Prüfungsnummer:MS-220

Prüfungsname:(deutsche Version und englische Version) Problembehandlung für Microsoft Exchange Online

Version:demo

Achtung: Aktuelle englische Version zu MS-220 bei uns ist gratis!!

1.Ihr Unternehmen verwendet Exchange Online.

Ein Benutzer erhält einen Unzustellbarkeitsbericht, wenn er E-Mails an externe Empfänger sendet.

Sie führen eine Nachrichtenablaufverfolgung durch und stellen fest, dass keine E-Mails aus der Exchange-Umgebung gesendet werden.

Sie müssen die Komponente identifizieren, die das Problem verursacht.

Welche Komponente verursacht das Problem?

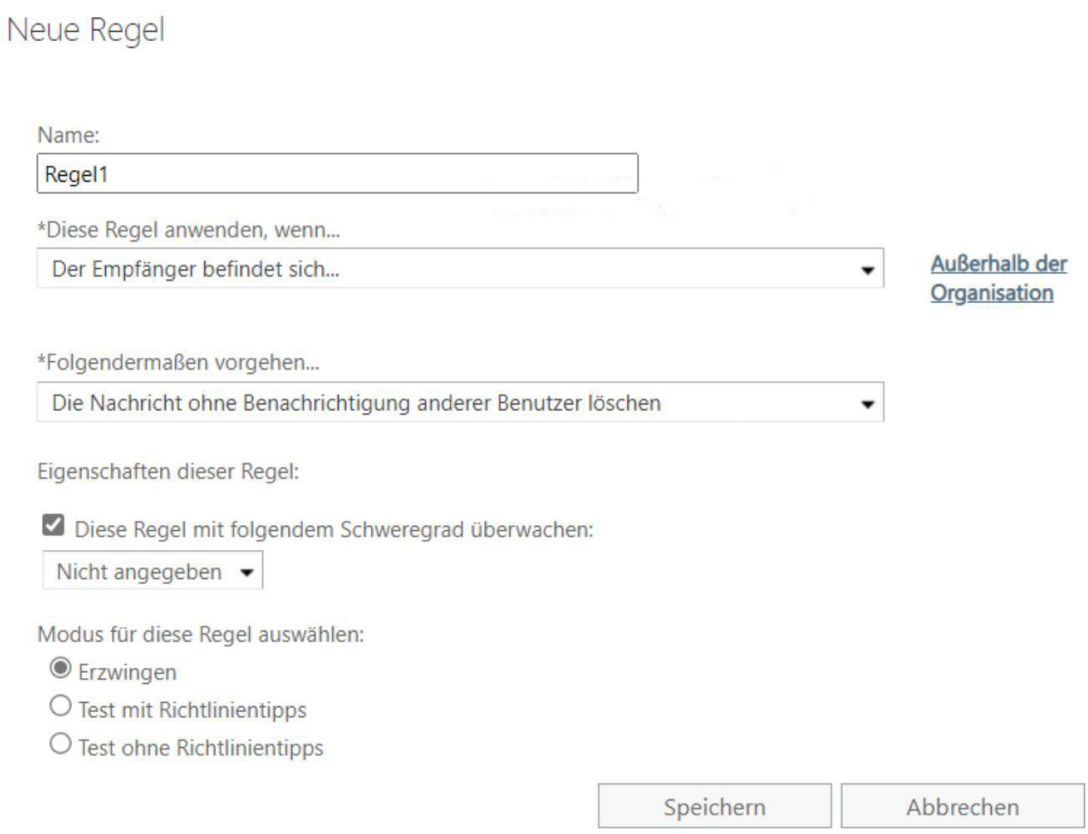
A.Antiphishing-Schutz
B.Antispoofing-Schutz
C.Richtlinien für Verbindungsfilter
D.E-Mail-Nachrichtenflussregeln

Korrekte Antwort: D

Erläuterungen:

Antiphishing-Schutz, Antispoofing-Schutz und Richtlinien für Verbindungsfilter wirken auf eingehende Nachrichten. Die wahrscheinlichste Ursache dafür, dass keine Nachrichten an externe Empfänger versendet werden, ist eine E-Mail-Flussregel, die ausgehende E-Mails an externe Empfänger blockiert.

In Exchange Online Organisationen oder eigenständigen Exchange Online Protection (EOP)-Organisationen ohne Exchange Online Postfächer können Sie E-Mail-Flussregeln (auch als Transportregeln bezeichnet) verwenden, um nach bestimmten Bedingungen für Nachrichten zu suchen, die ihre Organisation passieren, und Entsprechendes zu unternehmen.



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

Verwalten von Nachrichtenflussregeln in Exchange Online

2.Ein Unternehmen hat eine Microsoft Exchange Server 2019-Hybridumgebung. Der Exchange Server ist für die Verwendung der TLS-Verschlüsselung für SMTP konfiguriert.

Das TLS-Verschlüsselungszertifikat läuft ab.

Sie müssen ein neues Zertifikat für SMTP auf dem Server installieren.

Welche drei Cmdlets sollten Sie nacheinander ausführen?

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

Abbildung

A.Reihenfolge: 1, 4, 2
B.Reihenfolge: 1, 4, 3
C.Reihenfolge: 4, 6, 2
D.Reihenfolge: 4, 6, 3

Korrekte Antwort: B

Erläuterungen:

Transport Layer Security (TLS) und SSL, das vor TLS vorhanden war, sind kryptografische Protokolle, die die Kommunikation über ein Netzwerk sichern, indem Sicherheitszertifikate zum Verschlüsseln einer Verbindung zwischen Computern verwendet werden. TLS ersetzt Secure Sockets Layer (SSL) und wird häufig als SSL 3.1 bezeichnet. Exchange Online verwendet TLS, um die Verbindungen zwischen Exchange Servern und die Verbindungen zwischen Exchange Servern und anderen Servern wie Ihren lokalen Exchange servern oder den E-Mail-Servern Ihrer Empfänger zu verschlüsseln. Nachdem die Verbindung verschlüsselt ist, werden alle über diese Verbindung gesendeten Daten über den verschlüsselten Kanal gesendet. Wenn Sie eine Nachricht weiterleiten, die über eine TLS-verschlüsselte Verbindung gesendet wurde, ist diese Nachricht nicht unbedingt verschlüsselt. TLS verschlüsselt die Nachricht nicht, nur die Verbindung.

Zum Aktivieren der Verschlüsselung für einen oder mehrere Exchange-Dienste, muss der Exchange-Server ein Zertifikat verwenden. SMTP-Kommunikation zwischen internen Exchange-Servern wird durch das standardmäßige selbstsignierte Zertifikat verschlüsselt, das auf dem Exchange-Server installiert ist. Zum Verschlüsseln der Kommunikation mit

internen oder externen Clients, Servern oder Diensten möchten Sie wahrscheinlich ein Zertifikat verwenden, das automatisch von allen Clients, Diensten und Servern, die mit Ihrer Exchange-Organisation eine Verbindung herstellen, als vertrauenswürdig eingestuft wird.

Im ersten Schritt müssen wir das Cmdlet New-ExchangeCertificate verwenden, um eine neue Zertifikatsanforderungen (auch als Zertifikatssignierungsanforderungen bezeichnet) für ein neues Zertifikat bzw. eine Zertifikatserneuerung von einer Zertifizierungsstelle (CA) zu erstellen.

Im zweiten Schritt müssen wir das Cmdlet Import-ExchangeCertificate verwenden, um das neue Zertifikat auf unseren Exchange-Servern zu importieren.

Im dritten Schritt müssen wir das Cmdlet Switch-Certificate verwenden, um das alte Zertifikat durch das neue Zertifikat zu ersetzen.

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

Verlängern eines Exchange Server Zertifikats

New-ExchangeCertificate

Import-ExchangeCertificate

Switch-Certificate

3.Sie werten die folgenden DMARC-TXT-Einträge aus:

Unternehmen	DMARC-TXT-Eintrag
Contoso, Ltd.	_dmarc.contoso.com. TXT "v=DMARC1; p=none; sp=reject"
Fabrikam, Inc.	_dmarc.fabrikam.com. TXT "v=DMARC1; p=quarantine; sp=reject"
Litware, Inc.	_dmarc.litware.com. TXT "v=DMARC1; p=reject; sp=reject; pct=50"

Wählen Sie für jede der folgenden Aussagen "Ja", wenn die Aussage wahr ist. Andernfalls wählen Sie "Nein".

(Für jede korrekte Markierung erhalten Sie einen Punkt.)

Abbildung

Aussagen	Ja	Nein
E-Mails für Contoso, Ltd., bei denen die DMARC-Authentifizierung fehlschlägt, werden abgelehnt.	◯	◯
E-Mails von Unterdomänen von Fabrikam, Inc. werden abgelehnt.	◯	◯
Fünfzig Prozent der E-Mails für Litware, Inc., die die DMARC-Authentifizierung nicht bestehen, werden unter Quarantäne gestellt.	◯	◯

A.E-Mails für Contoso, Ltd., bei denen die DMARC-Authentifizierung fehlschlägt, werden abgelehnt: Ja
E-Mails von Unterdomänen von Fabrikam, Inc. werden abgelehnt: Ja
Fünfzig Prozent der E-Mails für Litware, Inc., die die DMARC-Authentifizierung nicht bestehen, werden unter Quarantäne gestellt: Ja
B.E-Mails für Contoso, Ltd., bei denen die DMARC-Authentifizierung fehlschlägt, werden abgelehnt: Ja
E-Mails von Unterdomänen von Fabrikam, Inc. werden abgelehnt: Ja
Fünfzig Prozent der E-Mails für Litware, Inc., die die DMARC-Authentifizierung nicht bestehen, werden unter Quarantäne gestellt: Nein
C.E-Mails für Contoso, Ltd., bei denen die DMARC-Authentifizierung fehlschlägt, werden abgelehnt: Ja
E-Mails von Unterdomänen von Fabrikam, Inc. werden abgelehnt: Nein
Fünfzig Prozent der E-Mails für Litware, Inc., die die DMARC-Authentifizierung nicht bestehen, werden unter Quarantäne gestellt: Ja
D.E-Mails für Contoso, Ltd., bei denen die DMARC-Authentifizierung fehlschlägt, werden abgelehnt: Nein
E-Mails von Unterdomänen von Fabrikam, Inc. werden abgelehnt: Ja
Fünfzig Prozent der E-Mails für Litware, Inc., die die DMARC-Authentifizierung nicht bestehen, werden unter Quarantäne gestellt: Nein
E.E-Mails für Contoso, Ltd., bei denen die DMARC-Authentifizierung fehlschlägt, werden abgelehnt: Nein
E-Mails von Unterdomänen von Fabrikam, Inc. werden abgelehnt: Nein
Fünfzig Prozent der E-Mails für Litware, Inc., die die DMARC-Authentifizierung nicht bestehen, werden unter Quarantäne gestellt: Ja
F.E-Mails für Contoso, Ltd., bei denen die DMARC-Authentifizierung fehlschlägt, werden abgelehnt: Nein
E-Mails von Unterdomänen von Fabrikam, Inc. werden abgelehnt: Nein
Fünfzig Prozent der E-Mails für Litware, Inc., die die DMARC-Authentifizierung nicht bestehen, werden unter Quarantäne gestellt: Nein

Korrekte Antwort: F

Erläuterungen:

Die domänenbasierte Nachrichtenauthentifizierung, Berichterstellung und Konformität (DMARC) funktioniert zusammen mit Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) bei der E-Mail-Absender-Authentifizierung.

DMARC stellt sicher, dass die Ziel-E-Mail-Systeme Nachrichten vertrauen, die von Ihrer Domäne gesendet werden. Die Verwendung von DMARC mit SPF und DKIM bietet Organisationen mehr Schutz vor Spoofing und Phishing-E-Mails. DMARC hilft beim Empfangen von E-Mail-Systemen bei der Entscheidung, was mit Nachrichten aus Ihrer Domäne geschieht, bei denen SPF- oder DKIM-Überprüfungen fehlschlagen.

Eine E-Mail-Nachricht kann mehrere Ersteller- oder Absenderadressen enthalten. Diese Adressen können für verschiedene Zwecke verwendet werden. Sehen Sie sich beispielsweise die folgenden Adressen an:

"E-Mail von"-Adresse: Identifiziert den Absender und gibt an, wohin Rücksendebenachrichtigungen gesendet werden sollen, wenn Probleme mit der Zustellung der Nachricht auftreten (z. B. Unzustellbarkeitsbenachrichtigungen). Mail "Von"-Adresse erscheint im Umschlagteil einer E-Mail-Nachricht und wird von Ihrer E-Mail-Anwendung nicht angezeigt, und wird manchmal als 5321.MailFrom-Adresse oder umgekehrte Pfadadresse bezeichnet.

"Von"-Adresse: die Adresse, die von der E-Mail-Anwendung als Absenderadresse angezeigt wird. "Von"-Adresse identifiziert den Autor der E-Mail. Das heißt, das Postfach der Person oder des Systems, das sich für das Schreiben der Nachricht verantwortlich zeichnet. Die "Von"-Adresse wird manchmal als 5322.From-Adresse bezeichnet.

SPF verwendet einen DNS TXT-Eintrag, um autorisierte sendende IP-Adressen für eine bestimmte Domäne aufzulisten. In der Regel werden SPF-Prüfungen nur für die „5321.MailFrom"-Adresse durchgeführt. Die 5322.From-Adresse wird nicht authentifiziert, wenn Sie SPF allein verwenden. Dies ermöglicht ein Szenario, in dem ein Benutzer eine Nachricht erhält, die SPF-Überprüfungen bestanden hat, aber über eine gefälschte Absenderadresse "5322.From" verfügt.

Obwohl es andere Syntaxoptionen gibt, die hier nicht erwähnt werden, sind dies die am häufigsten verwendeten Optionen für Microsoft 365. Erstellen Sie den DMARC-TXT-Eintrag für Ihre Domäne im folgenden Format:

_dmarc.domain TTL IN TXT "v=DMARC1; p=policy; pct=100"
Dabei gilt:

Domäne ist die Domäne, die Sie schützen möchten. Standardmäßig schützt der Eintrag E-Mail-Nachrichten von dieser Domäne und allen Unterdomänen. Beispiel: Wenn Sie

_dmarc.contoso.com angeben, schützt DMARC E-Mail-Nachrichten der Domäne und aller Unterdomänen, wie z. B. „housewares.contoso.com“ oder „plumbing.contoso.com“.

TTL (Gültigkeitsdauer) muss immer einer Stunde entsprechen. Die für „TTL“ verwendete Einheit, entweder Stunden (1 Stunde), Minuten (60 Minuten) oder Sekunden (3600 Sekunden), unterscheidet sich je nach Registrierungsstelle Ihrer Domäne.

pct=100 gibt an, dass diese Regel für alle E-Mail-Nachrichten (100 %) verwendet werden soll.

policy gibt an, welche Richtlinien der empfangende Server befolgen soll, wenn die DMARC-Prüfung nicht bestanden wird. Sie können für die Richtlinie „none“ (keine), „quarantine“ (Quarantäne) oder „reject“ (ablehnen) festlegen.

Info: Mit dem Parameter "sp" kann eine von der Organisationsdomäne abweichende Richtlinie für Unterdomänen festgelegt werden. E-Mails von Unterdomänen der Domäne fabrikam.com werden nur dann abgelehnt, wenn sie die DMARC-Validierung nicht bestehen.

Die DMARC-Einträge betreffen ausgehende Nachrichten der Unternehmen und werden von den Empfängern der Nachrichten validiert. Die DMARC-Einträge haben keine Auswirkungen auf die von den Unternehmen empfangenen Nachrichten.

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

Verwenden von DMARC zum Überprüfen von E-Mails

4.Ihr Unternehmen verwendet Microsoft Exchange Online. Das Unternehmen erstellt eine E-Mail-Nachrichtenflussregel, um einen Haftungsausschluss an eingehende E-Mails von externen Absendern anzuhängen.

Benutzer berichten, dass E-Mails von externen Absendern den Haftungsausschluss nicht enthalten.

Sie müssen das Problem beheben.

Wie gehen Sie vor?

A.Überprüfen Sie die Überwachungsprotokolle.
B.Führen Sie eine Pipelineablaufverfolgung durch.
C.Führen Sie eine Nachrichtenablaufverfolgung durch.
D.Überprüfen Sie die Nachrichtenverfolgungsprotokolle.

Korrekte Antwort: C

Erläuterungen:

Die Nachrichtenablaufverfolgung im modernen Exchange Admin Center (modernes EAC) verfolgt E-Mail-Nachrichten, während sie durch Ihre Exchange Online Organisation reisen. Sie können ermitteln, ob eine Nachricht vom Dienst empfangen, abgelehnt, zurückgestellt oder zugestellt wurde. Außerdem werden die Aktionen gezeigt, die auf die Nachricht angewendet werden, bevor diese ihren finalen Status erreicht hat.

Die Nachrichtenablaufverfolgung im modernen EAC verbessert die ursprüngliche Nachrichtenablaufverfolgung, die im klassischen Exchange Admin Center (klassisches EAC) verfügbar war. Sie können die Informationen aus der Nachrichtenablaufverfolgung verwenden, um Benutzerfragen zu Nachrichten effizient zu beantworten, Probleme mit dem Nachrichtenfluss zu beheben und Richtlinienänderungen zu überprüfen.

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

Nachrichtenablaufverfolgung im modernen Exchange Admin Center in Exchange Online

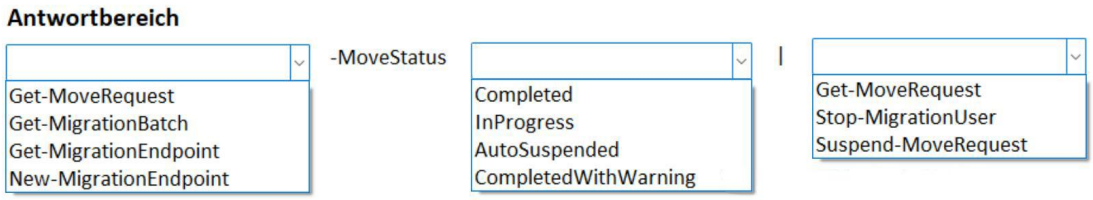
5.Ihr Unternehmen migriert von Microsoft Exchange Server 2019 zu Microsoft Exchange Online.

Sie müssen die Migration anhalten.

Wie vervollständigen Sie den gezeigten Befehl?

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

Abbildung



A.Get-MoveRequest -MoveStatus InProgress | Suspend-MoveRequest
B.Get-MigrationBatch -MoveStatus Completed | Stop-MigrationUser
C.Get-MigrationBatch -MoveStatus AutoSuspended | Get-MoveRequest

D.Get-MigrationEndpoint -MoveStatus InProgress | Suspend-MoveRequest
E.Get-MigrationEndpoint -MoveStatus CompletedWithWarning | Stop-MigrationUser
F.New-MigrationEndpoint -MoveStatus AutoSuspended | Get-MoveRequest

Korrekte Antwort: A

Erläuterungen:

Mithilfe des Cmdlets Get-MoveRequest -MoveStatus InProgress können wir den laufenden Migrationsvorgang als Objekt erfassen und per Pipeline an das Cmdlet Suspend-Moverequest weiterleiten, um ihn zu pausieren. Mithilfe des Cmdlets Resume-MoveRequest kann der Vorgang fortgesetzt werden.

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

Get-MoveRequest

Suspend-MoveRequest

6.Ihr Unternehmen migriert zu Microsoft Exchange Online.

Beim Migrieren eines Batches für öffentliche Ordner wird die folgende Fehlermeldung angezeigt:

Fehler (Für diesen Benutzer wurde kein Abonnement gefunden)

Sie müssen sicherstellen, dass der Migrationsbatch abgeschlossen wird.

Welche zwei Cmdlets sollten Sie verwenden?

(Jede korrekte Antwort stellt einen Teil der Lösung dar. Für jede richtige Auswahl erhalten Sie einen Punkt.)

A.Remove-MoveRequest
B.Start-MigrationBatch
C.Stop-MigrationBatch
D.Remove-MigrationBatch
E.Complete-MigrationBatch

Korrekte Antwort: B, C

Erläuterungen:

Das Problem kann auftreten, wenn die Postfachmigrationsanforderung für öffentliche Ordner, die dem Migrationsbenutzer zugeordnet ist, fehlt oder beschädigt ist,

Lösung
Beenden Sie den Migrationsbatch.

Stellen Sie sicher, dass der Migrationsbatch den Status "Angehalten" erreicht hat.

Starten Sie den Migrationsbatch neu. Dadurch wird die fehlende Migrationsanforderung für öffentliche Ordner erneut erstellt.

Das Cmdlet Start-MigrationBatch startet einen ausstehenden Migrationsbatch, der mit dem Cmdlet New-MigrationBatch erstellt, aber nicht gestartet wurde. Das Cmdlet Start-MigrationBatch setzt auch einen gestoppten Migrationsbatch fort oder wiederholt Fehler in einem Migrationsbatch, der fehlgeschlagen oder mit Fehlern synchronisiert ist.

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

Fehler (ein Abonnement wurde für diesen Benutzer nicht gefunden) beim Migrieren eines Öffentlichen Ordner-Batches

Start-MigrationBatch

7.Ihr Unternehmen verwendet eine Microsoft Exchange Server 2016-Hybridumgebung. Exchange Server enthält Konferenzraumpostfächer und Exchange Online enthält Benutzerpostfächer.

Benutzer in Exchange Online berichten, dass sie beim Planen von Besprechungen mit Konferenzraumpostfächern in Exchange Server nur verfügbare Zeiten anzeigen können.

Benutzer in Exchange Online benötigen die Möglichkeit, das Thema und den Ort anzuzeigen, wenn sie Besprechungen mit den Postfächern des Konferenzraums planen.

Sie müssen das Problem für Benutzer in Exchange Online beheben.

Welches Cmdlet sollten Sie verwenden?

A.Get-OrganizationRelationship
B.Get-AvailabilityAddressSpace
C.Get-IntraOrganizationConnector
D.Get-IntraOrganizationConfiguration

Korrekte Antwort: A

Erläuterungen:

Wir sollten das Cmdlet Get-OrganizationRelationship verwenden, um die Einstellungen für die Organisationsbeziehung abzurufen, die für die Hybridbereitstellung mit Exchange Online erstellt wurde.

Die Einstellungen sollten die Freigabe von Frei/Gebucht-Kalenderinformationen mit Uhrzeit, Betreff und Ort anstelle von Frei/Gebucht-Kalenderinformationen nur mit Zeit ermöglichen.

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

Get-OrganizationRelationship