Prüfungsnummer:SC-300

Prüfungsname: Microsoft Identity and Access Administrator

Version:demo

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

1.Sie haben einen Azure Active Directory (Azure AD)-Mandanten, der die folgenden Objekte enthält:
Ein Gerät namens Device1
Benutzer mit den Namen Benutzer1, Benutzer2, Benutzer3, Benutzer4 und Benutzer5
Gruppen mit den Namen Gruppe1, Gruppe2, Gruppe3, Gruppe4 und Gruppe5
Die Konfiguration der Gruppen wird in der folgenden Tabelle gezeigt:

Name	Typ	Mitgliedschaftstyp	Mitglieder
Gruppe1	Sicherheit	Zugewiesen	Benutzer1, Benutzer3, Gruppe2, Grupp3
Gruppe2	Sicherheit	Dynamischer Benutzer	Benutzer2
Gruppe3	Sicherheit	Dynamisches Gerät	Device1
Gruppe4	Microsoft 365	Zugewiesen	Benutzer4
Gruppe5	Microsoft 365	Dynamischer Benutzer	Benutzer5

Welchen Gruppen können Sie eine Microsoft Office 365 Enterprise E5-Lizenz direkt zuweisen?

A.Nur Gruppe1 und Gruppe4
B.Gruppe1, Gruppe2, Gruppe3, Gruppe4 und Gruppe5
C.Nur Gruppe1 und Gruppe2
D.Nur Gruppe1
E.Nur Gruppe1, Gruppe2, Gruppe4 und Gruppe5

Korrekte Antwort: B

Erläuterungen:

Für kostenpflichtige Microsoft-Clouddienste wie Microsoft 365, Enterprise Mobility + Security, Dynamics 365 und ähnliche Produkte werden Lizenzen benötigt. Diese Lizenzen werden jedem Benutzer zugewiesen, der Zugriff auf diese Dienste benötigt. Administratoren verwalten Lizenzen über eines der Verwaltungsportale (Office, Azure) und PowerShell-Cmdlets. Azure AD ist die zugrunde liegende Infrastruktur, die die Identitätsverwaltung für alle Microsoft-Clouddienste unterstützt. Azure AD speichert Informationen zum Lizenzzuweisungsstatus für Benutzer.

Azure AD beinhaltet die gruppenbasierte Lizenzierung, mit der Sie einer Gruppe eine oder mehrere Produktlizenzen zuweisen können. Azure AD stellt sicher, dass die Lizenzen

allen Mitgliedern der Gruppe zugewiesen werden. Allen neuen Mitgliedern, die der Gruppe beitreten, werden die entsprechenden Lizenzen zugewiesen. Wenn sie die Gruppe verlassen, werden diese Lizenzen entfernt. Dadurch ist keine automatisierte Lizenzverwaltung über PowerShell mehr erforderlich, um Änderungen in der Organisations- und Abteilungsstruktur benutzerbezogen widerzuspiegeln.

Das Feature kann nur mit Sicherheitsgruppen und Microsoft 365-Gruppen verwendet werden, für die "securityEnabled=TRUE" gilt.

Hinweis: Gruppe1 enthält neben Benutzern auch Gruppen als Mitglieder. Die Lizenzzuweisung an Gruppe1 wirkt sich nur auf Benutzer aus, die ein direktes Mitglied von Gruppe1 sind. Die gruppenbasierte Lizenzzuweisung unterstützt keine Mitglieder in verschachteleten Gruppen. Gruppe3 enthält ausschließlich Geräte. Wir können Gruppe3 dennoch direkt eine Lizenz zuweisen. Die Zuweisung wird jedoch niemals dazu führen, dass ein Benutzer eine Lizenz erhält.

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

Was ist die gruppenbasierte Lizenzierung in Azure Active Directory?

Szenarien, Einschränkungen und bekannte Probleme mit der Verwendung von Gruppen zum Verwalten der Lizenzierung in Azure Active Directory

Zuweisen von Lizenzen zu Benutzer nach Gruppenmitgliedschaft in Azure Active Directory

2.Sie haben eine Microsoft Exchange-Organisation, die den SMTP-Adressraum contoso.com verwendet.

Mehrere Benutzer verwenden ihre contoso.com-E-Mail-Adresse für die Self-Service-Registrierung bei Azure Active Directory (Azure AD).

Sie erhalten globale Administratorrechte für den Azure AD-Mandanten, der die selbstregistrierten Benutzer enthält.

Sie müssen die Benutzer daran hindern, Benutzerkonten im Azure AD-Mandanten contoso.com für die Self-Service-Registrierung bei Microsoft 365-Diensten zu erstellen.

Welches PowerShell-Cmdlet sollten Sie ausführen?

A.Set-MsolCompanySettings
B.Set-MsolDomainFederationSettings
C.Update-MsolFederatedDomain

D.Set-MsolDomain

Korrekte Antwort: A

Erläuterungen:

Self-Service-Registrierung ist eine Methode, mit der sich ein Benutzer für einen Clouddienst registriert, wobei für ihn basierend auf seiner E-Mail-Domäne automatisch eine Identität in Azure AD erstellt wird.

Gründe für das Verwenden der Self-Service-Registrierung
Kunden erhalten schneller die gewünschten Dienste.
Sie können E-Mail-basierte Angebote für einen Dienst erstellen.
Sie können E-Mail-basierte Registrierungsabläufe erstellen, mit denen Benutzer schnell Identitäten mithilfe ihrer einfach zu merkenden geschäftlichen E-Mail-Aliase erstellen können.
Ein per Self-Service erstellter Azure AD-Mandant kann in einen verwalteten Mandanten konvertiert werden, der für andere Dienste verwendet werden kann.
Wie steuere ich Self-Service-Einstellungen?
Administratoren stehen derzeit zwei Self-Service-Steuerungsmöglichkeiten zur Verfügung. Sie können steuern, ob:

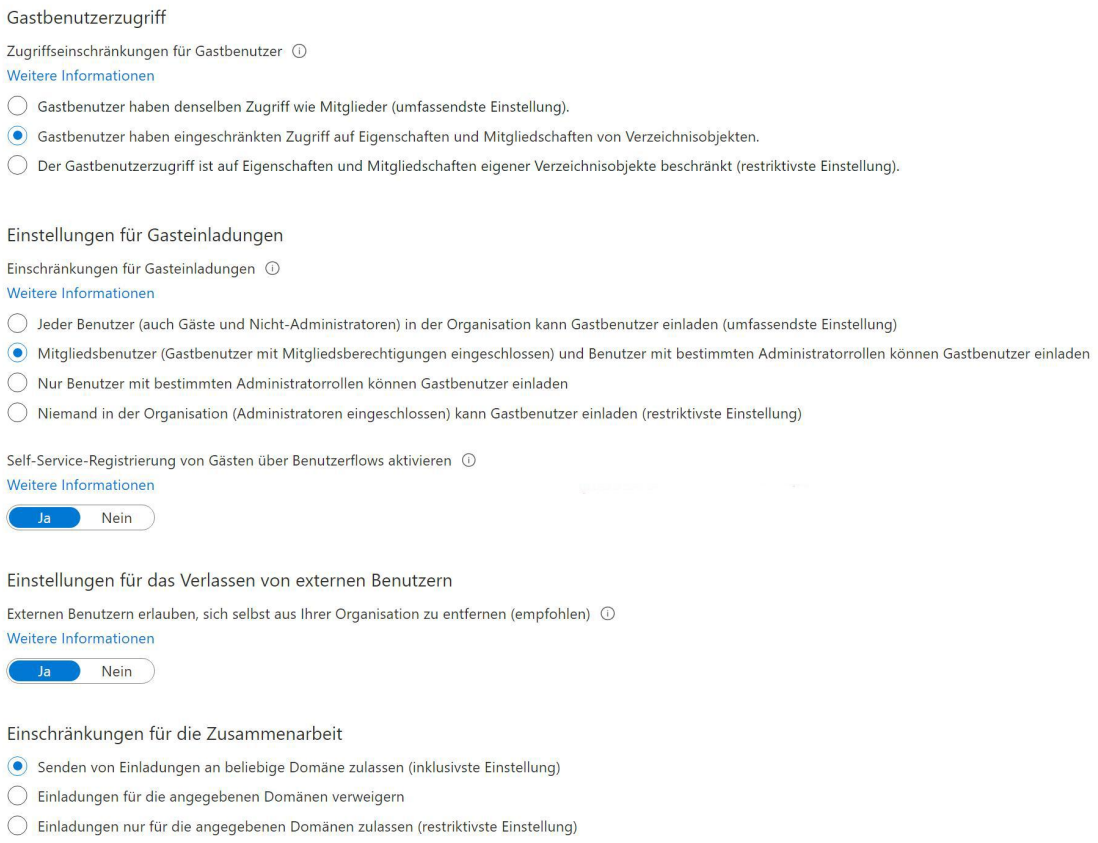
Benutzer dem Mandanten per E-Mail beitreten können.
Benutzer sich selbst für Anwendungen und Dienste lizenzieren können.
Wie können diese Funktionen gesteuert werden?
Ein Administrator kann diese Funktionen mit den folgenden Parametern des Azure AD-Cmdlets Set-MsolCompanySettings konfigurieren:

AllowEmailVerifiedUsers steuert, ob Benutzer dem Mandanten per E-Mail-Überprüfung beitreten können. Zum Beitreten muss der Benutzer über eine E-Mail-Adresse in einer Domäne verfügen, die einer der überprüften Domänen im Mandanten entspricht. Diese Einstellung wird unternehmensweit auf alle Domänen im Mandanten angewendet. Wenn Sie diesen Parameter auf „$false“ festlegen, können dem Mandanten keine über E-Mail verifizierten Benutzer beitreten.
AllowAdHocSubscriptions steuert, ob Benutzern das Ausführen der Self-Service-Registrierung erlaubt ist. Wenn Sie diesen Parameter auf „$false“ festlegen, können Benutzer keine Self-Service-Registrierung ausführen.
Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Was ist die Self-Service-Registrierung für Azure Active Directory?

3.Sie haben einen Microsoft 365-Mandanten, der eine Domäne namens fabrikam.com verwendet. Die Einstellungen für den Gastbenutzerzugriff in Azure Active Directory (Azure

AD) sind wie in der Abbildung gezeigt konfiguriert:



Ein Benutzer mit dem Namen bsmith@fabrikam.com gibt eine Microsoft SharePoint Online-Dokumentbibliothek für die in der folgenden Tabelle aufgeführten Benutzer frei:

Name	E-Mail	Beschreibung
Benutzer1	Benutzer1@contoso.com	Ein Gastbenutzer in fabrikam.com
Benutzer2	Benutzer2@outlook.com	Ein Benutzer, der noch nie auf Ressourcen in fabrikam.com zugegriffen hat
Benutzer3	Benutzer3@fabrikam.com	Ein Benutzer in fabrikam.com

Welche Benutzer erhalten einen Passcode per E-Mail?

A.Nur Benutzer2
B.Nur Benutzer1
C.Nur Benutzer1 und Benutzer2
D.Benutzer1, Benutzer2 und Benutzer3

Korrekte Antwort: A

Erläuterungen:

Das Feature „Einmalkennung per E-Mail“ ist eine Möglichkeit zum Authentifizieren von Benutzern für die B2B-Zusammenarbeit, wenn sie nicht auf andere Weise – z. B. Azure AD, Microsoft-Konto (MSA) oder soziales Netzwerk als Identitätsanbieter – authentifiziert werden können. Wenn ein B2B-Gastbenutzer versucht, Ihre Einladung einzulösen oder sich bei Ihren freigegebenen Ressourcen anzumelden, kann er eine temporäre Kennung anfordern, die an seine E-Mail-Adresse gesendet wird. Dann gibt er diesen so genannten „Passcode“ ein, um den Anmeldevorgang fortzusetzen.

Wenn ein Gastbenutzer eine Einladung einlöst oder einen Link zu einer Ressource verwendet, die für ihn freigegeben wurde, erhält er unter folgenden Bedingungen eine Einmalkennung:

Er besitzt kein Azure AD-Konto.
Er besitzt kein Microsoft-Konto.
Der einladende Mandant hat keinen Verbund mit sozialen Netzwerken (wie Google) oder anderen Identitätsanbietern eingerichtet.
Er verwendet keine andere Authentifizierungsmethode oder besitzt kein kennwortgeschütztes Konto.
Einmalkennung per E-Mail ist aktiviert.
Zum Zeitpunkt der Einladung gibt es keinen Hinweis darauf, dass der eingeladene Benutzer die Authentifizierung mit Einmalkennung verwendet. Wenn sich der Gastbenutzer jedoch anmeldet, wird die Authentifizierung mit Einmalkennung als alternative Methode verwendet, wenn keine anderen Authentifizierungsmethoden eingesetzt werden können.

Die E-Mail-Einmal-Passcode-Funktion ist jetzt standardmäßig für alle neuen Mandanten und für alle bestehenden Mandanten aktiviert, bei denen Sie sie nicht explizit deaktiviert haben.

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

Authentifizierung mit Einmalkennung per E-Mail

4.Sie haben 2.500 Benutzer, denen Microsoft Office 365 Enterprise E3-Lizenzen zugewiesen sind. Die Lizenzen sind einzelnen Benutzern zugewiesen.

Sie weisen den Benutzern Microsoft 365 Enterprise E5-Lizenzen über die Seite "Gruppen" im Azure Active Directory Admin Center zu.

Sie müssen die Office 365 Enterprise E3-Lizenzen mit dem geringsten administrativen Aufwand von den Benutzern entfernen.

Was sollten Sie verwenden?

A.Die Seite "Identity Governance" im Azure Active Directory Admin Center.
B.Das Cmdlet Set-AzureAdUser.
C.Die Seite Lizenzen im Azure Active Directory Admin Center.
D.Das Cmdlet Set-WindowsProductKey.

Korrekte Antwort: C

Erläuterungen:

Sie können eine Lizenz auf der Azure AD-Benutzerseite eines Benutzers und auf der Gruppenübersichtsseite für eine Gruppenzuweisung entfernen. Oder Sie beginnen auf der Azure AD-Seite Lizenzen, um die Benutzer und Gruppen für eine Lizenz anzuzeigen.

Wenn Sie PowerShell bevorzugen, können Sie das Cmdlet Set-MsolUserLicense verwenden, um die Lizenzzuweisung für einen Benutzer zu aktualisieren.

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

Zuweisen oder Entfernen von Lizenzen im Azure Active Directory-Portal

Set-MsolUserLicense

5.Sie haben einen Azure Active Directory (Azure AD)-Mandanten, der einen Benutzer mit dem Namen SecAdmin1 enthält. SecAdmin1 ist die Rolle Sicherheitsadministrator zugewiesen.

SecAdmin1 berichtet, dass er Kennwörter nicht über das Azure AD Identity Protection-Portal zurücksetzen kann.

Sie müssen sicherstellen, dass SecAdmin1 Kennwörter verwalten und Sitzungen im Namen von Benutzern ohne Administratorrechte entwerten kann. Die Lösung muss das Prinzip der Vergabe geringstmöglicher Berechtigungen verwenden.

Welche Rolle sollten Sie SecAdmin1 zuweisen?

A.Authentifizierungsadministrator
B.Helpdeskadministrator
C.Privilegierter Authentifizierungsadministrator
D.Sicherheitsoperator

Korrekte Antwort: B

Erläuterungen:

Benutzer mit der Rolle Helpdeskadministrator können Kennwörter ändern, Aktualisierungstoken entwerten, Dienstanforderungen verwalten und die Dienstintegrität überwachen. Durch das Entwerten eines Aktualisierungstokens werden Benutzer gezwungen, sich erneut anzumelden. Helpdeskadministratoren können Kennwörter zurücksetzen und Aktualisierungstoken anderer Benutzer entwerten, die keine Administratoren sind oder denen nur die folgenden Rollen zugewiesen wurden:

Verzeichnisleseberechtigte
Gasteinladender
Helpdeskadministrator
Nachrichtencenter-Leseberechtigter
Kennwortadministrator
Berichtleseberechtigter
Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Integrierte Rollen in Azure AD

6.Sie haben einen Microsoft 365-Mandanten.

Alle Benutzer haben Mobiltelefone und Laptops.

Die Benutzer arbeiten häufig von entfernten Standorten aus, die keinen Wi-Fi-Zugang und keine Mobiltelefonverbindung haben. Während sie von entfernten Standorten aus arbeiten, verbinden die Benutzer ihren Laptop mit einem kabelgebundenen Netzwerk mit Internetzugang.

Sie planen die Implementierung der mehrstufigen Authentifizierung (MFA).

Welche MFA-Authentifizierungsmethode können die Benutzer vom entfernten Standort verwenden?

A.Einen Bestätigungscode von der Microsoft Authenticator-App
B.Sicherheitsfragen
C.Sprachanruf
D.SMS

Korrekte Antwort: A

Erläuterungen:

Einige Authentifizierungsmethoden können als primärer Faktor verwendet werden, wenn Sie sich bei einer Anwendung oder einem Gerät anmelden, z. B. mit einem FIDO2-Sicherheitsschlüssel oder einem Kennwort. Andere Authentifizierungsmethoden sind nur als sekundärer Faktor verfügbar, wenn Sie Azure AD Multi-Factor Authentication oder Self-Service-Kennwortzurücksetzung (SSPR) verwenden.

Aus der folgenden Tabelle geht hervor, wann eine Authentifizierungsmethode bei einem Anmeldeereignis verwendet werden kann:

Methode	Primäre Authentifizierung	Sekundäre Authentifizierung
Windows Hello for Business	Ja	MFA*
Microsoft Authenticator-App	Ja	MFA und SSPR
FIDO2-Sicherheitsschlüssel	Ja	MFA
Zertifikatbasierte Authentifizierung (Vorschau)	Ja	Nein
OATH-Hardwaretoken (Vorschau)	Nein	MFA und SSPR
OATH-Softwaretoken	Nein	MFA und SSPR
SMS	Ja	MFA und SSPR
Anruf	Nein	MFA und SSPR
Kennwort	Ja	

Hinweis: Sicherheitsfragen werden nicht als Authentifizierungsmethode verwendet, können aber während des Self-Service-Kennwortzurücksetzungsprozesses (SSPR) verwendet werden. Für Sprachanrufe und SMS ist eine Mobiltelefonverbindung erforderlich.

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

Welche Authentifizierungs- und Prüfmethoden stehen in Azure Active Directory zur Verfügung?

7.Sie konfigurieren einen neuen Microsoft 365-Mandanten für die Verwendung einer Standarddomäne mit dem Namen contoso.com.

Sie müssen sicherstellen, dass Sie den Zugriff auf Microsoft 365-Ressourcen mithilfe von Richtlinien für bedingten Zugriff steuern können.

Was sollten Sie zuerst tun?

A.Deaktivieren Sie die Benutzereinwilligungseinstellungen.
B.Deaktivieren Sie die Sicherheitsstandards.
C.Konfigurieren Sie eine Registrierungsrichtlinie für die mehrstufige Authentifizierung (MFA).
D.Konfigurieren Sie den Kennwortschutz für Windows Server Active Directory.

Korrekte Antwort: B

Erläuterungen:

Wir können entweder Sicherheitsstandards aktivieren oder Richtlinien für bedingten Zugriff verwenden. Das Aktivieren von Sicherheitsstandards verhindert das Erstellen von Richtlinien für bedingten Zugriff. Umgekehrt verhindern bestehende Richtlinien für bedingten Zugriff die Aktivierung von Sicherheitsstandards.

Microsoft macht Sicherheitsstandard für alle verfügbar, da das Verwalten von Sicherheit schwierig sein kann. Identitätsbezogene Angriffe wie Kennwortspray- und Replay-Angriffe sowie Phishing sind heutzutage gängig. Mehr als 99,9 Prozent dieser identitätsbezogenen Angriffe werden mithilfe von Multi-Faktor-Authentifizierung (MFA) und durch Blockieren der Legacyauthentifizierung unterbunden. Das Ziel ist sicherzustellen, dass bei allen Organisationen mindestens eine Basissicherheitsebene ohne zusätzliche Kosten aktiviert ist.

Sicherheitsstandards können den Schutz Ihrer Organisation vor solchen identitätsbezogenen Angriffen mit vorkonfigurierten Sicherheitseinstellungen vereinfachen:

Festlegen, dass sich alle Benutzer für Azure AD Multi-Factor Authentication registrieren müssen
Administratoren müssen Multi-Faktor-Authentifizierung durchführen.
Benutzer müssen bei Bedarf Multi-Faktor-Authentifizierung durchführen.
Blockieren älterer Authentifizierungsprotokolle
Schützen privilegierter Aktivitäten wie Zugriff auf das Azure-Portal
Für wen eignet sich diese Funktion?
Organisationen, die ihren Sicherheitsstatus erhöhen möchten, aber nicht wissen, wie und wo sie damit beginnen sollen
Organisationen, die den kostenlos Tarif für Azure Active Directory verwenden
Wer sollte bedingten Zugriff verwenden?
Wenn Sie zu einer Organisation gehören, die derzeit Richtlinien für den bedingten Zugriff verwendet, sind Sicherheitsstandards wahrscheinlich nicht das Richtige für Sie.
Wenn Sie als Organisation über Azure Active Directory Premium-Lizenzen verfügen, sind die Sicherheitsstandards wahrscheinlich nicht die richtige Wahl für Sie.

Bei komplexen Sicherheitsanforderungen empfiehlt sich ggf. die Verwendung von bedingtem Zugriff.
Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Sicherheitsstandards in Azure AD

8.Sie haben einen Azure Active Directory (Azure AD)-Mandanten.

Sie öffnen den Risikoerkennungsbericht.

Welcher Risikoerkennungstyp wird als Benutzerrisiko eingestuft?

A.Unmöglicher Ortswechsel
B.Anonyme IP-Adresse
C.Ungewöhnlicher Ortswechsel
D.Kompromittierte Anmeldeinformationen

Korrekte Antwort: D

Erläuterungen:

Risikoerkennungen in Azure AD Identity Protection umfassen alle identifizierten verdächtigen Aktionen im Zusammenhang mit Benutzerkonten im Verzeichnis. Risikoerkennungen (im Zusammenhang mit Benutzern und Anmeldungen) tragen zur Gesamtrisikobewertung des Benutzers bei, die im Bericht zu riskanten Benutzern enthalten ist.

Risiken können auf Ebene der Benutzer und der Anmeldungen erkannt werden, und es gibt zwei Arten der Erkennung oder Berechnung (Echtzeit und Offline). Einige Risiken werden als Premium eingestuft, die nur für Azure AD Premium P2-Kunden verfügbar sind, während andere für Free- und Azure AD Premium P1-Kunden zur Verfügung stehen.

Der Risikoerkennungstyp Kompromittierte Anmeldeinformationen ist eine nicht-Premium-Benutzerrisikoerkennung und gibt an, dass die gültigen Anmeldeinformationen des Benutzers kompromittiert wurden. Wenn Internetkriminelle an gültige Kennwörter von berechtigten Benutzern gelangen, geben sie diese Anmeldeinformationen häufig weiter. Diese Freigabe erfolgt in der Regel durch eine Veröffentlichung im Darknet oder auf Paste Sites oder durch den Handel und Verkauf der Anmeldeinformationen auf dem Schwarzmarkt. Wenn der Microsoft-Dienst für durchgesickerte Anmeldedaten Benutzeranmeldedaten aus dem Dark Web, von Paste-Sites oder anderen Quellen erhält, werden diese mit den aktuellen gültigen Anmeldedaten der Azure AD-Benutzer abgeglichen, um gültige Übereinstimmungen zu finden.

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

Was bedeutet Risiko?