Prüfungsnummer:MS-500

Prüfungsname: Microsoft 365 Security Administration

Version:demo

Achtung: Aktuelle englische Version zu MS-500 bei uns ist gratis!!

1. Sie haben eine hybride Microsoft 365-Umgebung. Alle Computer haben Windows 10 installiert und werden durch Microsoft Intune verwaltet.

Sie müssen eine bedingte Zugriffsrichtlinie für Microsoft Azure Active Directory (Azure AD) erstellen, mit der nur Windows 10-Computer, die als kompatibel gekennzeichnet sind, eine VPN-Verbindung zum On-Premises Netzwerk herstellen können.

Welchen Schritt führen Sie als erstes durch?

A.Erstellen Sie im Azure Active Directory Admin Center ein neues Zertifikat.
B.Aktivieren Sie den Anwendungsproxy in Azure AD.
C.Erstellen Sie im Active Directory-Verwaltungscenter eine Richtlinie für die dynamische Zugriffssteuerung.
D.Konfigurieren Sie die Authentifizierungsmethoden im Azure Active Directory Admin Center.

Korrekte Antwort: A

Erläuterungen:
Mit Azure AD bedingter Zugriff für VPN-Konnektivität können Sie die VPN-Verbindungen schützen. Beim bedingten Zugriff handelt es sich um ein richtlinienbasiertes Auswertungsmodul, mit dem Sie Zugriffsregeln für alle mit Azure Active Directory (Azure AD) verknüpften Anwendungen erstellen können.

Zum Konfigurieren von Azure Active Directory bedingter Zugriff für VPN-Konnektivität muss Folgendes konfiguriert sein:

Server Infrastruktur
RAS-Server für Always on-VPN
Netzwerkrichtlinienserver (NPS)
DNS-und Firewalleinstellungen
Windows 10-Client Always On VPN-Verbindungen

Zum Konfigurieren des bedingten Zugriffs für VPN-Konnektivität müssen Sie folgende Schritte ausführen:

Erstellen Sie ein VPN-Zertifikat in der Azure-Portal.
Laden Sie das VPN-Zertifikat herunter.

Stellen Sie das Zertifikat auf Ihrem VPN-Server bereit.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Bedingter Zugriff für VPN-Konnektivität mithilfe von Azure AD

2. Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat ein Microsoft 365-Abonnement.

Sie erstellen im Microsoft 365 Admin Center einen neuen Benutzer. Sie möchten dem Benutzer die Rolle Berichtleseberechtigter zuweisen.

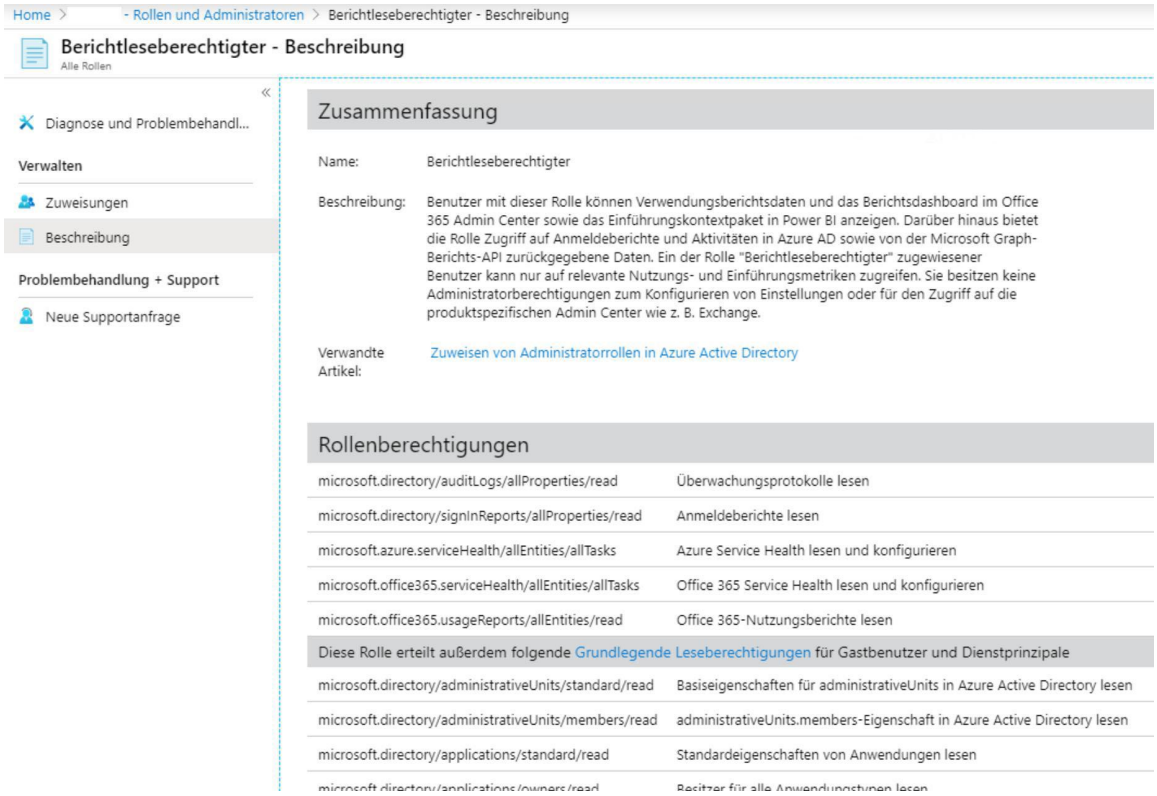
Sie wollen zuvor die Berechtigungen der Rolle Berichtleseberechtigter einsehen.

Welches Admin Center verwenden Sie?

A.Azure Active Directory
B.Cloud App Security
C.Security & Compliance
D.Microsoft 365

Korrekte Antwort: A

Erläuterungen:
Die Berechtigungen einer Rolle können über das "Rollen und Administratoren"-Blade im Azure Active Directory Admin Center eingesehen werden.



3. Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat einen Microsoft 365-Mandanten.

Sie haben 500 Computer, auf denen Windows 10 ausgeführt wird.

Sie planen, die Computer mithilfe von Windows Defender Advanced Threat Protection (Windows Defender ATP) zu überwachen, nachdem die Computer bei Microsoft Intune registriert wurden.

Sie müssen sicherstellen, dass die Computer eine Verbindung zu Windows Defender ATP herstellen.

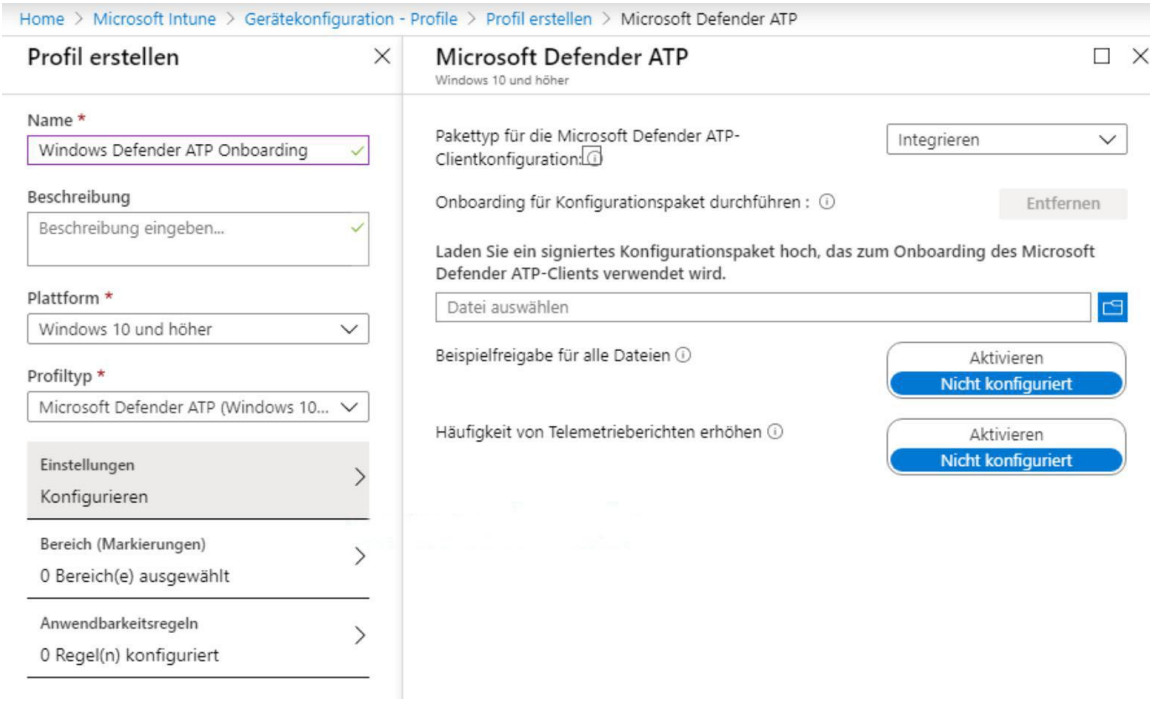
Wie sollten Sie Intune für Windows Defender ATP vorbereiten?

A.Konfigurieren Sie eine Registrierungsbeschränkung.
B.Erstellen Sie ein Gerätekonfigurationsprofil.
C.Erstellen Sie eine Richtlinie für bedingten Zugriff.
D.Erstellen Sie ein Windows Autopilot-Bereitstellungsprofil.

Korrekte Antwort: B

Erläuterungen:
Statt das Onboarding-Skript aus dem Windows Defender ATP Admin Center

herunterzuladen und auf jedem Computer einzeln auszuführen, kann das Script auch per Intune Konfigurationsprofil auf die Clientcomputer angewandt werden.



Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Onboarding von Geräten mithilfe eines Konfigurationsprofils durchführen

4. Ihr Netzwerk enthält eine On-Premises Active Directory-Domäne mit dem Namen it-pruefungen.de. Die Domäne enthält die in der folgenden Tabelle aufgeführten Gruppen:

Name	Typ	E-Mail-Adresse
Gruppe1	Sicherheitsgruppe - Domänenlokal	Gruppe1@it-pruefungen.de
Gruppe2	Sicherheitgruppe - Universal	Keine
Gruppe3	Verteilergruppe - Global	Keine
Gruppe4	Verteilergruppe - Universal	Gruppe4@it-pruefungen.de

Die Domäne wird mit einem Microsoft Azure Active Directory (Azure AD)-Mandanten synchronisiert, der die in der folgenden Tabelle aufgeführten Gruppen enthält:

Name	Typ	Mitgliedschaftstyp
Gruppe11	Sicherheitsgruppe	Zugewiesen
Gruppe12	Sicherheitsgruppe	Dynamisch
Gruppe13	Office 365 Gruppe	Zugewiesen
Gruppe14	Mail-aktivierte Sicherheitsgruppe	Zugewiesen

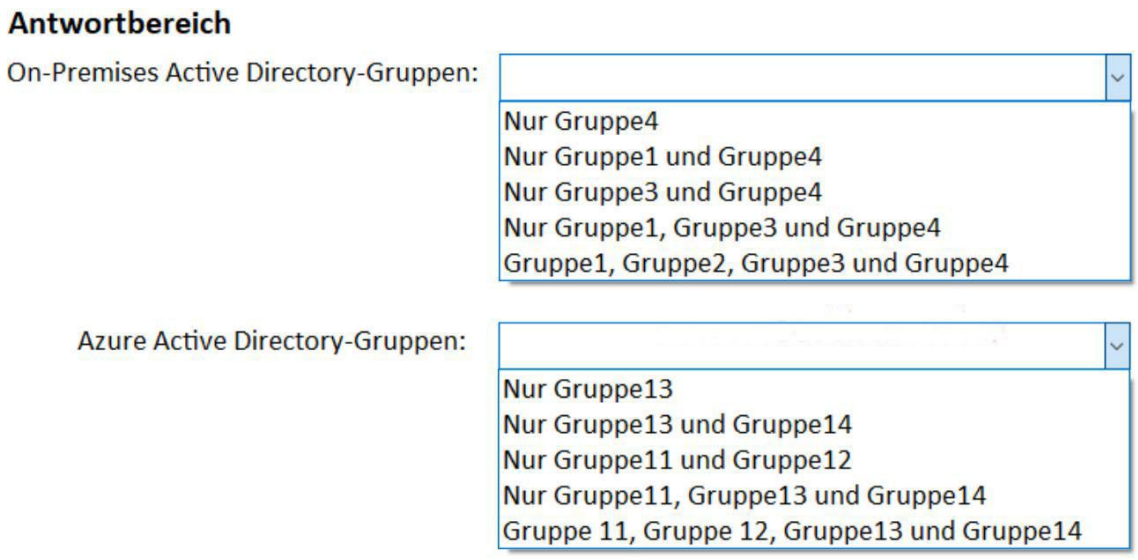
Sie erstellen eine Azure Information Protection-Richtlinie mit dem Namen Richtlinie1.

Sie müssen Richtlinie1 anwenden.

Auf welche Gruppen können Sie Richtlinie1 anwenden?

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

Abbildung



A.On-Premises Active Directory-Gruppen: Nur Gruppe4
Azure Active Directory-Gruppen: Nur Gruppe13
B.On-Premises Active Directory-Gruppen: Nur Gruppe4
Azure Active Directory-Gruppen: Nur Gruppe11, Gruppe13 und Gruppe14
C.On-Premises Active Directory-Gruppen: Nur Gruppe1 und Gruppe4
Azure Active Directory-Gruppen: Nur Gruppe13 und Gruppe14
D.On-Premises Active Directory-Gruppen: Nur Gruppe3 und Gruppe4
Azure Active Directory-Gruppen: Gruppe 11, Gruppe 12, Gruppe13 und Gruppe14
E.On-Premises Active Directory-Gruppen: Nur Gruppe1, Gruppe3 und Gruppe4
Azure Active Directory-Gruppen: Nur Gruppe11 und Gruppe12
F.On-Premises Active Directory-Gruppen: Gruppe1, Gruppe2, Gruppe3 und Gruppe4
Azure Active Directory-Gruppen: Nur Gruppe11, Gruppe13 und Gruppe14

Korrekte Antwort: C

Erläuterungen:

Bevor Sie Azure Information Protection für Ihre Organisation bereitstellen, vergewissern Sie sich, dass Sie in Azure AD über Benutzer und Gruppenkonten für die Mandanten Ihrer Organisation verfügen.

Es gibt verschiedene Verfahren zum Erstellen dieser Konten für Benutzer und Gruppen, z.B.:

Sie können die Benutzer im Microsoft 365 Admin Center und die Gruppen in Exchange Online Admin Center erstellen.

Sie können die Benutzer und Gruppen im Azure-Portal erstellen.

Sie können die Benutzer und Gruppen mithilfe von Azure AD PowerShell und Exchange Online-Cmdlets erstellen.

Sie können die Benutzer und Gruppen in Ihrem lokalen Active Directory erstellen und mit Azure AD synchronisieren.

Sie können die Benutzer und Gruppen einem anderen Verzeichnis erstellen und mit Azure AD synchronisieren.

Wenn Sie Benutzer und Gruppen mit den ersten drei Methoden aus dieser Liste erstellen, werden sie mit einer Ausnahme automatisch in Azure AD erstellt und können von Azure Information Protection direkt verwendet werden. Allerdings werden Benutzer und Gruppen in vielen Unternehmensnetzwerke in einem lokalen Verzeichnis erstellt und verwaltet. Diese Konten können von Azure Information Protection nicht direkt verwendet werden, sondern müssen erst mit Azure AD synchronisiert werden.

Die im vorherigen Abschnitt erwähnte Ausnahme sind dynamische Verteilerlisten, die für Exchange Online erstellt werden können. Anders als statische Verteilerlisten werden diese Gruppen nicht nach Azure AD repliziert und können daher von Azure Information Protection nicht verwendet werden.
Azure Information Protection-Anforderungen für Gruppenkonten

Für die Zuweisung von Bezeichnungen:

Um bereichsbezogene Richtlinien zu konfigurieren, die Gruppenmitgliedern zusätzliche Bezeichnungen zuweisen, können Sie alle Arten von Gruppen in Azure AD verwenden, die über eine E-Mail-Adresse einer überprüften Domäne für den Mandanten

des Benutzers verfügen. Eine Gruppe mit einer E-Mail-Adresse wird häufig als E-Mail-aktivierte Gruppe bezeichnet.

Sie können z. B. eine E-Mail-aktivierte Sicherheitsgruppe, eine statische Verteilergruppe und eine Office 365-Gruppe verwenden. Sie können keine Sicherheitsgruppe (dynamisch oder statisch) verwenden, da dieser Typ keine E-Mail-Adresse besitzt. Ferner können Sie keine dynamische Verteilerliste von Exchange Online verwenden, da diese Gruppe nicht nach Azure AD repliziert wird.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Vorbereiten von Benutzern und Gruppen für Azure Information Protection

5. Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat ein Microsoft 365-Abonnement.

Sie identifizieren die folgenden Anforderungen für die Verhinderung von Datenverlust:

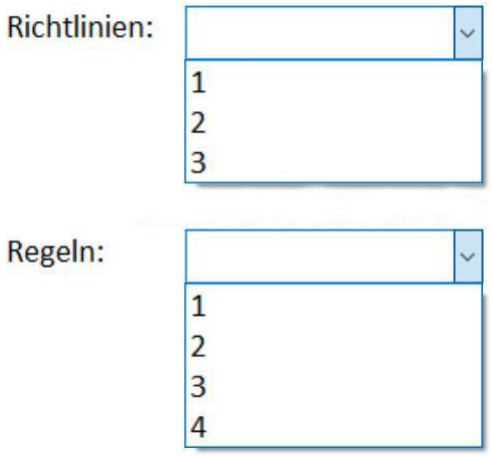
Benutzer müssen Benachrichtigungen erhalten, wenn sie versuchen, Anhänge zu senden, die EU-Sozialversicherungsnummern enthalten.
Es muss verhindert werden, dass E-Mail-Nachrichten mit Kreditkartennummern an Empfänger außerhalb Ihres Unternehmens gesendet werden.
Die externe Freigabe von Microsoft OneDrive-Inhalten, die EU-Passnummern enthalten, muss blockiert werden.
Wenn Regelübereinstimmungen auftreten, müssen Administratoren E-Mail-Benachrichtigungen erhalten.

Wie viele Richtlinien zur Verhinderung von Datenverlust (DLP-Richtlinien) und Regeln müssen Sie mindestens erstellen, um die Anforderungen zu erfüllen?

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

Abbildung

Antwortbereich



A.Richtlinien: 1
Regeln: 1
B.Richtlinien: 1
Regeln: 2
C.Richtlinien: 2
Regeln: 3
D.Richtlinien: 2
Regeln: 4
E.Richtlinien: 3
Regeln: 3
F.Richtlinien: 3
Regeln: 4

Korrekte Antwort: C

Erläuterungen:

Die Verhinderung vor Datenverlust ist ein Compliance-Feature von Office 365, mit dem Ihre Organisation verhindern kann, dass vertrauliche Informationen absichtlich oder versehentlich an unerwünschte Personen übertragen werden. DLP hat seinen Ursprung in Exchange Server und Exchange Online und kann auch in SharePoint Online und OneDrive for Business angewendet werden.

DLP verwendet ein Inhaltsanalysemodul, um den Inhalt von E-Mail-Nachrichten und Dateien zu überprüfen und nach vertraulichen Informationen wie Kreditkartennummern und personenbezogenen Informationen (Personally Identifiable Information, PII) zu suchen. Vertrauliche Informationen sollten in der Regel nicht per E-Mail gesendet oder in Dokumente einbezogen werden, ohne zusätzliche Schritte auszuführen, wie z. B. die Verschlüsselung der betreffenden E-Mail-Nachrichten oder Dateien. Mithilfe von DLP können Sie vertrauliche Informationen identifizieren und die folgenden Aktionen vorsehen:

Protokollieren des Ereignisses zu Überwachungszwecken

Anzeigen einer Warnung für den Endbenutzer, der die E-Mail-Nachricht senden oder die Datei freigeben möchte

Aktives Blockieren der E-Mail-Nachricht oder der Dateifreigabe

Wir benötigen eine DLP-Richtlinie, die ausschließlich auf Exchange Online angewendet wird. Die Richtlinie muss zwei Regeln enthalten. Eine Regel, um das Senden von Anhängen mit EU-Sozialversicherungsnummern zu verhindern und eine zweite Regel, die verhindert, dass E-Mail-Nachrichten mit Kreditkartennummern an Empfänger außerhalb Ihres Unternehmens gesendet werden.

Außerdem müssen wir eine DLP-Richtlinie mit einer einzelnen Regel für OneDrive erstellen, um die externe Freigabe von Microsoft OneDrive-Inhalten zu blockieren, die EU-Passnummern enthalten.

Jede Regel kann so konfiguriert werden, dass Vorfallberichte an Administratoren gesendet werden, wenn eine Regelübereinstimmung auftritt.

Insgesamt benötigen wir mindestens zwei Richtlinien und drei Regeln.