Prüfungsnummer:MD-101

Prüfungsname: Managing Modern Desktops

Version:demo

https://www.it-pruefungen.ch/

Achtung: Aktuelle englische Version zu MD-101 bei uns ist gratis!!

1. Sie sind als Administrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen verfügt über eine Infrastruktur, die Folgendes umfasst:

Einen Microsoft 365-Mandanten
Eine Active Directory-Gesamtstruktur
Microsoft Store for Business
Einen Server für den Schlüsselverwaltungsdienst (Key Management Service, KMS)
Einen Windows-Bereitstellungsdienste-Server (Windows Deployment Services, WDS)
Einen Microsoft Azure Active Directory (Azure AD) Premium-Mandanten

Das Unternehmen kauft 100 neue Computer, auf denen Windows 10 ausgeführt wird.
Sie müssen sicherstellen, dass die neuen Computer mithilfe von Windows AutoPilot automatisch mit Azure AD verbunden werden.
Was sollten Sie verwenden?
(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)
Abbildung

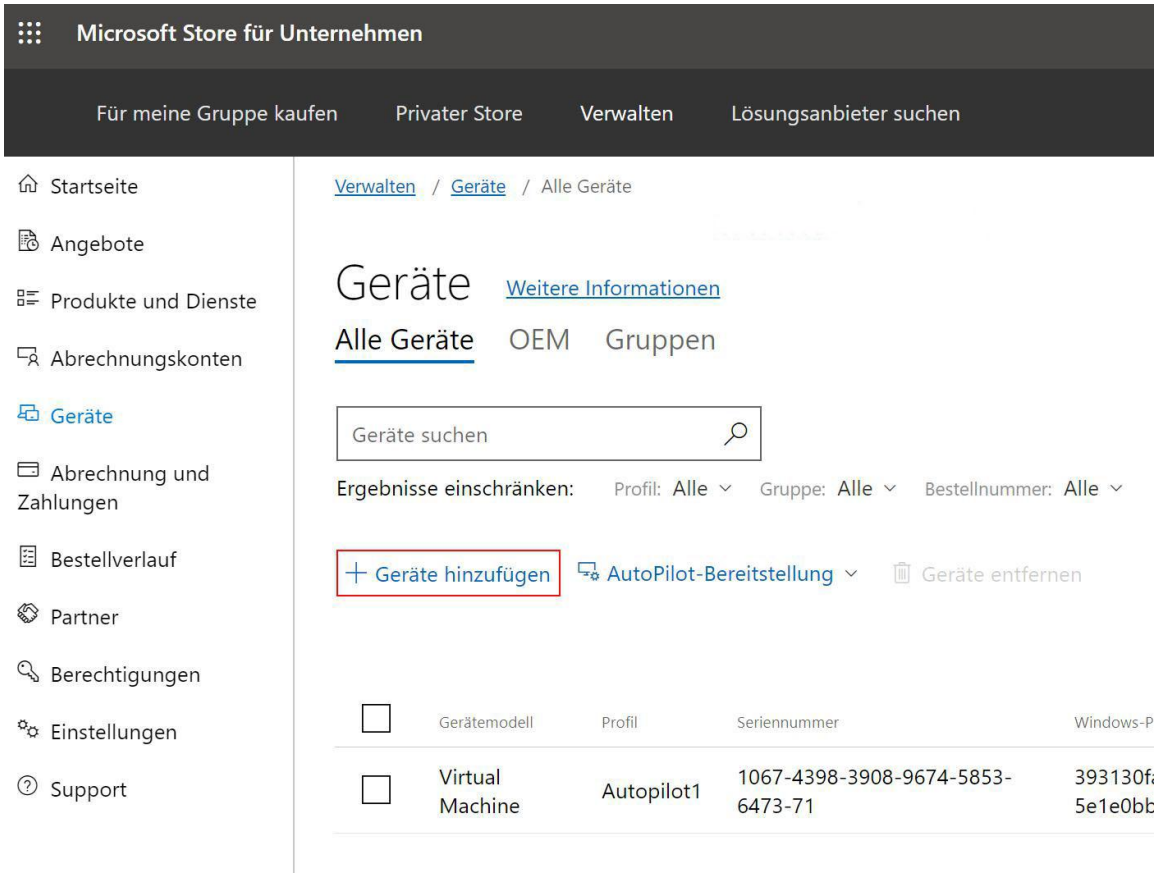
A.Verwaltungstool: Azure Active Directory Admin Center
Von jedem Computer benötigte Informationen: MAC-Adresse und Computername
B.Verwaltungstool: Azure Active Directory Admin Center
Von jedem Computer benötigte Informationen: Geräte-Seriennummer und Hardwarehash
C.Verwaltungstool: Microsoft Store for Business
Von jedem Computer benötigte Informationen: Geräte-Seriennummer und Hardwarehash
D.Verwaltungstool: Microsoft Store for Business
Von jedem Computer benötigte Informationen: Volume License Key and computer name
E.Verwaltungstool: Volume Activation Verwaltungstool (VAMT)-Konsole
Von jedem Computer benötigte Informationen: Volume License Key and computer name
F.Verwaltungstool: Windows-Bereitstellungsdienste-Konsole

Von jedem Computer benötigte Informationen: MAC-Adresse und Computername

Korrekte Antwort: C

Erläuterungen:
Vor der Bereitstellung eines Geräts mit Windows Autopilot, muss das Gerät mit dem Windows Autopilot Deployment-Dienst registriert werden. Im Idealfall würde dies durch den OEM, Händler, oder Verteiler, von dem die Geräte erworben wurden, durchgeführt. Sie können die Registrierung jedoch auch manuell durchführen.
Für die Registrierung von Geräten in Windows AutoPilot werden die Hardware-IDs (auch bekannt als ein Hardwarehash) und die Seriennummern der Geräte benötigt. Die Produkt-ID kann optional angegeben werden.

Für das Registrieren der Geräte können Sie Intune im Azure-Portal oder den Windows Store for Business verwenden.

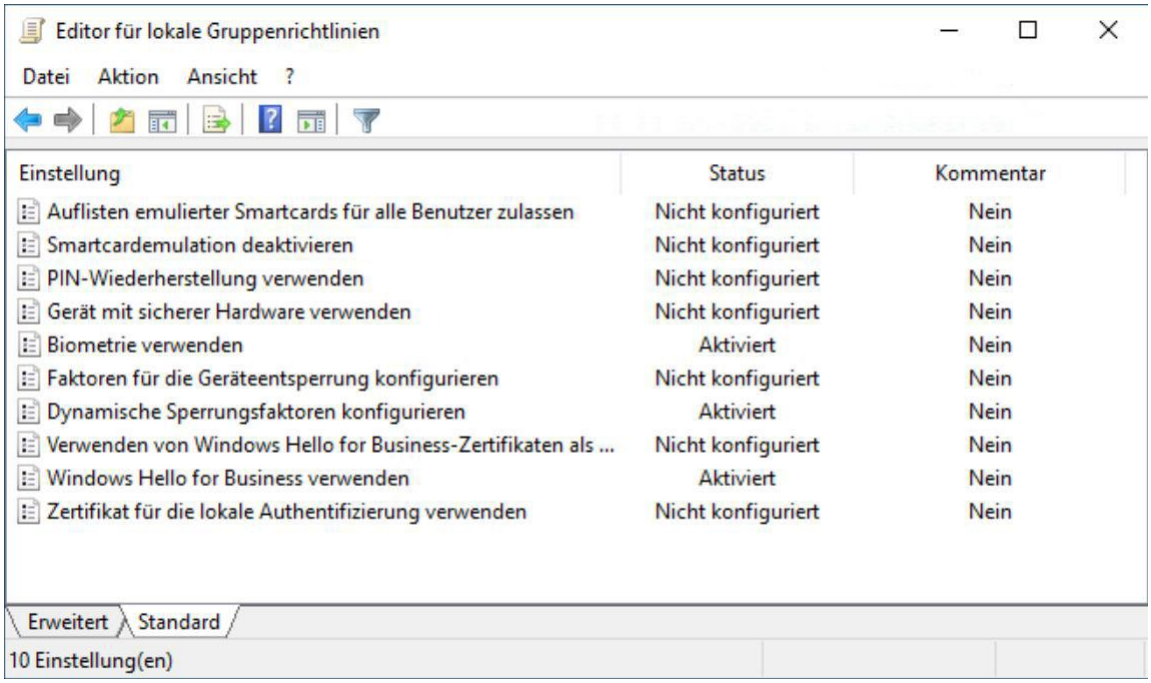


Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Registrieren von Windows-Geräten in Intune mithilfe von Windows Autopilot

2. Ihr Unternehmen kauft neue Computer, auf denen Windows 10 ausgeführt wird. Die Computer verfügen über Kameras, die Windows Hello for Business unterstützen.

Sie konfigurieren die Gruppenrichtlinieneinstellungen von Windows Hello for Business wie in der folgenden Abbildung gezeigt:



Welches sind zwei gültige Methoden, die ein Benutzer für die Anmeldung nutzen kann? (Jede korrekte Antwort stellt einen Teil der Lösung dar. Wählen Sie zwei Antworten.)

A.Gesichtserkennung
B.Eine Bluetooth aktivierte Smartwatch
C.Einen PIN
D.Einen USB-Schlüssel

Korrekte Antwort: A, C

Erläuterungen:
Windows Hello for Business ist aktiviert und ermöglicht das Anmelden eines Benutzers durch Gesichtserkennung.
Die Richtlinie "Dynamische Sperrungsfaktoren konfigurieren" konfiguriert standardmäßig die folgende Regel:

<rule schemaVersion="1.0"> <signal type="bluetooth" scenario="Dynamic Lock" classOfDevice="512" rssiMin="-10" rssiMaxDelta="-10"/> </rule>

Die Regel aktiviert die dynamische Sperre. Die dynamische Sperre stellt sicher, dass der Computer gesperrt wird, wenn der Benutzer sein gekoppeltes mobiles Bluetooth-Gerät aus dem Verbindungsbereich des Computers entfernt.
Beschreibung der aktivierten Richtlinien
Biometrie verwenden

Windows Hello for Business ermöglicht Benutzern die Verwendung der biometrischen Erkennung, z. B. durch Gesicht und Fingerabdruck, als Alternative zu PINs. Benutzer müssen jedoch trotzdem eine PIN konfigurieren, die im Fall einer Störung verwendet wird.

Wenn Sie die Richtlinieneinstellung aktivieren oder nicht konfigurieren, lässt Windows Hello for Business die Verwendung der biometrischen Erkennung zu.

Wenn Sie die Richtlinieneinstellung deaktivieren, verhindert Windows Hello for Business die Verwendung der biometrischen Erkennung.

HINWEIS: Durch das Deaktivieren dieser Richtlinie wird der Benutzer daran gehindert, die biometrische Erkennung auf dem Gerät zu verwenden; dies gilt für alle Kontotypen.

Dynamische Sperrungsfaktoren konfigurieren
Konfigurieren Sie eine durch Trennzeichen getrennte Liste von Signalregeln im XML-Format für jeden Signaltyp.

Wenn Sie diese Richtlinieneinstellung aktivieren, wird anhand dieser Signalregeln festgestellt, ob der Benutzer abwesend ist, und das Gerät automatisch gesperrt.

Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Benutzer die Sperrung mithilfe der vorhandenen Sperroptionen fortsetzen.

Windows Hello for Business verwenden
Windows Hello for Business ist eine alternative Anmeldemethode für Windows, bei der Sie anstelle von Kennwörtern, Smartcards oder virtuellen Smartcards Ihr Active Directory- oder Azure Active Directory-Konto verwenden können.

Wenn Sie diese Richtlinie aktivieren, stellt das Gerät Windows Hello for Business mithilfe von Schlüsseln oder Zertifikaten für alle Benutzer bereit.

Wenn Sie diese Richtlinieneinstellung deaktivieren, stellt das Gerät Windows Hello for Business für keinen Benutzer bereit.

Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, können Benutzer Windows Hello for Business als Komfortanmeldung zur Verschlüsselung ihres Domänenkennworts bereitstellen.

Aktivieren Sie das Kontrollkästchen "Windows Hello-Bereitstellung nach der Anmeldung nicht starten", wenn Sie Windows Hello for Business mithilfe einer Drittanbieterlösung bereitstellen.

Wenn Sie das Kontrollkästchen "Windows Hello-Bereitstellung nach der Anmeldung nicht starten" aktivieren, wird die Bereitstellung von Windows Hello for Business nicht

automatisch nach der Benutzeranmeldung gestartet.

Wenn Sie das Kontrollkästchen "Windows Hello-Bereitstellung nach der Anmeldung nicht starten" nicht aktivieren, wird die Bereitstellung von Windows Hello for Business nach der Benutzeranmeldung automatisch gestartet.

3. Sie haben 10 Computer, auf denen Windows 7 ausgeführt wird. Die Computer haben die folgende Ausstattung und Konfiguration:

- Eine einzelne Festplatte, die im MBR-Partitionsstil initialisiert ist
- Einen deaktivierten Trusted Platform Module (TPM)-Chip
- Deaktivierte Hardware-Virtualisierung
- UEFI-Firmware im BIOS-Modus
- Aktivierte Data Execution Prevention (DEP)

Sie möchten die Computer auf Windows 10 aktualisieren.
Sie müssen sicherstellen, dass die Computer den sicheren Start (Secure Boot) verwenden können.
Welche zwei Aktionen sollten Sie ausführen?
(Jede korrekte Antwort stellt einen Teil der Lösung dar. Wählen Sie zwei Antworten.)

A.Konvertieren Sie den MBR-Datenträger in einen GPT-Datenträger.
B.Aktivieren Sie den TPM-Chip.
C.Deaktivieren Sie Data Execution Prevention (DEP).
D.Aktivieren Sie die Hardwarevirtualisierung.
E.Konvertieren Sie die Firmware von BIOS nach UEFI.

Korrekte Antwort: A, E

Erläuterungen:
Secure Boot ist ein Sicherheitsstandard, der von Mitgliedern der PC-Industrie entwickelt wurde, um sicherzustellen, dass ein Gerät nur mit Software startet, die vom Original Equipment Manufacturer (OEM) als vertrauenswürdig eingestuft wird. Wenn der PC startet, prüft die Firmware die Signatur jeder Boot-Software, einschließlich UEFI-Firmware-Treiber (auch als Option-ROMs bezeichnet), EFI-Anwendungen und des Betriebssystems. Wenn die Signaturen gültig sind, startet der PC, und die Firmware gibt dem Betriebssystem die Kontrolle.
Info: Im BIOS-Setup können Sie auch bei UEFI-Firmware einstellen, dass das Betriebssystem im BIOS-Modus starten soll. Secure Boot funktioniert nur, wenn das System im UEFI-Modus bootet. Im UEFI-Modus ist ein Datenträger mit GUID-Partitionstabelle (GPT) Pflicht.

4. Ihr Netzwerk enthält eine Active Directory-Domäne. Die Domäne enthält 2.000 Computer, auf denen Windows 10 ausgeführt wird.

Sie implementieren die Hybridbereitstellung von Microsoft Azure Active Directory (Azure AD) und Microsoft Intune.
Sie müssen alle vorhandenen Computer automatisch bei Azure AD registrieren und die Computer bei Intune registrieren. Ihre Lösung muss den Verwaltungsaufwand möglichst gering halten.
Was verwenden Sie?

A.Einen DNS-Eintrag für die AutoErmittlung.
B.Ein Windows AutoPilot-Bereitstellungsprofil.
C.Einen Dienstverbindungspunkt (SCP) für die AutoErmittlung.
D.Ein Gruppenrichtlinienobjekt (GPO).

Korrekte Antwort: D

Erläuterungen:
In der Aufgabe heißt es:
"Sie implementieren die Hybridbereitstellung von Microsoft Azure Active Directory (Azure AD)".

Die hybride Bereitstellung von Azure AD beinhaltet Azure AD Hybrid Join. Azure Active Directory (Azure AD) Hybrid Join ist ein Prozess für die automatische Registrierung Ihrer lokalen in die Domäne eingebundenen Geräte bei Azure AD. Der Prozess basiert auf Azure AD Connect für die Synchronisation von Benutzer- und Computerobjekten.

Der erste Teil der Aufgabe ist bereits fertig. Wir brauchen uns nur um die Intune-Registrierung zu kümmern.
Ab Windows 10, Version 1709, können Sie eine Gruppenrichtlinie verwenden, um die automatische Registrierung von Active Directory-Domänengeräten (AD) für Intune auszulösen.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Enroll a Windows 10 device automatically using Group Policy

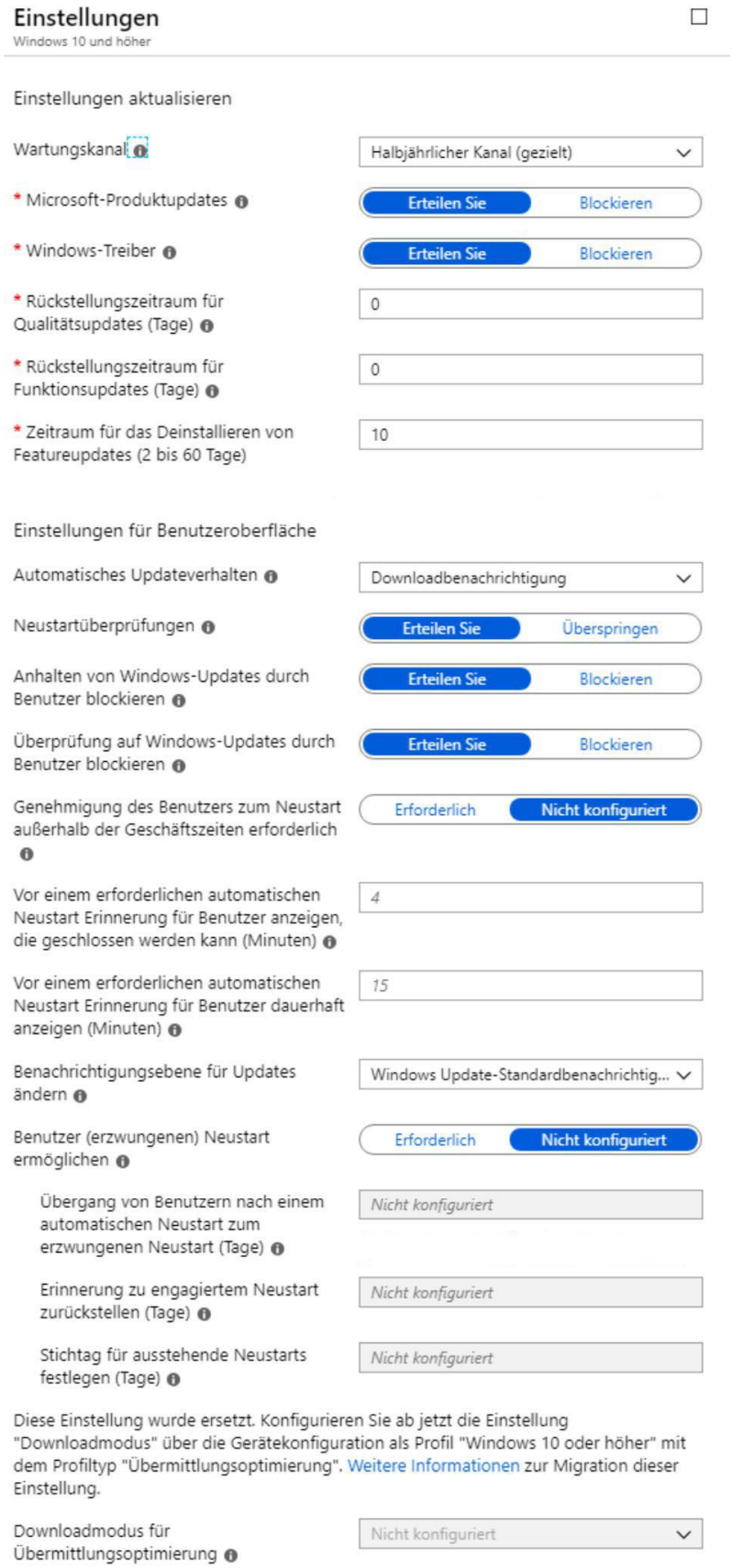
5. Ihr Netzwerk enthält eine Active Directory-Domäne. Die Domäne enthält Computer, auf denen Windows 10 ausgeführt wird und die bei Microsoft Intune registriert sind. Updates werden mithilfe von Windows Update for Business bereitgestellt.
Benutzer in einer Gruppe mit dem Namen Gruppe1 müssen die folgenden Anforderungen erfüllen:

Updateinstallationen dürfen an jedem Tag zwischen 00:00 und 05:00 Uhr erfolgen.

Updates müssen von Microsoft und von anderen Computern des Unternehmens heruntergeladen werden, auf denen die Updates bereits heruntergeladen wurden.

Sie müssen die Windows 10-Update-Ringe in Intune konfigurieren, um die Anforderungen

zu erfüllen.
Welche zwei Einstellungen ändern Sie?
(Um zu antworten, wählen Sie die entsprechenden Einstellungen im Antwortbereich aus. Sie erhalten für jede korrekte Auswahl einen Punkt.)
Abbildung



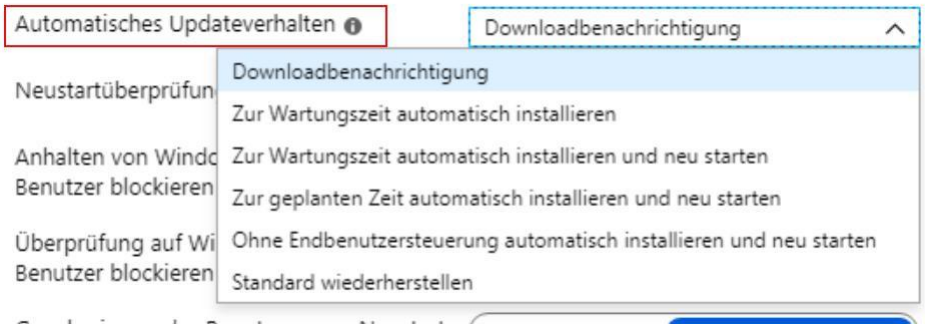
A.Wartungskanal

B.Automatisches Updateverhalten

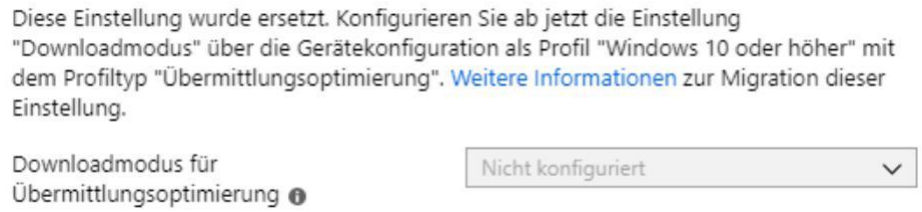
C.Genehmigung des Benutzers zum Neustart außerhalb der Geschäftszeiten erforderlich
D.Benachrichtigungsebene für Updates ändern
E.Benutzer (erzwungenen) Neustart ermöglichen
F.Downloadmodus für Übermittlungsoptimierung

Korrekte Antwort: B, F

Erläuterungen:
Die Option "Automatisches Updateverhalten" steuert das Verhalten der Updateinstallation. Die Option ist so festgelegt, das Benutzer lediglich benachrichtigt werden. Die Einstellung muss so gewählt werden, dass Updates automatisch zur festgelegten Wartungszeit installiert werden.



Der "Downloadmodus für Übermittlungsoptimierung" ermöglichte das Aktivieren der Übermittlungsoptimierung.



Anmerkung: Die Konfiguration der Option wurde zwischenzeitlich verlegt.

6. Sie haben 200 Computer, auf denen Windows 10 ausgeführt wird. Die Computer sind Microsoft Azure Active Directory (AD) beigetreten und bei Microsoft Intune registriert.
Sie müssen das die Self-Service-Kennwortzurücksetzung auf dem Anmeldebildschirm aktivieren.
Welche Einstellungen sollten Sie in Microsoft Intune konfigurieren?

A.Gerätekonfiguration
B.Gerätekompatibilität
C.Geräteregistrierung
D.Bedingter Zugriff

Korrekte Antwort: A

Erläuterungen:
Die Bereitstellung der Konfigurationsänderung zum Aktivieren der Kennwortzurücksetzung über den Anmeldebildschirm mithilfe von Intune ist die flexibelste Methode. Mit Intune können Sie die Konfigurationsänderung für eine bestimmte Gruppe von Computern bereitstellen, die Sie definieren. Diese Methode erfordert die Registrierung des Gerätes über Intune.
Erstellen einer Richtlinie für die Gerätekonfiguration in Intune

Melden Sie sich beim Azure-Portal an, und klicken Sie auf Intune.

Erstellen Sie ein neues Profil für die Gerätekonfiguration, indem Sie zu Gerätekonfiguration > Profile > Profil erstellen navigieren.

Geben Sie einen aussagekräftigen Namen für das Profil an.

Geben Sie optional eine aussagekräftige Beschreibung des Profils an.

Plattform Windows 10 und höher

Profiltyp Benutzerdefiniert

Konfigurieren von Einstellungen

Fügen Sie mit Hinzufügen die folgende OMA-URI-Einstellung hinzu, um den Link „Kennwort zurücksetzen“ zu aktivieren.

Geben Sie einen aussagekräftigen Namen an, um den Zweck der Einstellung zu verdeutlichen.

Geben Sie optional eine aussagekräftige Beschreibung der Einstellung an.

Festlegung von OMA-URI auf ./Vendor/MSFT/Policy/Config/Authentication/AllowAadPasswordReset

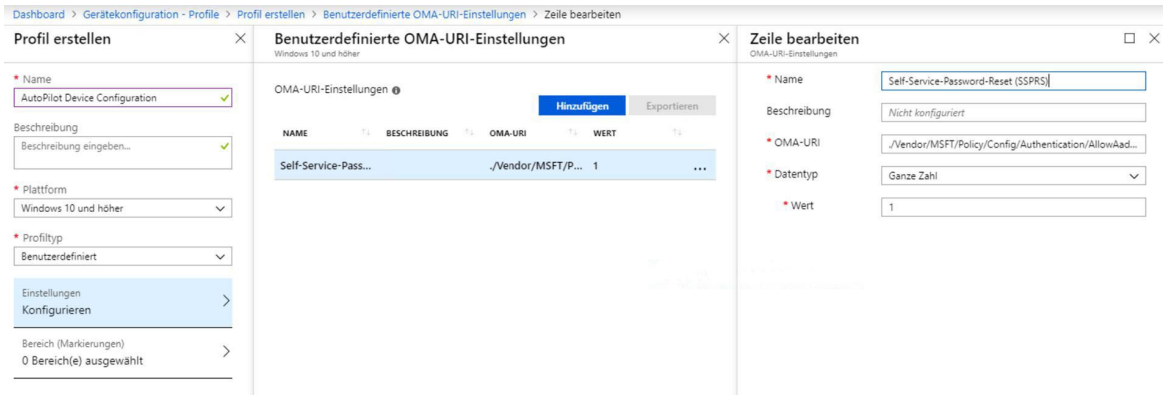
Festlegung von Data type auf Integer

Festlegung von Value auf 1

Klicken Sie auf OK

Klicken Sie auf OK

Klicken Sie auf Erstellen



Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Tutorial: Azure AD-Kennwortzurücksetzung über den Anmeldebildschirm

7. Sie haben einen Windows 10 Computer mit dem Namen Computer1. Auf Computer1 sind die in der folgenden Tabelle gezeigten Benutzer konfiguriert:

Name	Mitglied von
Benutzer1	Administratoren
Benutzer2	Replikations-Operator
Benutzer3	Gäste

Benutzer1 meldet sich an Computer1 an, erstellt die folgenden Dateien und meldet sich dann ab:

Datei1.docx in C:\Users\Benutzer1\Desktop
Datei2.docx in C:\Users\Public\Public Desktop
Datei3.docx in C:\Users\Default\Desktop

Benutzer3 meldet sich bei Computer1 an und erstellt eine Datei mit dem Namen Datei4.docx in C:\Users\Benutzer3\Desktop.

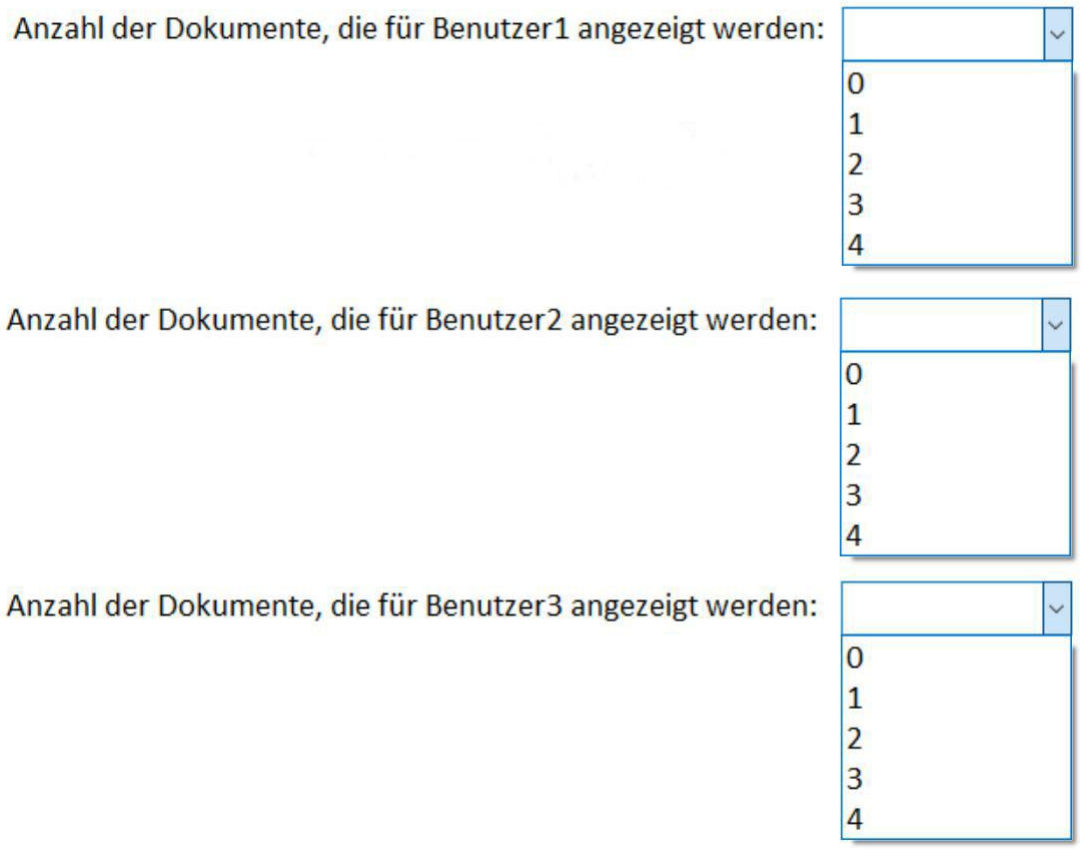
Benutzer2 hat sich noch nie an Computer1 angemeldet.

Wie viele DOCX-Dateien werden bei der nächsten Anmeldung jedes Benutzers auf dem Desktop jedes Benutzers angezeigt?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung

Antwortbereich



A.Anzahl der Dokumente, die für Benutzer1 angezeigt werden: 3
Anzahl der Dokumente, die für Benutzer2 angezeigt werden: 0
Anzahl der Dokumente, die für Benutzer3 angezeigt werden: 1

B.Anzahl der Dokumente, die für Benutzer1 angezeigt werden: 3
Anzahl der Dokumente, die für Benutzer2 angezeigt werden: 1
Anzahl der Dokumente, die für Benutzer3 angezeigt werden: 2
C.Anzahl der Dokumente, die für Benutzer1 angezeigt werden: 2
Anzahl der Dokumente, die für Benutzer2 angezeigt werden: 2
Anzahl der Dokumente, die für Benutzer3 angezeigt werden: 2
D.Anzahl der Dokumente, die für Benutzer1 angezeigt werden: 4
Anzahl der Dokumente, die für Benutzer2 angezeigt werden: 4
Anzahl der Dokumente, die für Benutzer3 angezeigt werden: 4
E.Anzahl der Dokumente, die für Benutzer1 angezeigt werden: 2
Anzahl der Dokumente, die für Benutzer2 angezeigt werden: 2
Anzahl der Dokumente, die für Benutzer3 angezeigt werden: 3
F.Anzahl der Dokumente, die für Benutzer1 angezeigt werden: 3
Anzahl der Dokumente, die für Benutzer2 angezeigt werden: 2
Anzahl der Dokumente, die für Benutzer3 angezeigt werden: 2

Korrekte Antwort: E

Erläuterungen:
Jeder Benutzer bekommt die Dateien innerhalb des Desktop-Verzeichnisses seines Profils und die Dateien innerhalb des Desktop-Verzeichnisses des öffentlichen Profils angezeigt.

Bei der ersten Anmeldung eines Benutzers wird für den Benutzer ein neues Profil durch Kopieren des Profils "Default" erstellt. Benutzer2 und Benutzer3 melden sich an, nachdem Benutzer1 die Datei Datei3.docx erstellt hat und bekommen diese daher angezeigt.