Prüfungsnummer:MD-102

Prüfungsname: Endpoint Administrator

Version:demo

Achtung: Aktuelle englische Version zu MD-102 bei uns ist gratis!!

1.Sie haben ein Microsoft 365-Abonnement.

Sie verwenden die Microsoft Intune Suite, um Geräte zu verwalten.

Sie haben die in der folgenden Abbildung gezeigte App-Schutzrichtlinie für iOS/iPadOS.

Zugriffsanforderungen

PIN für Zugriff	Anfordern
PIN-Typ	Numerisch
Einfache PIN	Erteilen Sie
PIN-Mindestlänge auswählen	6
Touch ID anstelle von PIN für Zugriff (iOS 8 und höher/iPadOS)	Erteilen Sie
PIN setzt Biometrie nach Timeout außer Kraft	Anfordern
Timeout (Minuten der Inaktivität)	30
Face ID anstelle von PIN für Zugriff (iOS 11 und höher/iPadOS)	Blockieren
Anzahl von Tagen für PIN-Zurücksetzung	Nein
Anzahl Tage	0
App-PIN, wenn Geräte-PIN festgelegt ist	Anfordern
Anmeldeinformationen für Geschäfts-, Schul- oder Unikonto für Zugriff	Anfordern
Zugriffsanforderungen nach (Minuten der Inaktivität) erneut überprüfen	30

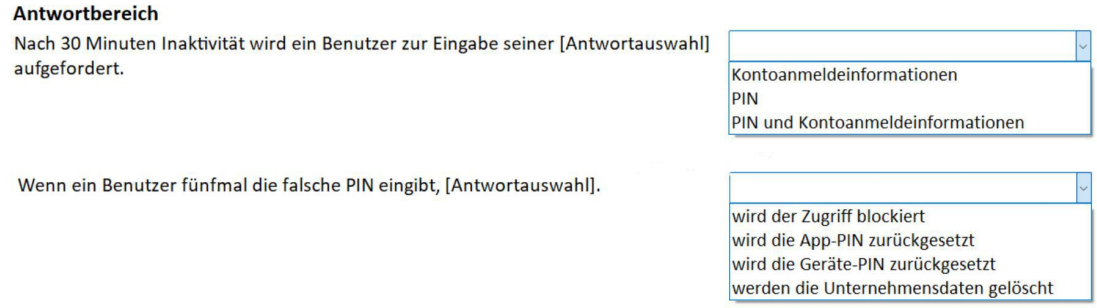
Bedingter Start

Einstellung	Wert	Aktion
Maximal zulässige PIN-Versuche	5	PIN zurücksetzen
Offlinetoleranzperiode	720	Zugriff blockieren (Minuten)
Offlinetoleranzperiode	90	Daten löschen (Tage)
Geräte mit Jailbreak/entfernten Nutzungsbeschränkungen		Zugriff blockieren

Verwenden Sie die Dropdown-Menüs, um die Antwortoption auszuwählen, die jede Aussage basierend auf den in der Grafik dargestellten Informationen beantwortet.

(Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung



A.Nach 30 Minuten Inaktivität wird ein Benutzer zur Eingabe seiner Kontoanmeldeinformationen aufgefordert.
Wenn ein Benutzer fünfmal die falsche PIN eingibt, wird der Zugriff blockiert.
B.Nach 30 Minuten Inaktivität wird ein Benutzer zur Eingabe seiner Kontoanmeldeinformationen aufgefordert.
Wenn ein Benutzer fünfmal die falsche PIN eingibt, wird die App-PIN zurückgesetzt.
C.Nach 30 Minuten Inaktivität wird ein Benutzer zur Eingabe seiner PIN aufgefordert.
Wenn ein Benutzer fünfmal die falsche PIN eingibt, wird die Geräte-PIN zurückgesetzt .
D.Nach 30 Minuten Inaktivität wird ein Benutzer zur Eingabe seiner PIN aufgefordert.
Wenn ein Benutzer fünfmal die falsche PIN eingibt, wird der Zugriff blockiert.
E.Nach 30 Minuten Inaktivität wird ein Benutzer zur Eingabe seiner PIN und Kontoanmeldeinformationen aufgefordert.
Wenn ein Benutzer fünfmal die falsche PIN eingibt, wird die App-PIN zurückgesetzt.
F.Nach 30 Minuten Inaktivität wird ein Benutzer zur Eingabe seiner PIN und Kontoanmeldeinformationen aufgefordert.
Wenn ein Benutzer fünfmal die falsche PIN eingibt, werden die Unternehmensdaten gelöscht.

Korrekte Antwort: E

Erläuterungen:

Wenn die Option Anmeldeinformationen für Geschäfts-, Schul- oder Unikonto für Zugriff auf Anfordern festgelegt ist, müssen Anmeldeinformationen für Geschäfts-, Schul- oder Uni-Konten verwendet werden, um auf die von der Richtlinie verwaltete App zuzugreifen. Wenn außerdem eine PIN oder biometrische Methoden für den Zugriff auf die App erforderlich sind, werden die Anmeldeinformationen für das Geschäfts-, Schul- oder Uni-Konto zusätzlich zu diesen Eingabeaufforderungen benötigt.

Die Option Maximal zulässige PIN-Versuche gibt die Anzahl der Versuche an, die der Benutzer zum erfolgreichen Eingeben seiner PIN hat, ehe die konfigurierte Aktion ausgeführt wird. Wenn der Benutzer es nicht schafft, seine PIN innerhalb der maximalen Anzahl der Versuche für die PIN-Eingabe einzugeben, muss er seine PIN zurücksetzen, nachdem er sich erfolgreich bei seinem Konto angemeldet und ggf. eine mehrstufige Authentifizierung (Multi-Factor Authentication, MFA) durchgeführt hat. Dieses Richtlinieneinstellungsformat unterstützt eine positive ganze Zahl. Zu den Aktionen zählen:

PIN zurücksetzen: Der Benutzer muss die PIN zurücksetzen.
Daten löschen: Das Benutzerkonto, das der Anwendung zugewiesen ist, wird vom Gerät gelöscht.
Die Option ist auf PIN zurücksetzen festgelegt.

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Einstellungen für App-Schutzrichtlinien für iOS

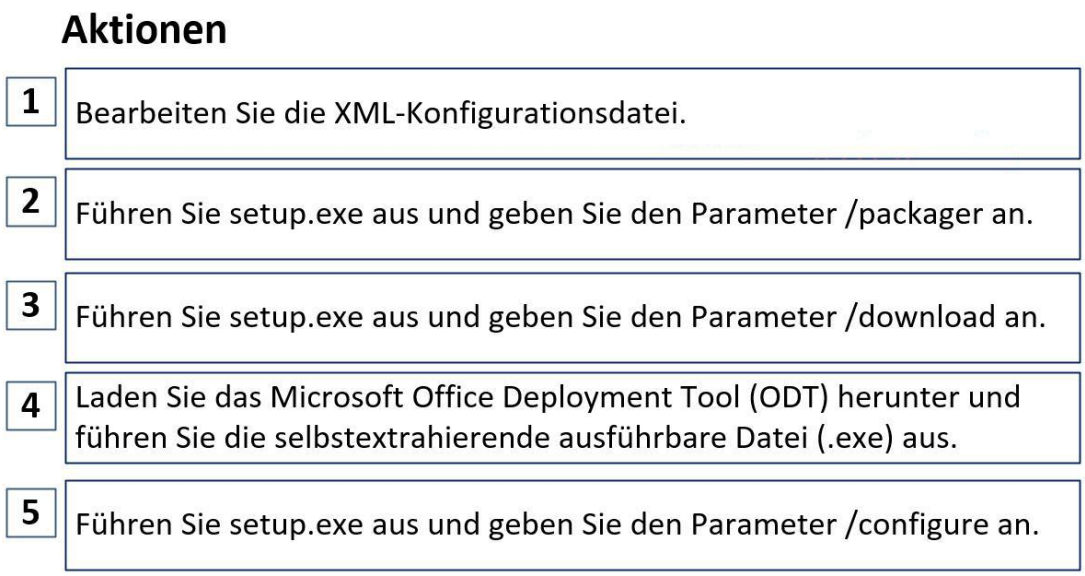
2.Sie haben ein Microsoft 365 E5-Abonnement und einen Computer, auf dem Windows 11 ausgeführt wird.

Sie müssen eine benutzerdefinierte Installation von Microsoft 365-Apps für Unternehmen erstellen.

Welche vier Aktionen sollten Sie nacheinander ausführen?

(Die verfügbaren Aktionen werden in der Abbildung gezeigt. Klicken Sie auf die Schaltfläche Zeichnung und ordnen Sie die erforderlichen Schritte in der richtigen Reihenfolge an.)

Abbildung



A.Reihenfolge: 3, 1, 5, 2
B.Reihenfolge: 4, 1, 3, 5
C.Reihenfolge: 4, 1, 5, 3
D.Reihenfolge: 3, 1, 2, 5

Korrekte Antwort: B

Erläuterungen:

Das Office Deployment Tool (ODT) ist ein Befehlszeilentool, mit dem Sie Microsoft 365 Apps herunterladen und auf Ihren Clientcomputern bereitstellen können. Das Office-Bereitstellungstool bietet Ihnen mehr Kontrolle über eine Office-Installation: Sie können definieren, welche Produkte und Sprachen installiert werden, wie diese Produkte aktualisiert werden sollen und ob den Benutzern der Installationsvorgang angezeigt werden soll.

Führen Sie nach dem Download die selbst entpackende ausführbare Datei aus, die die ausführbare Datei (setup.exe) und eine Beispielkonfigurationsdatei (configuration.xml) für das Office-Bereitstellungstool enthält.

Das ODT besteht aus zwei Dateien: setup.exe und configuration.xml. Um mit dem Tool zu arbeiten, bearbeiten Sie die Konfigurationsdatei, um die gewünschten Optionen zu definieren, und führen dann setup.exe über die Befehlszeile aus. Beispielsweise können Sie die Konfigurationsdatei bearbeiten, um die englische 64-Bit-Version von Office zu installieren, wobei die Lizenzbedingungen automatisch akzeptiert werden.

Beim Ausführen des Office-Bereitstellungstools müssen Sie den Speicherort der Konfigurationsdatei angeben und definieren, in welchem Modus das Office-Bereitstellungstool ausgeführt werden soll:

Verwenden Sie den Downloadmodus, um Microsoft 365 Apps Produkte und Sprachen herunterzuladen. Beispiel: setup.exe /download downloadconfig.xml. Wenn Sie Office in einen Ordner herunterladen, der diese Version von Office bereits enthält, spart das ODT Ihre Netzwerkbandbreite, indem nur die fehlenden Dateien heruntergeladen werden. Wenn Sie z. B. das ODT verwenden, um Office in Englisch und Deutsch in einen Ordner herunterzuladen, der Office bereits in Englisch enthält, wird nur das deutsche Sprachpaket heruntergeladen.

Verwenden Sie den Konfigurationsmodus, um die heruntergeladenen Microsoft 365 Apps Produkte und Sprachen auf einem Clientcomputer zu installieren. Diesen Modus können Sie auch zum Entfernen und Aktualisieren von Office-Produkten und -sprachen verwenden. Beispiel: setup.exe /configure installconfig.xml

Verwenden Sie den Anpassungsmodus, um neue Anwendungseinstellungen auf Clientcomputer anzuwenden, auf denen bereits Microsoft 365 Apps installiert sind. In diesem Modus werden nur Anwendungseinstellungen angewendet, ohne dass andere Bereitstellungseinstellungen geändert werden. Beispiel: setup.exe /customize preferencesconfig.xml

Verwenden Sie den Packager-Modus, um ein App-V-Paket aus den heruntergeladenen Microsoft 365 Apps Produkten und Sprachen zu erstellen. Beispiel: setup.exe /packager packageconfig.xml

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Übersicht über das Office-Bereitstellungstool

3.Sie haben einen Azure Active Directory-Mandanten mit dem Namen it-pruefungen.de, der die in der folgenden Tabelle aufgeführten Geräte enthält.

Name	Betriebssystem
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

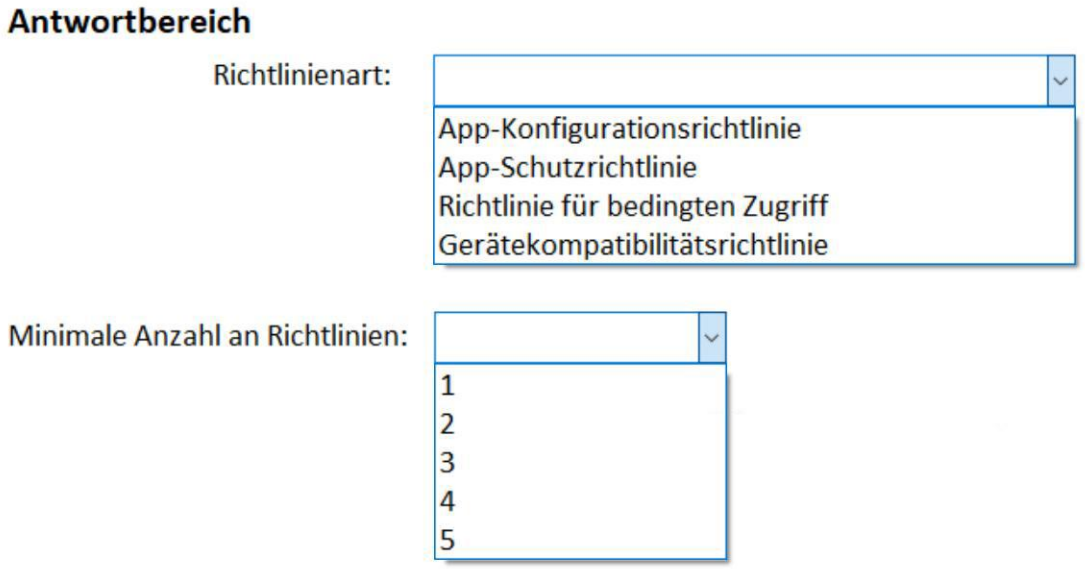
Alle Geräte enthalten eine App mit dem Namen App1 und alle Geräte sind bei Microsoft Intune registriert.

Sie müssen verhindern, dass Benutzer Daten aus App1 kopieren und in andere Apps einfügen.

Welche Art von Richtlinie und wie viele dieser Richtlinien sollten Sie in Intune erstellen?

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

Abbildung



A.Richtlinienart: App-Konfigurationsrichtlinie
Minimale Anzahl an Richtlinien: 5
B.Richtlinienart: App-Konfigurationsrichtlinie
Minimale Anzahl an Richtlinien: 1
C.Richtlinienart: App-Schutzrichtlinie
Minimale Anzahl an Richtlinien: 3
D.Richtlinienart: App-Schutzrichtlinie
Minimale Anzahl an Richtlinien: 5
E.Richtlinienart: Richtlinie für bedingten Zugriff
Minimale Anzahl an Richtlinien: 1
F.Richtlinienart: Gerätekompatibilitätsrichtlinie
Minimale Anzahl an Richtlinien: 3

Korrekte Antwort: C

Erläuterungen:

Wir benötigen drei App-Schutzrichtlinien. Für jede der drei verwendeten Plattformen (Windows 10, Android, iOS/iPadOS) wird eine separate App-Schutzrichtlinie benötigt.

App-Schutzrichtlinien sind Regeln, die sicherstellen, dass die Daten einer Organisation in einer verwalteten App jederzeit sicher sind und dort verbleiben. Eine Richtlinie kann eine Regel sein, die erzwungen wird, wenn ein Benutzer versucht, auf unternehmenseigene Daten zuzugreifen oder diese zu verschieben. Es kann sich auch um eine Reihe von Aktionen handeln, die nicht zulässig sind oder überwacht werden, wenn sich ein Benutzer in der App befindet. Eine verwaltete App ist eine App, auf die App-Schutzrichtlinien angewendet wurden und die von Intune verwaltet werden kann.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Übersicht über App-Schutzrichtlinien

4.Sie haben ein Microsoft 365-Abonnement, das Microsoft Intune Suite verwendet.

Sie verwenden Microsoft Intune, um Geräte zu verwalten.

Sie planen, zwei Apps mit den Namen App1 und App2 auf allen Windows-Geräten bereitzustellen. App1 muss vor App2 installiert werden.

Sie stellen im Intune Admin Center zwei Windows-App (Win32)-Apps bereit. Sie müssen sicherstellen, dass App1 auf jedem Gerät vor App2 installiert wird.

Was sollten Sie konfigurieren?

A.Die Bereitstellungskonfiguration für App1
B.Eine dynamische Gerätegruppe
C.Eine Erkennungsregel
D.Die Bereitstellungskonfiguration für App2

Korrekte Antwort: D

Erläuterungen:

Bereitstellunngskonfigurationen für Win32-Apps unterstützen das Konfigurieren von Anforderungen, die Geräte vor der App-Installation erfüllen müssen. Wir können der Bereitstellungskonfiguration für App2 eine Anforderungsregel vom Typ "Datei" hinzufügen, die erfordert, dass eine Datei oder ein Ordner, die zu App1 gehört, in einem bestimmten Pfad verfügbar ist.

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Hinzufügen, Zuweisen und Überwachen einer Win32-App in Microsoft Intune

5.Sie haben ein Microsoft 365-Abonnement, das 100 bei Microsoft Intune registrierte Geräte enthält.

Sie müssen die Startprozesse überprüfen und ermitteln, wie oft jedes Gerät neu gestartet wird.

Was sollten Sie verwenden?

A.Azure Monitor
B.Intune Data Warehouse
C.Microsoft Defender for Endpoint
D.Endpunktanalyse

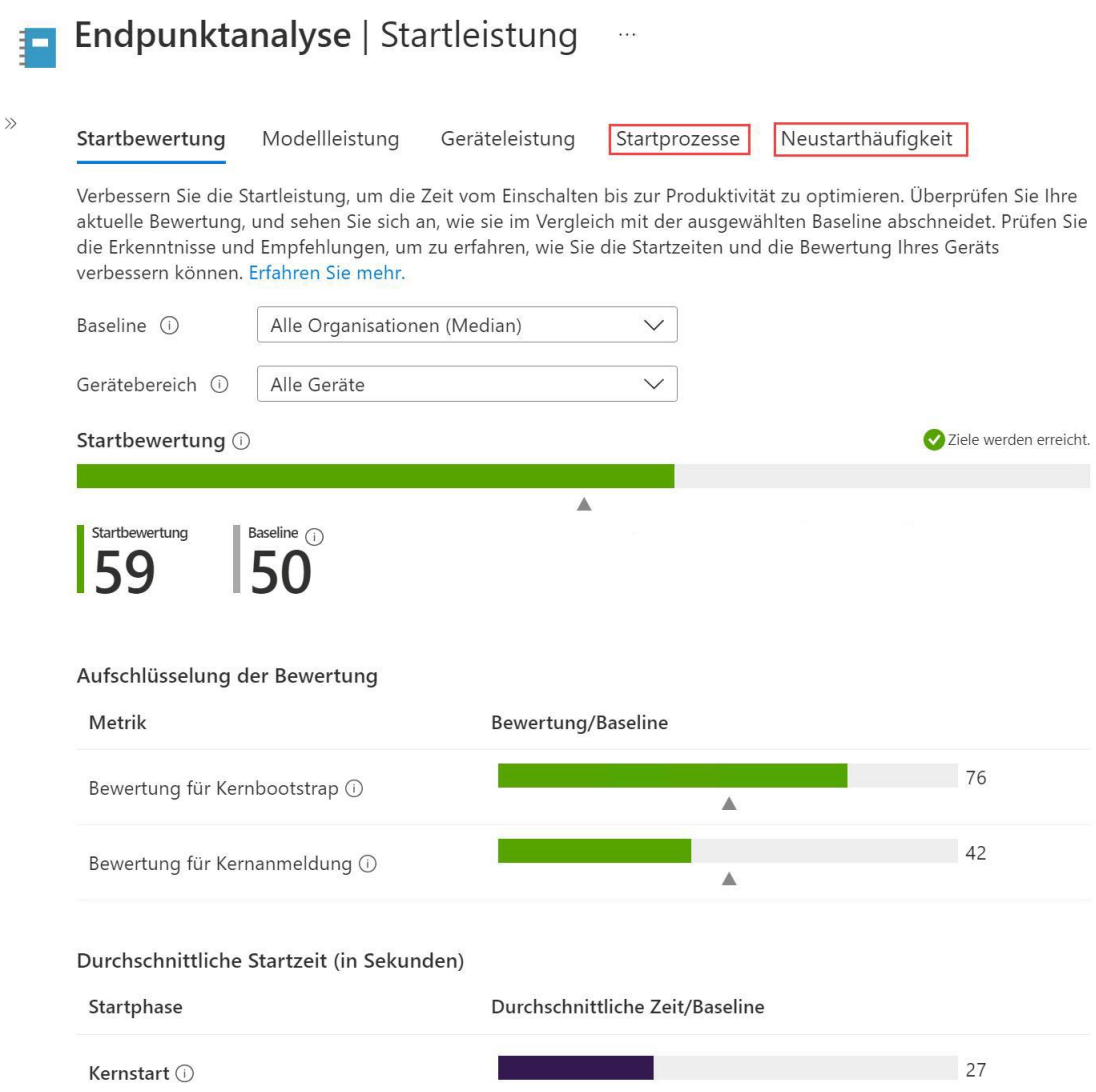
Korrekte Antwort: D

Erläuterungen:

Es ist nicht ungewöhnlich, dass Endbenutzer lange Startzeiten oder andere Unterbrechungen erleben. Diese Unterbrechungen können auf eine Kombination folgender Punkte zurückzuführen sein:

Legacyhardware
Softwarekonfigurationen, die nicht für die Endbenutzererfahrung optimiert sind
Probleme, die durch Konfigurationsänderungen und Updates verursacht werden
Diese Probleme und andere Probleme bei der Endbenutzererfahrung bleiben bestehen, da die IT-Abteilung keinen großen Einblick in die Endbenutzererfahrung hat. Im Allgemeinen erfolgt der einzige Einblick in diese Probleme über einen langsamen, kostspieligen Supportkanal, der in der Regel keine klaren Informationen zu den zu optimierenden Anforderungen liefert. Es ist aber nicht nur der IT-Support, der die Kosten für diese Probleme trägt. Die Zeit, die IT-Mitarbeiter für Probleme aufwenden, ist auch wertvoll. Leistungs-, Zuverlässigkeits- und Supportprobleme, die die Benutzerproduktivität reduzieren, können sich auch stark auf die Bilanz eines Unternehmens auswirken.

Die Endpunktanalyse zielt darauf ab, durch Erkenntnisse über die Benutzerfreundlichkeit die Benutzerproduktivität zu verbessern und die IT-Supportkosten zu senken. Anhand dieser Erkenntnisse können IT-Mitarbeiter die Endbenutzererfahrung mit proaktivem Support optimieren und Regressionen der Benutzerfreundlichkeit erkennen, indem die Auswirkungen auf Benutzer von Konfigurationsänderungen bewertet werden.



Reference: Startleistung

6.Sie haben Computer, auf denen Windows 10 ausgeführt wird. Die Computer sind mit einem Azure Log Analytics-Arbeitsbereich verbunden. Der Arbeitsbereich ist so konfiguriert, dass alle verfügbaren Ereignisse aus Windows-Ereignisprotokollen erfasst werden.

Die Computer haben die in der folgenden Tabelle aufgeführten Ereignisse protokolliert:

Ereignis-ID	Protokoll	Typ	Computer
1	Anwendung	Erfolgreich	Computer1
2	System	Information	Computer1
3	Sicherheit	Überwachung erfolgreich	Computer2
4	System	Fehler	Computer2

Welche Ereignisse sind im Log Analytics-Arbeitsbereich erfasst?

A.Nur Ereignis-ID 1
B.Nur Ereignis-ID 2 und 3
C.Nur Ereignis-ID 1 und 3
D.Nur Ereignis-ID 1, 2 und 4
E.Ereignis-ID 1, 2, 3 und 4

Korrekte Antwort: D

Erläuterungen:

In der folgenden Tabelle sind die Datentypen aufgeführt, die Sie für die Erfassung in einem Log Analytics-Arbeitsbereich von allen verbundenen Agents konfigurieren können:

Data source	BESCHREIBUNG
Windows-Ereignisprotokolle	An das Windows-System für die Ereignisprotokollierung gesendete Informationen
Syslog	Informationen, die an das Linux-System für die Ereignisprotokollierung gesendet werden
Leistung	Numerische Werte zum Messen der Leistung verschiedener Betriebssystem- und Workloadaspekte
IIS-Protokolle	Nutzungsinformationen für IIS-Websites, die unter dem Gastbetriebssystem ausgeführt werden
Benutzerdefinierte Protokolle	Ereignisse aus Textdateien auf Windows- und Linux-Computern

Windows-Ereignisprotokolle sind eine der gängigsten Datenquellen für Log Analytics-Agents auf virtuellen Windows-Computern, weil viele Anwendungen Daten in das Windows-Ereignisprotokoll schreiben. Sie können Ereignisse aus Standardprotokollen, wie z. B. „System“ und „Anwendung“, und aus benutzerdefinierten Protokollen sammeln, die von zu überwachenden Anwendungen erstellt wurden.

Wichtig: Sie können mit dem Log Analytics-Agent keine Sammlung von Ereignissen aus dem Protokoll Sicherheit konfigurieren. Sie müssen Microsoft Defender für Cloud oder Microsoft Sentinel verwenden, um Sicherheitsereignisse zu sammeln.

Die folgenden Microsoft Learn-Artikel enthalten weitere Informationen zum Thema:

Übersicht über den Log Analytics-Agent

Datenquellen für das Sammeln von Windows-Ereignisprotokolldaten mit dem Log Analytics-Agent

7.Sie haben ein Microsoft 365 E5-Abonnement, das 10 Android Enterprise-Geräte enthält. Jedes Gerät verfügt über ein unternehmenseigenes Arbeitsprofil und ist bei Microsoft Intune registriert.

Sie müssen die Geräte so konfigurieren, dass sie eine einzelne App im Kioskmodus ausführen.

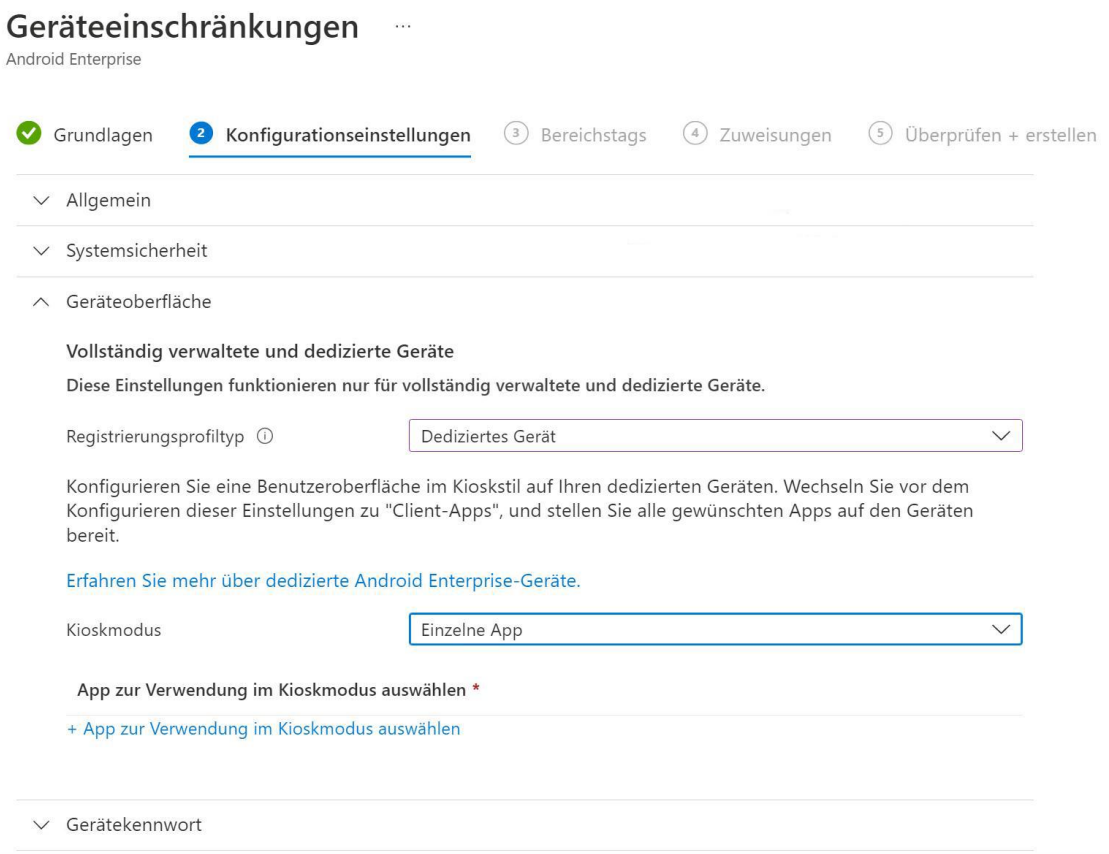
Welche Konfigurationseinstellungen sollten Sie im Geräteeinschränkungsprofil ändern?

A.Allgemein
B.Benutzer und Konten
C.Systemsicherheit
D.Geräteoberfläche

Korrekte Antwort: D

Erläuterungen:

Wir sollten die Einstellungen im Abschnitt "Geräteoberfläche" konfigurieren:



Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Android Enterprise-Geräteeinstellungen zum Zulassen oder Einschränken von Features mithilfe von Intune

8.Sie haben eine Azure Active Directory-Gruppe mit dem Namen Gruppe1. Gruppe1 enthält zwei Windows 10 Enterprise-Geräte mit den Namen Device1 und Device2.

Sie erstellen ein Gerätekonfigurationsprofil mit dem Namen Profil1. Sie weisen Profil1 Gruppe1 zu.

Sie müssen sicherstellen, dass Profil1 nur auf Device1 angewendet wird.

Was ändern Sie in Profil1?

A.Die Zuweisung
B.Die Einstellungen
C.Den Bereich (Markierungen)
D.Die Anwendbarkeitsregeln

Korrekte Antwort: A

Erläuterungen:

Um sicherzustellen, dass Profil1 nur auf Device1 angewendet wird, müssen wir die Zuordnung ändern. Wir können die Zuweisung entweder so ändern, dass sie nur Gerät1 einschließt, oder wir können einen Ausschluss für Gerät2 konfigurieren.

Profilzuweisungen basieren auf Gruppen. Bevor wir nur Device1 einschließen oder Device2 ausschließen können, müssen wir eine neue Gruppe erstellen, die das jeweilige Gerät enthält.

Hinweis:

Für Windows 10-Geräte können Sie Anwendbarkeitsregeln hinzufügen, um das Profil nur auf eine bestimmte Betriebssystemversion oder eine bestimmte Windows-Edition anzuwenden. Da auf beiden Geräten Windows 10 Enterprise ausgeführt wird, sind die Anwendbarkeitsregeln in diesem Fall nicht zur Lösung geeignet.

Bereichstags sind eine Möglichkeit, um zu filtern, welche Objekte Administratoren im Portal sehen können. Sie können die rollenbasierte Zugriffssteuerung und Bereichstags verwenden, um sicherzustellen, dass die richtigen Administratoren den richtigen Zugriff und die richtige Sichtbarkeit für die Intune-Objekte haben. Rollen legen fest, welche

Administratoren Zugriff auf welche Objekte haben. Bereichstags bestimmen, welche Objekte Administratoren sehen können. Bereichstags eignen sich nicht zum Einschränken des Anwendungsbereichs von Profilen.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Zuweisen von Benutzer- und Geräteprofilen in Microsoft Intune