QUESTION 15
HOTSPOT
Your company has a Microsoft Azure Active Directory (Azure AD) tenant and computers that run Windows 10.

The company uses Microsoft Intune to manage the computers.

The Azure AD tenant has the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Intune are configured as shown in the following table:

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

User3 is a device enrollment manager (DEM) in Intune.

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 a Windows device in Intune.	○	○
User2 can enroll a Windows device in Intune.	○	○
User3 can enroll an iOS device in Intune.	○	○

Correct Answer:

Statements	Yes	No
User1 can enroll a Windows device in Intune.	○	[○]
User2 can enroll a Windows device in Intune.	○	[○]
User3 can enroll an iOS device in Intune.	[○]	○

QUESTION 16
You manage 1,000 computers that run Windows 10. All the computers are enrolled in Microsoft Intune. You manage the servicing channel settings of the computers by using Intune.

You need to review the servicing status of a computer.

What should you do?

A. From Device configuration-Profiles, view the device status.
B. From Device compliance, view the device compliance.
C. From Software updates, view the audit logs.
D. From Software updates, view the Per update ring deployment state.

Correct Answer: D
Explanation:
https://docs.microsoft.com/en-us/intune/windows-update-compliance-reports

QUESTION 17
You need to assign the same deployment profile to all the computers that are configured by using Windows Autopilot.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: each correct selection is worth one point.

A. Join the computers to Microsoft Azure Active Directory (Azure AD)
B. Assign a Windows AutoPilot deployment profile to a group
C. Join the computers to an on-premises Active Directory domain
D. Create a Microsoft Azure Active Directory (Azure AD) group that has dynamic membership rules and uses the operatingSystem tag
E. Create a Group Policy object (GPO) that is linked to a domain
F. Create a Microsoft Azure Active Directory (Azure AD) group that has dynamic membership rules and uses the ZTDID tag

Correct Answer: BF
Explanation:
https://www.petervanderwoude.nl/post/automatically-assign-windows-autopilot-deployment-profile-to-windowsautopilot-devices/

QUESTION 18
HOTSPOT

You have a computer named Computer1 that runs Windows 10.

Computer1 has the users shown in the following table.

Name	Member of
User1	Administrators
User2	Replicator
User3	Guests

User1 signs in to Computer1, creates the following files, and then signs out:

- docx in C:\Users\User1\Desktop
- docx in C:\Users\Public\Public Desktop
- docx in C:\Users\Default\ Desktop

User3 signs in to Computer1 and creates a file named File4.docx in C:\Users\User3\Desktop.

User2 has never signed in to Computer1.

How many DOCX files will appear on the desktop of each user the nest time each user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Number of documents that will appear for User1:

0
1
2
3
4

Number of documents that will appear for User2:

0
1
2
3
4

Number of documents that will appear for User3:

0
1
2
3
4

Correct Answer:

Number of documents that will appear for User1:

0
1
2
3
4

Number of documents that will appear for User2:

0
1
2
3
4

Number of documents that will appear for User3:

0
1
2
3
4

QUESTION 19
Your company has a Microsoft 365 subscription.

The company uses Microsoft Intune to manage all devices.

The company uses conditional access to restrict access to Microsoft 365 services for devices that do not comply with the company's security policies.

You need to identify which devices will be prevented from accessing Microsoft 365 services.

What should you use?

A. The Device Health solution in Windows Analytics.
B. Windows Defender Security Center.
C. The Device compliance blade in the Intune admin center.
D. The Conditional access blade in the Azure Active Directory admin center.

Correct Answer: C