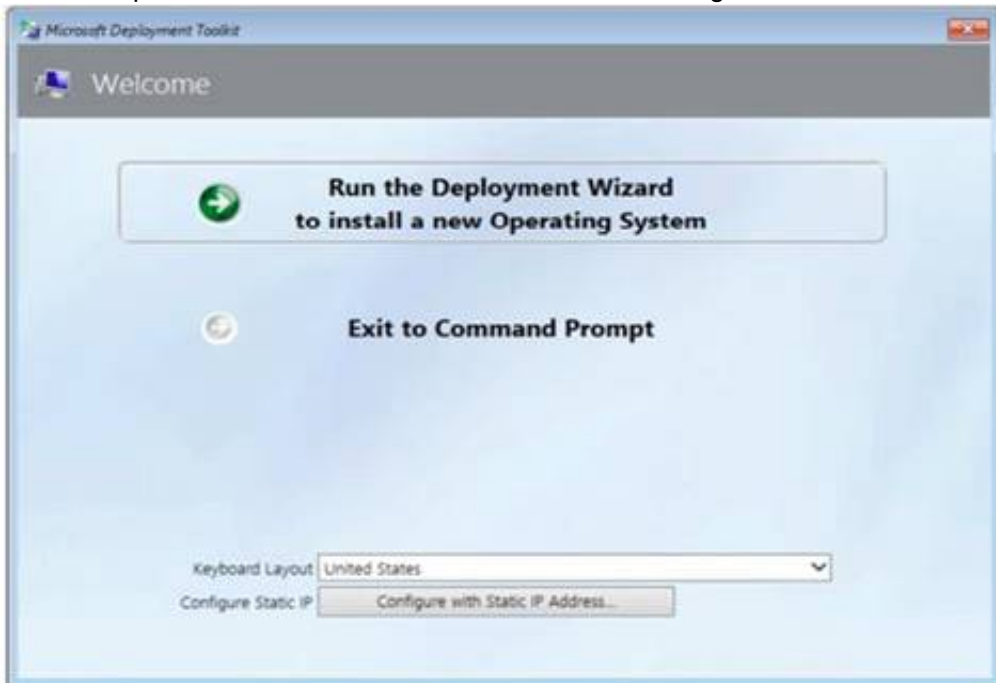
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-install-with-int>

NEW QUESTION 46

- (Exam Topic 3)

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE_x64.iso image and connect to MDT1, the welcome screen appears as shown In the following exhibit.



You need to prevent the welcome screen from appearing when the computers connect to MDT1.

Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Modify the CustomSettings.ini file.	
Update the deployment share.	
Modify the Bootstrap.ini file.	
Replace the ISO image.	
Modify the task sequence.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Modify the Bootstrap.ini file.

Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:

SkipBDDWelcome=YES

Box 2: Modify the CustomSettings.ini file. SkipBDDWelcome

Indicates whether the Welcome to Windows Deployment wizard page is skipped.

For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.

Box 3: Update the deployment share. Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages>

NEW QUESTION 50

- (Exam Topic 3)

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 54

- (Exam Topic 3)
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

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

Answer Area

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

Answer Area

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

NEW QUESTION 56

- (Exam Topic 3)
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 58

- (Exam Topic 3)
You have a computer that runs Windows 10 and contains two local users named User1 and User2. You need to ensure that the users can perform the following actions:

- User 1 must be able to adjust the date and time.
- User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.
To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Groups

Administrators

Event Log Readers

Performance Log Users

Power Users

System Managed Accounts Group

Answer Area

User1:

User2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Groups

Administrators

Event Log Readers

Performance Log Users

Power Users

System Managed Accounts Group

Answer Area

User1: Administrators

User2: Event Log Readers

NEW QUESTION 61

- (Exam Topic 3)

Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.

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

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

computer1

Actions

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

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

Answer Area

Computer1 will be a member of:

Group3 only

Group4 only

Grou5 only

Group3, Group4, and Group5 only

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

Group1 only

Group2 only

Group1 and Group2 only

Group1, Group2, Group3, Group4, and Group5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1 will be a member of:

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

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

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

NEW QUESTION 65

- (Exam Topic 3)

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

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

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 70

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your MD-102 Exam with Our Prep Materials Via below:

<https://www.certleader.com/MD-102-dumps.html>