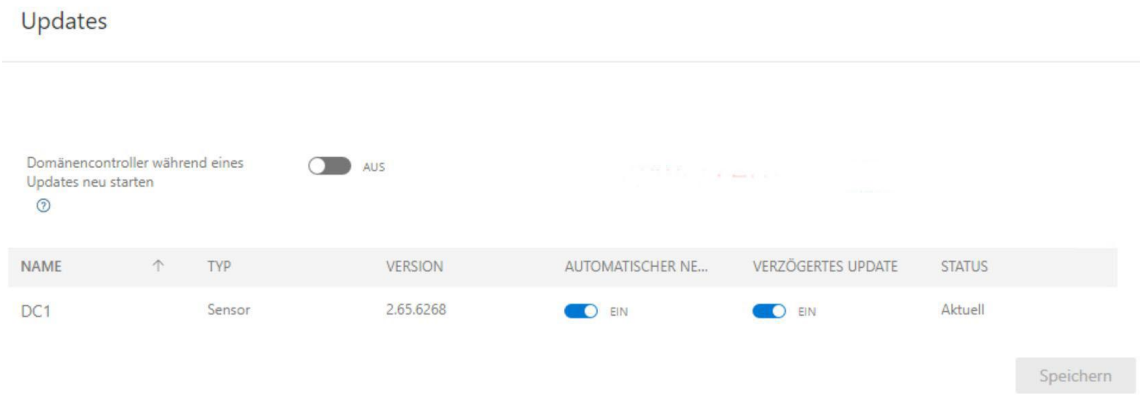
**Prüfungsnummer:**MS-101

**Prüfungsname:**Microsoft 365 Mobility and Security

**Version:**demo

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

1.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Sie implementieren Microsoft Azure Advanced Threat Protection (Azure ATP).
Sie haben einen Azure ATP-Sensor konfiguriert. Ihre Konfiguration wird nachstehend gezeigt.




Wie lange dauert es, nachdem der Azure ATP-Clouddienst aktualisiert wurde, bis der Sensor aktualisiert wird?

A.1 Stunde
B.12 Stunden
C.48 Stunden
D.7 Tage
E.4 Stunden

Korrekte Antwort: C

Erläuterungen:
Der Azure ATP-Dienst wird in der Regel mehrmals pro Monat mit neuen Erkennungen, Features und Leistungsverbesserungen aktualisiert. In der Regel enthalten diese Updates auch ein entsprechendes Nebenversionsupdate für die Sensoren. Azure ATP-Sensoren und die entsprechenden Updates haben niemals Schreibberechtigungen für Ihre Domänencontroller. Sensorupdatepakete steuern nur die Azure ATP-Sensoren und die Erkennungsfunktionen der Sensoren.

Updatetypen für den Azure ATP-Sensor
Azure ATP-Sensoren unterstützen zwei verschiedene Arten von Updates:

Updates von Nebenversionen:

Häufig
Keine Installation von MSI und keine Änderungen der Registrierung erforderlich
Neu gestartet: Azure ATP-Sensordienste
Nicht neu gestartet: Domänencontroller-Dienste und Server-Betriebssystem
Updates der Hauptversion:

Selten
Umfassen wichtige Änderungen
Neu gestartet: Azure ATP-Sensordienste
Möglicherweise Neustart erforderlich: Domänencontroller-Dienste und Server-Betriebssystem
Wenn Sie mehr als ein Versionsupdate nicht installieren und Ihre Sensoren nicht aktualisieren, können diese nicht mehr mit dem Azure ATP-Clouddienst kommunizieren. Dadurch ist der Azure ATP-Dienst möglicherweise nicht mehr verfügbar und bietet keinen Schutz für Ihr Unternehmen.

Verzögertes Sensorupdate
Angesichts der rasanten Azure ATP-Entwicklung und der raschen Freigabe von Updates können Sie eine Untergruppe Ihrer Sensoren als verzögerten Updatering definieren, was einen graduellen Updateprozess für Ihre Sensoren ermöglicht. Mit Azure ATP können Sie auswählen, wie Ihre Sensoren aktualisiert werden, und jeden Sensor als Kandidat für ein verzögertes Update festlegen.

Sensoren, die nicht für ein verzögertes Update ausgewählt wurden, werden bei jedem Update des Azure ATP-Diensts automatisch aktualisiert. Sensoren, für die ein verzögertes Update festgelegt wurde, werden mit einer Verzögerung von 72 Stunden nach der offiziellen Freigabe der einzelnen Dienstupdates aktualisiert.

Mit der Option für ein verzögertes Update können Sie bestimmte Sensoren als automatischen Updatering auswählen, bei dem alle Updates automatisch erfolgen, und für den Rest der Sensoren ein verzögertes Update festlegen. Das gibt Ihnen Zeit, zuerst die erfolgreiche Ausführung der automatischen Aktualisierung Ihrer Sensoren zu bestätigen.

Updateprozess für den Sensor
Die Azure ATP-Sensoren prüfen im Abstand weniger Minuten, ob sie bereits auf die neuste Version aktualisiert worden sind. Wenn der Azure ATP-Clouddienst auf eine neuere Version aktualisiert wird, startet der Azure ATP-Sensordienst den Aktualisierungsprozess:

Der Azure ATP-Clouddienst führt ein Update auf die neueste Version durch.

Der Azure ATP-Sensor-Aktualisierungsdienst stellt fest, dass eine aktualisierte Version verfügbar ist.

Bei den Sensoren, für die kein verzögertes Update festgelegt, beginnt der sensorweise Updateprozess:

Der Azure ATP-Sensor-Aktualisierungsdienst bezieht vom Clouddienst die aktualisierte Version (im CAB-Dateiformat).
Der Azure ATP-Sensor-Aktualisierungsdienst überprüft die Dateisignatur.
Der Azure ATP-Sensor-Aktualisierungsdienst extrahiert die CAB-Datei in einen neuen Unterordner im Installationsverzeichnis des Sensors.Standardmäßig wird sie in folgenden Ordner extrahiert: C:\Programme\Azure Advanced Threat Protection Sensor<Versionsnummer>
Der Azure ATP-Sensordienst verweist auf die neuen Dateien, die aus der CAB-Datei extrahiert wurden.
Der Azure ATP-Sensor-Aktualisierungsdienst startet den Azure ATP-Sensordienst neu.
Die Sensoren werden auf Basis der neuen aktualisierten Version ausgeführt.
Der Sensor erhält eine Freigabe vom Azure-Clouddienst. Den Sensorstatus können Sie auf der Seite Updates überprüfen.
Der nächste Sensor startet den Aktualisierungsprozess.
72 Stunden nach der Aktualisierung des Azure ATP-Clouddiensts startet der Updateprozess für die Sensoren, für die ein verzögertes Update ausgewählt wurde.
Dieser Updateprozess entspricht dabei dem Vorgang für automatisch aktualisierte Sensoren.

48 Stunden ist die Antwort, die am nähesten an der richtigen Antwort (72 Stunden) dran liegt.
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Aktualisieren von Azure ATP-Sensoren

2.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat ein Microsoft 365 E5-Abonnement.
Benutzer der Forschungsabteilung arbeiten mit sensiblen Daten.
Sie müssen verhindern, dass Benutzer der Forschungsabteilung auf potenziell unsichere Websites zugreifen, indem Sie Hyperlinks verwenden, die in E-Mail-Nachrichten und Dokumenten eingebettet sind. Benutzer in anderen Abteilungen dürfen nicht eingeschränkt werden.
Welchen Schritt führen Sie im Security & Compliance Admin Center aus?

A.Erstellen Sie eine DLP-Richtlinie (Data Loss Prevention), die eine Bedingung vom Typ „Content is shared“ verwendet.
B.Ändern Sie die Standardrichtlinie für sichere Links.

C.Erstellen Sie eine DLP-Richtlinie (Data Loss Prevention), die eine Bedingung vom Typ „Content contains“ verwendet.
D.Erstellen Sie eine neue Richtlinie für sichere Links.

Korrekte Antwort: D

Erläuterungen:
Eine Microsoft 365 E5-Lizenz enthält Office 365 Advanced Thread Protection (ATP).

Da die Standardrichtlinie für sichere Links für die gesamte Organisation gilt, muss eine neue Richtlinie für sichere Links erstellt werden, die nur für Benutzer der Forschungsabteilung gilt.

Office 365 ATP-Safe Links (Sichere Links)
Mit Office 365 ATP-Sichere Links können Sie Ihr Unternehmen schützen, indem Sie die Überprüfung von Webadressen (URLs) in E-Mail-Nachrichten und Office-Dokumenten zur Zeit des Aufrufs (Klickzeit) aktivieren. Der Schutz wird durch ATP Safe Links-Richtlinien definiert, die von Ihrem Office 365-Sicherheitsteam festgelegt werden.

Sobald Ihre ATP Safe Links-Richtlinien implementiert sind, können globale Administratoren, Sicherheitsadministratoren und Sicherheitsleser von Office 365 Berichte für Advanced Threat Protection anzeigen. Die Informationen in diesen Berichten können Ihrem Sicherheitsteam helfen, weitere Schritte zum Schutz Ihrer Organisation oder zur Untersuchung von Sicherheitsvorfällen zu unternehmen.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
ATP-sichere Links in Office 365

3.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Sie haben einen Microsoft 365-Mandanten.
Sie haben eine Geschäftsanwendung mit dem Namen App1. Die Benutzer nutzen das My Apps-Portal, um auf App1 zuzugreifen.
Nach einigen Sicherheitsvorfällen verwenden Sie das Cloud App Security-Portal und erstellen für App1 eine Richtlinie für den bedingten Zugriff.
Sie müssen per E-Mail benachrichtigt werden, wenn für einen Benutzer von App1 eine Annomalieerkennung vom Typ „unmöglicher Ortswechsel“ (Impossible Travel) festgestellt wird. Ihre Lösung muss sicherstellen, dass Alarme nur für App1 generiert werden.
Wie gehen Sie vor?

A.Erstellen Sie im Microsoft Cloud App Security-Portal eine Richtlinie zur Erkennung von Cloud Discovery-Anomalien.
B.Ändern Sie im Microsoft Cloud App Security-Portal die Richtlinie für unmögliche Ortswechsel (Impossible Travel).

C.Erstellen Sie im Microsoft Cloud App Security-Portal eine App-Ermittliungs-Richtlinie.
D.Ändern Sie im Azure Active Directory-Admin Center die Richtlinie für den bedingten Zugriff.

Korrekte Antwort: D

Erläuterungen:
Eine Richtlinie vom Typ unmöglicher Ortswechsel profiliert Ihre Umgebung und löst Warnungen aus, wenn Aktivitäten desselben Benutzers an verschiedenen Standorten innerhalb eines Zeitraums erkannt werden, der kürzer ist als die erwartete Reisezeit zwischen den beiden Standorten. Dies kann darauf hinweisen, dass ein anderer Benutzer dieselben Anmeldeinformationen verwendet. Das Erkennen dieses anomalen Verhaltens erfordert eine anfängliche Lernphase von 7 Tagen, in der das Aktivitätsmuster eines neuen Benutzers gelernt wird.

Führen Sie die folgenden Schritte aus, um Azure AD-Apps so zu konfigurieren, dass sie über Microsoft Cloud App Security Conditional Access App Control gesteuert werden.

Schritt 1: Wechseln Sie zum Azure AD-Portal, und erstellen Sie für die Apps eine Richtlinie für den bedingten Zugriff. Leiten Sie die Sitzung dann an Cloud App Security weiter.

Schritt 2: Melden Sie sich als Benutzer im Geltungsbereich der Richtlinie an den Apps an.

Schritt 3: Wenn Sie keine integrierte Cloud App Security-Richtlinie in Azure AD ausgewählt haben, oder wenn Sie die Richtlinie auf eine nicht unterstützte App anwenden möchten, rufen Sie das Cloud App Security-Portal auf.

Schritt 4: Testen Sie die Bereitstellung.
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Bereitstellen von Conditional Access App Control für Azure AD-Apps

4.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen verwendet Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP enthält die in der folgenden Tabelle aufgeführten Gerätegruppen.

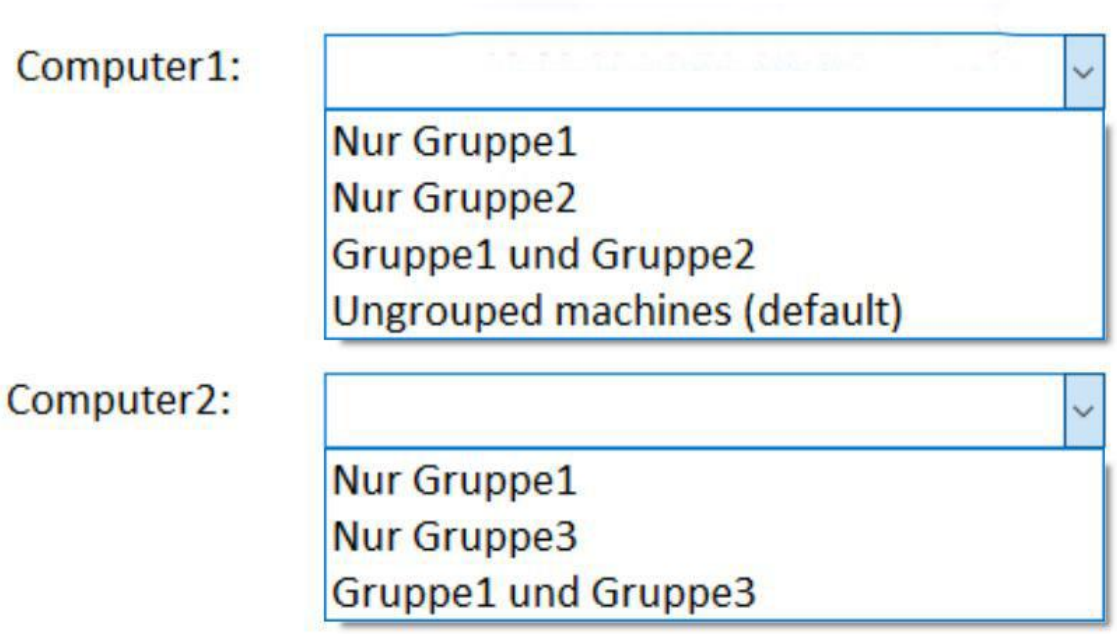
| Rank | Machine Group | Members |
|---|---|---|
| 1 | Gruppe1 | Name Starts with COMP |
| 2 | Gruppe2 | Name Starts with COMP And OS In Windows 10 |
| 3 | Gruppe3 | OS In Windows Server 2016 |
| Last | Ungrouped machines (default) | Nicht zutreffend |

Sie integrieren die folgenden Computer in Windows Defender ATP:

| Name | Betriebssystem |
|---|---|
| Computer1 | Windows 10 |
| Computer2 | Windows Server 2016 |

Welcher Gruppe bzw. welchen Gruppen gehören Computer1 und Computer2 an?
(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

**Antwortbereich**




A.Computer1: Nur Gruppe1
Computer2: Nur Gruppe1
B.Computer1: Nur Gruppe2
Computer2: Gruppe1 und Gruppe3
C.Computer1: Nur Gruppe2
Computer2: Nur Gruppe3
D.Computer1: Gruppe1 und Gruppe2
Computer2: Gruppe1 und Gruppe3
E.Computer1: Gruppe1 und Gruppe2
Computer2: Nur Gruppe1
F.Computer1: Ungrouped machines (default)
Computer2: Nur Gruppe3

Korrekte Antwort: A

Erläuterungen:
Computer1 erfüllt die Mitgliedschaftsregeln für Gruppe1 und Gruppe2.
Computer2 erfüllt nur die Mitgliedschaftsregeln für Gruppe1.
Wenn eine Maschine mit mehr als einer Gruppe übereinstimmt, wird sie nur der Gruppe mit dem höchsten Rang hinzugefügt.
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Erstellen und Verwalten von Computergruppen in Windows Defender ATP

5.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat einen Microsoft 365-Mandanten.
Sie möchten Benutzern aus der Konstruktionsabteilung ermöglichen, ihr mobiles Gerät in Mobile Device Management (MDM) zu registrieren.
Die Gerätetypbeschränkungen sind wie in der folgenden Tabelle gezeigt konfiguriert.

| Priorität | Name | Allowed platform | Zugewiesen für |
|---|---|---|---|
| 1 | iOS | iOS | Marketing |
| 2 | Android | Android | Engineering |
| Standard | Alle Benutzer | Alle Plattformen | Alle Benutzer |

Die Konfiguration der Einschränkungen zum Gerätelimit wird in der folgenden Tabelle gezeigt.

| Priorität | Name | Gerätelimit | Zugewiesen für |
|---|---|---|---|
| 1 | Engineering | 15 | Engineering |
| 2 | Production | 5 | Engineering |
| Standard | Alle Benutzer | 10 | Alle Benutzer |

Wie ist die effektive Konfiguration für die Mitglieder der Gruppe Engineering?
(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)
Abbildung

## Antwortbereich


A.Gerätelimit: 5
Zulässige Plattformen: Nur iOS
B.Gerätelimit: 5
Zulässige Plattformen: Alle Plattformen
C.Gerätelimit: 10
Zulässige Plattformen: Nur iOS
D.Gerätelimit: 10
Zulässige Plattformen: Nur Android
E.Gerätelimit: 15
Zulässige Plattformen: Alle Plattformen
F.Gerätelimit: 15
Zulässige Plattformen: Nur Android

Korrekte Antwort: F

Erläuterungen:
Als Intune-Administrator können Sie Registrierungsbeschränkungen erstellen und verwalten, die die Anzahl und Typen von Geräten festlegen, die sich für die Verwaltung mit Intune registrieren können. Sie können mehrere Beschränkungen definieren und diese verschiedenen Benutzergruppen zuordnen. Für Ihre verschiedenen Beschränkungen können Sie eine Prioritätsreihenfolge festlegen.
Sie können u.a. die folgenden spezifischen Registrierungsbeschränkungen festlegen:

Maximale Anzahl registrierter Geräte
Geräteplattformen, die registriert werden können:

Android
Android-Arbeitsprofil
iOS
macOS
Windows
Plattformbetriebssystemversion für iOS, Android, Android-Arbeitsprofil und Windows. (Es können nur Windows 10-Versionen verwendet werden. Dieses Feld bleibt leer, wenn Windows 8.1 zulässig ist.)
Mindestens erforderliche Version
Maximal zulässige Version
Private Geräte einschränken (nur iOS, Android, Android-Arbeitsprofil, macOS und Windows)
Ein Gerät muss die Registrierungsbeschränkungen mit der höchsten Priorität erfüllen, die dem Benutzer zugeordnet wurden. Sie können eine Gerätebeschränkung verschieben, um ihre Priorität zu ändern. Standardbeschränkungen weisen für alle Benutzer die niedrigste Priorität auf und dienen zur Steuerung benutzerloser Registrierungen. Standardbeschränkungen können bearbeitet, aber nicht gelöscht werden.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Festlegen von Registrierungseinschränkungen