Prüfungsnummer:MS-100

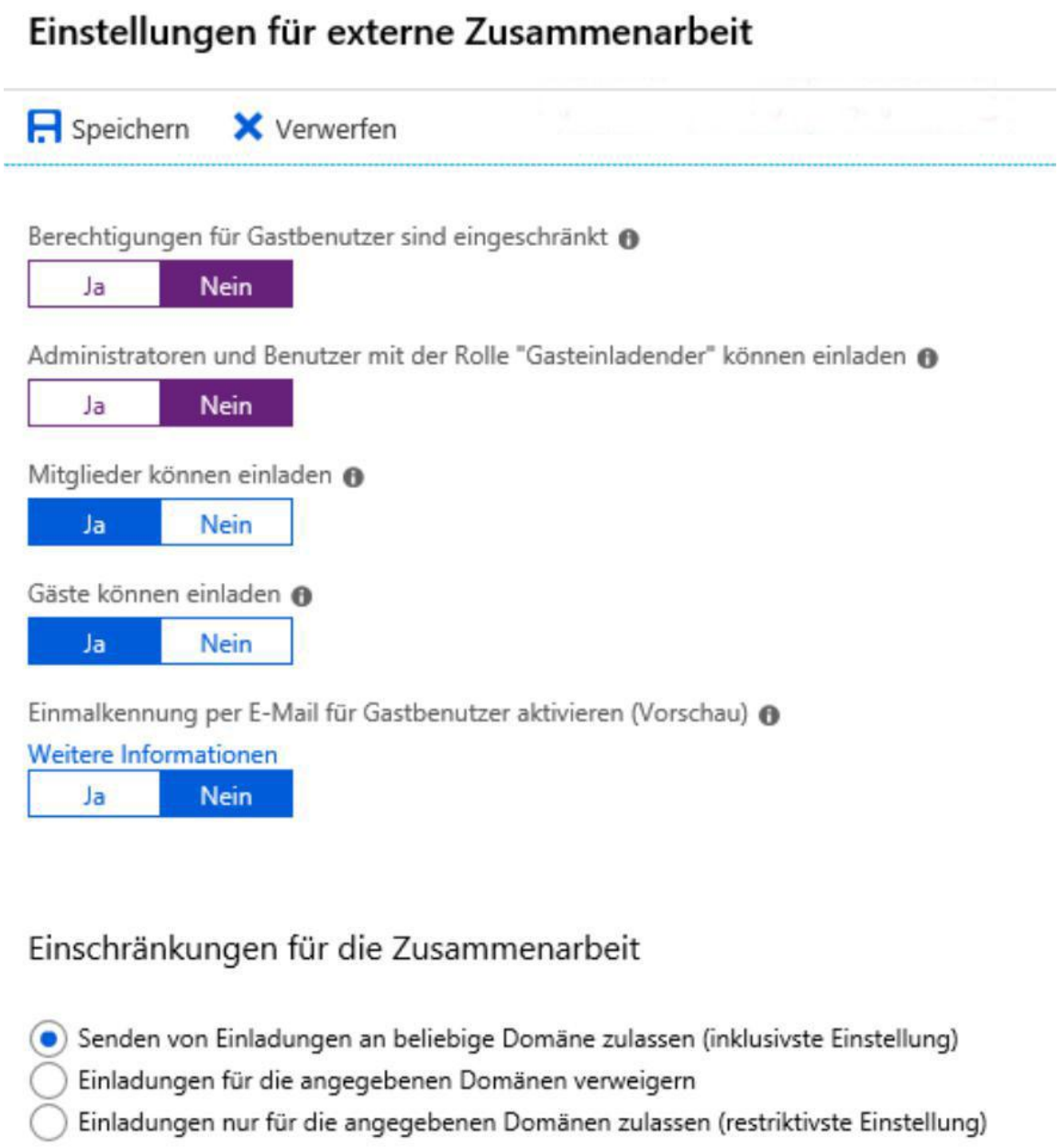
Prüfungsname: Microsoft 365 Identity and Services

Version:demo

1.Sie haben ein Microsoft 365-Abonnement und einen Microsoft Azure Active Directory (Azure AD)-Mandanten mit dem Namen it-pruefungen.de. it-pruefungen.de enthält die in der folgenden Tabelle aufgeführten Benutzer:

Name	Benutzertyp	Rolle
Benutzer1	Member	Keine
Benutzer2	Member	Sicherheitsadministrator, Gasteinladender
Benutzer3	Member	Benutzeradministrator
Benutzer4	Guest	Keine

Die Einstellungen für die externe Zusammenarbeit des Mandanten werden nachstehend gezeigt:



Sie müssen sicherstellen, dass Gastkonten erstellt werden können.
Welche Einstellung ändern Sie?

A.Gäste können einladen.
B.Berechtigungen für Gastbenutzer sind eingeschränkt.
C.Mitglieder können einladen.
D.Administratoren und Benutzer mit der Rolle „Gasteinladender“ können einladen.
E.Einladungen für die angegebenen Domänen verweigern.

Korrekte Antwort: D

Erläuterungen:
Administratoren und Mitglieder der Rolle "Gasteinladender" können keine Gäste für den

Mandanten einladen. Die entsprechende Option muss mit "Ja" festgelegt werden.
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Delegieren von Einladungen zur Azure Active Directory B2B-Zusammenarbeit

2.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat kürzlich ein Microsoft 365-Abonnement erworben.
Sie aktivieren die Microsoft Azure-Multi-Factor-Authentifizierung (MFA) für alle 500 Benutzer im Azure Active Directory-Mandanten (Azure AD).
Sie müssen einen Bericht generieren, der alle Benutzer auflistet, die den Azure MFA-Registrierungsvorgang abgeschlossen haben.
Was ist der beste Ansatz, um das Ziel zu erreichen?
(Zum Erreichen des Ziels kann mehr als eine Antwort geeignet sein. Wählen Sie die beste Antwort.)

A.Führen Sie in der Azure Cloud Shell das Cmdlet Get-AzureADUser aus.
B.Führen Sie in der Azure Cloud Shell das Cmdlet Get-MsolUser aus.
C.Verwenden Sie das Blade „MFA“ im Azure Active Directory-Verwaltungscenter.
D.Verwenden Sie das Blade „Benutzer mit Risikomarkierung“ im Azure Active Directory-Verwaltungscenter.

Korrekte Antwort: C

Erläuterungen:
Es gibt zwei Ansätze, um die zweistufige Überprüfung zu erzwingen, wobei beide die Verwendung eines globalen Administratorkontos erfordern. Die erste Option besteht darin, jeden einzelnen Benutzer für Azure Multi-Factor Authentication (MFA) zu aktivieren. Wenn Benutzer einzeln aktiviert werden, führen sie die zweistufige Überprüfung bei jeder Anmeldung durch (bis auf einige Ausnahmen, beispielsweise wenn sie sich von vertrauenswürdigen IP-Adressen aus anmelden oder wenn die Funktion Gespeicherte Geräte aktiviert ist). Die zweite Möglichkeit besteht darin, eine Richtlinie für bedingten Zugriff einzurichten, die unter bestimmten Umständen eine zweistufige Überprüfung erfordert.
Benutzerkonten in Azure Multi-Factor Authentication können die folgenden drei Zustände aufweisen:

Status	BESCHREIBUNG	Nicht-Browser-Apps betroffen	Browser-Apps betroffen	Moderne Authentifizierung betroffen
Deaktiviert	Der Standardstatus eines neuen Benutzers, der nicht für Azure MFA registriert ist.	Nein	Nein	Nein
Aktiviert	Der Prozess der Registrierung für Azure MFA für den Benutzer wurde begonnen, aber noch nicht abgeschlossen. Der Benutzer wird aufgefordert, sich bei der nächsten Anmeldung zu registrieren.	Nein. Sie werden weiterhin ausgeführt, bis die Registrierung abgeschlossen ist.	Ja. Nachdem die Sitzung abläuft, ist eine Azure MFA-Registrierung erforderlich.	Ja. Nachdem das Zugriffstoken abläuft, ist eine Azure MFA-Registrierung erforderlich.
Erzwungen	Der Benutzer wurde registriert und hat den Registrierungsprozess für Azure MFA abgeschlossen.	Ja. Für Apps sind App-Kennwörter erforderlich.	Ja. Azure MFA ist bei der Anmeldung erforderlich.	Ja. Azure MFA ist bei der Anmeldung erforderlich.

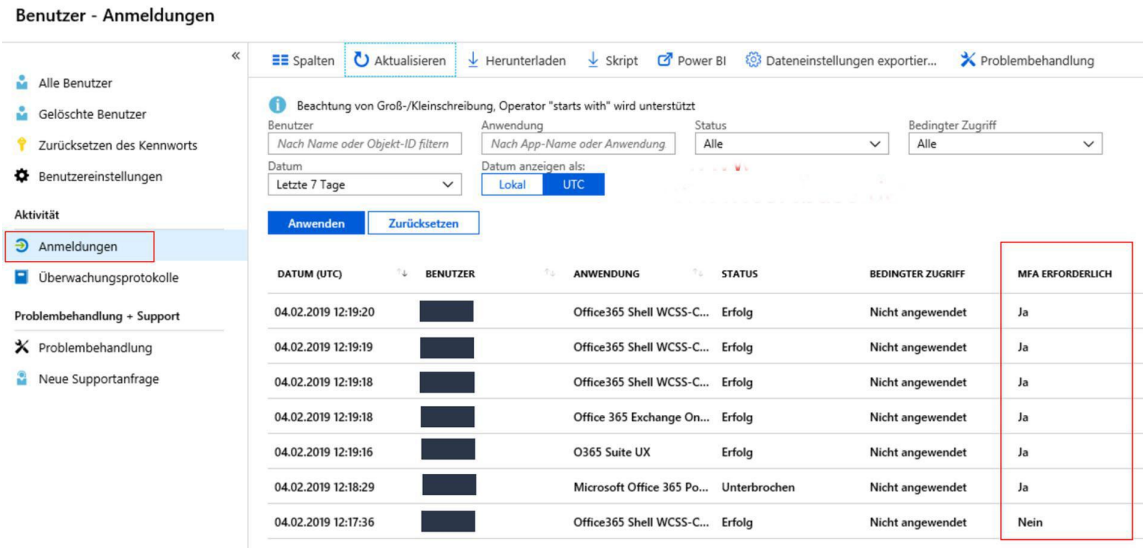
Anzeigen des Status eines Benutzers
Führen Sie die folgenden Schritte aus, um auf die Seite zuzugreifen, auf der Sie Benutzerstatus anzeigen und verwalten können:
Melden Sie sich beim Azure-Portal als Administrator an.
Navigieren Sie zu Azure Active Directory > Benutzer und Gruppen > Alle Benutzer.
Wählen Sie Multi-Factor Authentication aus.
Es wird eine neue Seite geöffnet, auf der die Benutzerstatus angezeigt werden.
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Vorgehensweise zum Erzwingen einer zweistufigen Überprüfung für einen Benutzer

3.Sie sind Administrator eines Unternehmens. Sie haben ein Microsoft 365 Enterprise-Abonnement.
Sie haben eine Richtlinie für den bedingten Zugriff erstellt, um die Multi-Faktor-Authentifizierung beim Zugriff auf Microsoft SharePoint von einem mobilen Gerät aus zu erzwingen.
Sie müssen anzeigen, welche Benutzer mithilfe der Multi-Faktor-Authentifizierung authentifiziert wurden.
Wie gehen Sie vor?

A.Verwenden Sie das Microsoft 365 Admin Center und sehen Sie die Security Compiance-Berichte ein.
B.Verwenden Sie das Azure Active Directory-Verwaltungscenter und sehen Sie die Anmeldungen ein.
C.Verwenden Sie das Microsoft 365 Admin Center und sehen Sie die Nutzungsberichte ein.
D.Verwenden Sie das Azure Active Directory-Verwaltungscenter und sehen Sie die Überwachungsprotokolle ein.

Korrekte Antwort: B

Erläuterungen:
Auf der Seite „Anmeldungen“ im Azure AD-Portal können Sie eine Liste der Benutzeranmeldungen einsehen. In der Spalte „MFA ERFORDERLICH“ wird angezeigt, ob der Benutzer mehrstufig authentifiziert wurde.



4.Sie sind als Administrator für das Unternehmen it-pruefungen.de tätig. Sie haben ein Microsoft 365 Enterprise E5-Abonnement.
Sie müssen für die Mitarbeiter der Finanzabteilung die Multi-Faktor-Authentifizierung für alle Cloud-basierten Anwendungen erzwingen.
Wie gehen Sie vor?

A.Erstellen Sie eine Cloud App Security-Aktivitätsrichtlinie.
B.Erstellen Sie eine Richtlinie zum Anmelderisiko.
C.Erstellen Sie eine Cloud App Security-Sitzungsrichtlinie.
D.Erstellen Sie eine Cloud App Security-App-Ermittlungsrichtlinie.

Korrekte Antwort: B

Erläuterungen:
Azure Active Directory erkennt Risikoereignistypen in Echtzeit und offline. Alle Risikoereignisse, die bei der Anmeldung eines Benutzers erkannt wurden, tragen zu einem logischen Konzept bei, das als „riskante Anmeldung“ bezeichnet wird. Eine risikobehaftete Anmeldung ist ein Hinweis auf einen Anmeldeversuch, der nicht vom rechtmäßigen Besitzer eines Benutzerkontos durchgeführt wurde.
Azure AD analysiert jede Anmeldung eines Benutzers. Das Ziel der Analyse besteht darin, verdächtige Aktionen zu erkennen, die mit der Anmeldung verbunden sind. Wird die Anmeldung beispielsweise mit einer anonymen IP-Adresse durchgeführt, oder wird die

Anmeldung von einem unbekannten Ort aus initiiert? In Azure AD werden die verdächtigen Aktionen, die vom System erkannt werden können, auch als Risikoereignisse bezeichnet. Basierend auf den Risikoereignissen, die während einer Anmeldung erkannt wurden, berechnet Azure AD einen Wert. Der Wert steht für die Wahrscheinlichkeit (gering, mittel, hoch), dass die Anmeldung nicht vom befugten Benutzer durchgeführt wird. Die Wahrscheinlichkeit wird als Risikostufe der Anmeldung bezeichnet.
Die Richtlinie zum Anmelderisiko ist eine automatisierte Antwort, die Sie für eine bestimmte Risikostufe der Anmeldung konfigurieren können. In Ihrer Antwort können Sie den Zugriff auf Ihre Ressourcen blockieren oder die Durchführung einer mehrstufigen Authentifizierung (Multi-Factor Authentication, MFA) zur Bedingung machen, bevor der Zugriff gewährt wird.
Die Richtlinie zum Anmelderisiko befindet sich auf der Azure AD Identity Protection-Seite im Abschnitt Konfigurieren.
Mit einer Richtlinie zum Anmelderisiko kann die mehrstufige Authentifizierung für eine bestimmte Benutzergruppe auf ähnliche Weise wie mit einer Richtlinie für den bedingten Zugriff erzwungen werden.
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Anleitung: Konfigurieren der Richtlinie zum Anmelderisiko

5.Sie sind als Administrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen verfügt über eine On-Premises Microsoft Exchange Server 2013-Organisation.
Das Unternehmen hat 100 Benutzer.
Das Unternehmen kauft Microsoft 365-Lizenzen und plant, die gesamte Infrastruktur in die Cloud zu verlagern. Das Unternehmen möchte die lokale Active Directory-Domäne nicht mit Microsoft Azure Active Directory (Azure AD) synchronisieren.
Sie müssen empfehlen, mit welcher Art von Migration alle E-Mail-Nachrichten, Kontakte und Kalenderelemente nach Exchange Online verschoben werden sollen.
Welche Migrationsmethode empfehlen Sie?

A.Übernahmemigration
B.IMAP-Migration
C.Remoteverschiebevorgang
D.Mehrstufige Migration

Korrekte Antwort: A

Erläuterungen:
Daten können auf unterschiedliche Weise aus einer lokalen E-Mail-Organisation zu Microsoft Exchange Online in Microsoft Office 365 migriert werden. Bei der Planung einer Migration zu Exchange Online stellt sich häufig die Frage nach einer Verbesserung der Datenmigrationsleistung sowie nach einer Optimierung der Migrationsgeschwindigkeit.

Häufig verwendete Migrationsmethoden:

IMAP-Migration

Sie können mit der Exchange-Verwaltungskonsole oder der Exchange-Verwaltungsshell den Inhalt der Benutzerpostfächer von einem IMAP-Nachrichtensystem zu den Exchange Online-Postfächern der Benutzer migrieren. Hierzu gehört auch das Migrieren der Postfächer von anderen gehosteten E-Mail-Diensten, z. B. Google Mail oder Yahoo Mail.

Übernahmemigration

Mithilfe einer Übernahmemigration können Sie alle lokalen Postfächer innerhalb von wenigen Tagen zu Exchange Online migrieren. Dieser Migrationstyp bietet sich an, wenn Sie planen, Ihre gesamte E-Mail-Organisation zu Office 365 zu verschieben und Benutzerkonten in Office 365 zu verwalten. Bei einer Übernahmemigration können maximal 2.000 Postfächer aus der lokalen Exchange-Organisation zu Exchange Online migriert werden. Die E-Mail-Kontakte und Verteilergruppen in Ihrer lokalen Exchange-Organisation werden ebenfalls migriert.

Mehrstufige Migration

Verwenden Sie eine mehrstufige Migration, wenn Sie planen, sämtliche Postfächer Ihres Unternehmens nach und nach zu Exchange Online zu migrieren. Wenn Sie eine mehrstufige Migration verwenden, werden Batches lokaler Postfächer über einen Zeitraum von ein paar Wochen oder Monaten zu Exchange Online migriert. Ihr Ziel besteht darin, die E-Mail-Organisation dauerhaft in Office 365 zu verschieben.

Hybridbereitstellung (Remoteverschiebevorgang)

Eine Hybridbereitstellung bietet Unternehmen die Möglichkeit, den Funktionsreichtum und die Verwaltungskontrolle, die die vorhandene lokale Microsoft Exchange-Organisation bietet, auf die Cloud auszudehnen. Eine Hybridbereitstellung bietet für eine lokale Exchange 2013 oder 2010-Organisation und Exchange Online in Microsoft Office 365 ein einheitliches Erscheinungsbild als nahtlose Exchange-Organisation. Darüber hinaus kann eine Hybridbereitstellung als Zwischenschritt vor dem vollständigen Wechsel zu einer Exchange Online-Organisation dienen.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Methoden zum Migrieren mehrerer E-Mail-Konten zu Office 365