

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : MD-102

Title : Endpoint Administrator

Version : DEMO

1. Testlet 1

Case study

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG), and finance (FIN) departments.

Contoso recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment

The network contains an Active Directory domain named contoso.com that is synced to Azure AD. All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration

The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	None	GroupB

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	Not applicable	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	Not applicable	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	Not applicable	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	None
Policy2	Group2	Group3
Policy3	Group1	None

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements

Planned changes

Contoso plans to implement the following changes:

- Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
- Implement co-management for the computers.

Technical Requirements

Contoso must meet the following technical requirements:

- Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
- Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
- Create a provisioning package for new computers in the HR department.
- Block iOS devices from sending diagnostic and usage telemetry data.
- Use the principle of least privilege whenever possible.
- Enable the users in the MKG department to use App1.
- Pilot co-management for the IT department.

You need to prepare for the deployment of the Phoenix office computers.

What should you do first?

- A. Generalize the computers and configure the Device settings from the Microsoft Entra admin center.
- B. Extract the serial number of each computer to an XML file and upload the file from the Microsoft Intune admin center.
- C. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.
- D. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Microsoft Entra admin center.
- E. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.

Answer: C

Explanation:

To manage devices through Microsoft Store for Business and Education, you'll need a .csv file that contains specific information about the devices. You should be able to get this from your Microsoft account contact, or the store where you purchased the devices. Upload the .csv file to Microsoft Store to add the devices.

Note:

Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.

Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.

Reference: <https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices>

2.HOTSPOT

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

User1 can enroll a maximum of:

	▼
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

User2 can enroll a maximum of:

	▼
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

Answer:

Answer Area

User1 can enroll a maximum of:

	▼
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

User2 can enroll a maximum of:

	▼
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

Explanation:

Box 1: 10 devices

User1 is a member of GroupA. GroupA device limit is 10.

Box 2: 15 devices

User2 is a member of GroupB. GroupB device limit is 15.

Deploy Windows client

3. Testlet 2

Case study

Overview

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment

Network Environment

The network contains an on-premises Active Directory domain named adatum.com.

The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration

Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are 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)  

The Automatic Enrolment settings have the following configurations:

- MDM user scope GroupA
- MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

- Name: Protection1
- Folder protection: Enable
- List of apps that have access to protected folders: CV\AppA.exe
- List of additional folders that need to be protected: D:\Folder1
- Assignments - Included groups: Group2, GroupB

Windows Autopilot Configuration

ADatum has a Windows Autopilot deployment profile 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	User-Driven
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	Group2

Currently, there are no devices deployed by using Windows Autopilot.
The Intune connector for Active Directory is installed on Server1.

Contoso plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
- Deploy a network boundary configuration profile that will have the following settings:
 - Name Boundary 1
 - Network boundary 192.168.1.0/24
 - Scope tags: Tag 1
 - Assignments;

* included groups: Group 1. Group2

• Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

- Name: Connection 1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
 - * Included groups: Group1. Group2, GroupA
 - * Excluded groups: —
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
 - included groups: GroupA
 - Excluded groups: GroupB

Technical Requirements

Contoso must meet the following technical requirements:

- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

HOTSPOT

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 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

User1 is a Cloud device administrator.

Local administrative privileges are required when enrolling an already configured Windows 10 device in Intune.

Cloud Device Administrator

Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.

Note: The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

Box 2: Yes

User2 is an Azure AD joined device local administrator.

Azure AD Joined Device Local Administrator

This role is available for assignment only as an additional local administrator in Device settings. Users with this role become local machine administrators on all Windows 10 devices that are joined to Azure Active Directory. They do not have the ability to manage devices objects in Azure Active Directory.

Box 3: No

User3 is a Global reader.

Global Reader

Users in this role can read settings and administrative information across Microsoft 365 services but can't take management actions.

Reference: <https://docs.microsoft.com/en-us/troubleshoot/mem/intune/no-permission-to-enroll-windows-devices>

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

4.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. Server1

- B. DC1
- C. GroupA
- D. Server2

Answer: A

Explanation:

Scenario:

The Intune connector for Active Directory is installed on Server1.

Contoso must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

Administrative effort must be minimized.

Note: To be clear, the entire domain join process will work without any direct connection to the on-premise network and domain controllers. The computer object is created on-premises through the Intune Connector for Active Directory triggered by the Windows Autopilot and Intune.

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

5.Which user can enroll Device6 in Intune?

- A. User4 and User1 only
- B. User4 and User2 only
- C. User4, User1, and User2 only
- D. User1, User2, User3, and User4

Answer: D

Explanation:

All the users can enroll devices to Intune.

Deploy Windows client